radware

Report

2026 E-Commerce Bot Threat Report

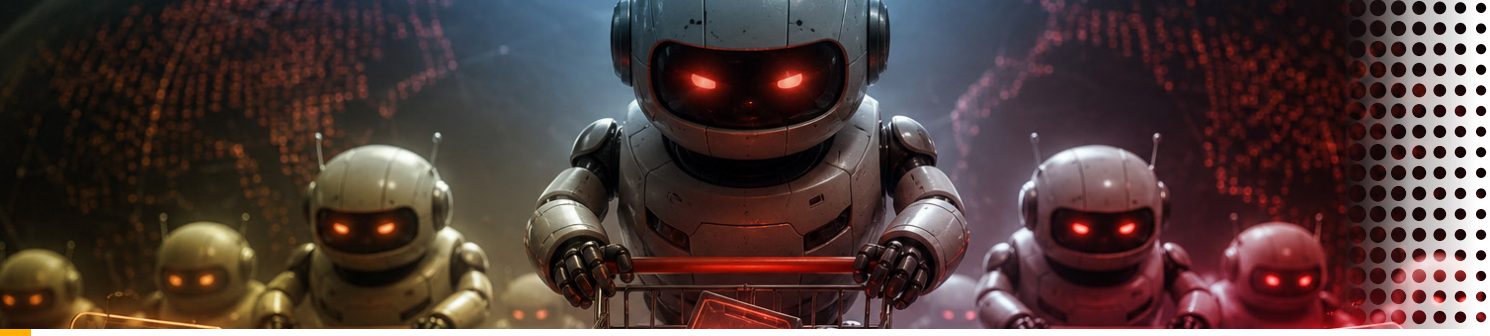


Table of Contents

Executive Summary

For years, the defining story of holiday web traffic has been the steady rise of bots in overall traffic volume. In last year's report, we observed that it crossed a long-anticipated threshold: overall bot traffic exceeded human traffic for the first time. For this year's report, that milestone still holds, but the story has sharpened further. It is no longer about the overall share of bots, but about the share of *malicious bots* specifically, and how close it has drawn to human traffic.

During the 2025 holiday sales period from Thanksgiving through Cyber Monday known as Cyber 5, bad bots accounted for 43% of all traffic to the e-commerce retailers that Radware protects, compared with just 46% from genuine human shoppers.

> As they approach the size of the entire human shopping audience, bad bots are no longer a fraction of automated traffic—they're on the verge of overtaking it.

At the macro level, Radware's 2026 Global Threat Analysis Report found global bad bot volume rose 92% year over year, further proof of the acceleration in bad bot activity.

There is also a shift in *who* is attacking. Although close to 70% of the bad-bot traffic we observed during the last holiday shopping season was low in sophistication, that's not the reassurance it appears to be. It only indicates that the barrier to building a functional malicious bot has collapsed. What once took real development skill now takes a plain-language prompt. Generative AI has redefined the bot threat landscape, making sophisticated attacks more evasive while arming a larger population of less-skilled attackers that could never have attacked at scale before.

A third dimension this season is that of AI crawling at scale, operated by AI platforms as they train large language models (LLMs), index for AI search and retrieve live answers. These are neither malicious nor straightforwardly beneficial to websites. They consume infrastructure, harvest product and pricing data, all with an intent that sits in an ambiguous middle ground.

Even with these new dimensions, the more established attack types did not scale down this past holiday season. Instead, price scraping, account takeovers (ATOs), carding, cart abandonment attacks, etc. on e-retailers all intensified, several by orders of magnitude.

> For security and business leaders, the implication is direct. Automation is now the baseline condition of web traffic and malicious threats are taking over. The question is whether you have visibility into all these types of automation, can distinguish wanted automation from unwanted, and manage them based on business context, all in real-time and at scale on the busiest revenue days of the year.

Key Takeaways

1

Malicious bots drew nearly level with human shoppers.
During the 2025 Cyber 5, bad bots reached 43% of e-commerce web traffic against 46% human traffic. This is up from 31% a year earlier, a roughly one-third jump in a single season.

2

The attacker pool widened more than it deepened.
Close to 70% of bad bot traffic was low in sophistication, up from 44% a year earlier. This shift reflects AI collapsing the barrier to entry, arming a large population of low-skill attackers even as experienced ones use AI to make their attacks more evasive.

3

Attack volumes climbed across every major attack type.
At one large multinational retailer, account takeover more than quintupled and carding rose roughly 15x year over year, against an industry backdrop of broad-based growth across attack types.

4

Attacks struck before the sale, not just during it.
The threat window opened ahead of the sales events themselves, often spiking in the days before Black Friday, timed to when dormant accounts are reactivated and payment methods refreshed, and at their most valuable.

5

AI crawlers are a growing presence, most of them used for LLM training.
Across the season, the mix of crawlers was 54% for training, 27% indexing and 19% retrieval. These results were led overwhelmingly by two operators, with OpenAI's crawlers alone making up 65% of activity and Anthropic's training crawler a further 20%.

6

Advanced attackers keep routing through ISP networks to evade defenses.
Despite the rise of low-sophistication bots, typically data center-based, the relatively unchanged 23% ISP share of bad bot origin signals that sophisticated attackers are still investing in residential proxies and ISP-based routing to mask traffic and evade defenses.

7

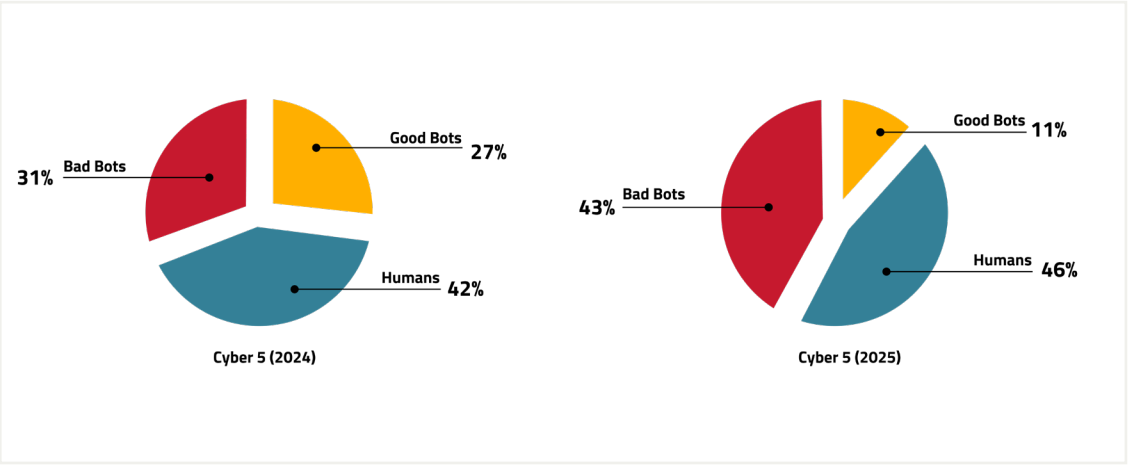
Agentic AI is the next frontier.
AI agents that browse, compare and buy on a genuine user's behalf—in the shift toward agentic commerce—do not fit the human vs. bot binary that bot defenses traditionally rely on. They make the ability to separate trusted from untrusted automation the defining capability for the upcoming shopping seasons.

The State of Holiday Bot Traffic

The defining story of this past year's holiday season web traffic is how close malicious bot share has come to that of human traffic. During the 2025 Cyber 5, human traffic to Radware-protected e-commerce retailers stood at 46% with bad bot traffic at 43%. Good bots accounted for the remaining 11%. A year earlier, the same period split very differently, with humans at 42%, bad bots at 31% and good bots at 27%.

Figure 1:

Web traffic split during Cyber 5 (2024 vs 2025)



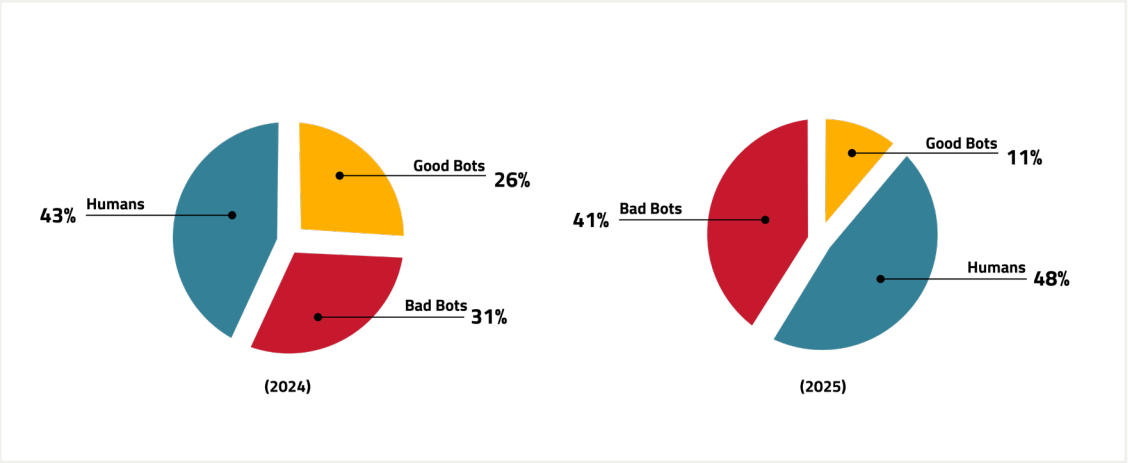
The gap closed largely because bad bot share climbed from 31% to 43% over the Cyber 5, a more than one-third increase in a single year, while human traffic share increased slightly. Malicious bots are now within three percentage points of the entire human shopping audience during the highest revenue days of the year.

The second shift is easy to misread. Good bot share more than halved, from 27% to 11%, but this is not due to a collapse in good-bot activity. Good bot volume held broadly steady, but its share shrank because of the expansion in human shopping and above all, the surge in malicious bot traffic.

The pattern is not confined to the Cyber 5. Across the holiday season period (Figure 2), a similar split appears, with 48% humans, 41% bad bot, and 11% good bots. Whether measured over the Cyber 5 or the larger holiday shopping season, the conclusion is identical. Malicious bot share has expanded to draw nearly level with human traffic, while good bot share has compressed.

Figure 2:

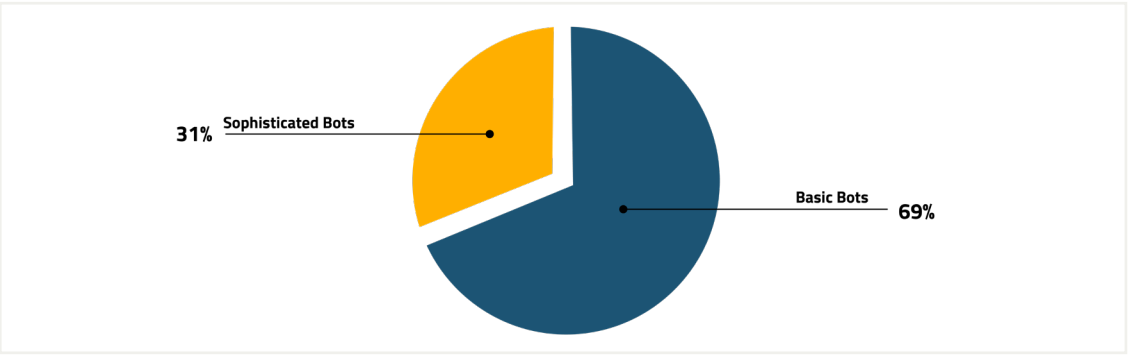
Web traffic split during the holiday shopping season (2024 vs 2025)



Another key finding from this past holiday season's bad bot traffic is the rise of low-sophistication attacks among overall bad bot traffic. Close to 70% of the traffic was low in sophistication or basic in nature, with sophisticated bots making up the remaining 31%. In previous seasons, the balance ran the other way with sophisticated bots being the majority.

Figure 3:

Split of bad bot traffic based on sophistication level (2025)



> Unlike what the numbers seem to convey, the indication here is not that bad bots have become easier to stop. Instead, the opposite is true, and AI has collapsed the barrier to entry for attackers.

Building a functional attack bot that once required real development skill now only requires plain-language prompts.

> And the sophisticated threat hasn't gone anywhere. With the use of AI-based tooling it has only grown more capable, more human-like, and faster to iterate and relaunch. What changed is that the barrier protecting retailers from the less-skilled attackers has fallen.

A large base of low-skill attackers—the “script kiddies” of the AI era—are now able to generate and launch high-volume, low-sophistication attacks with almost no expertise. The two effects run in parallel, with experienced attackers enhancing the sophistication of their bots on the other end.

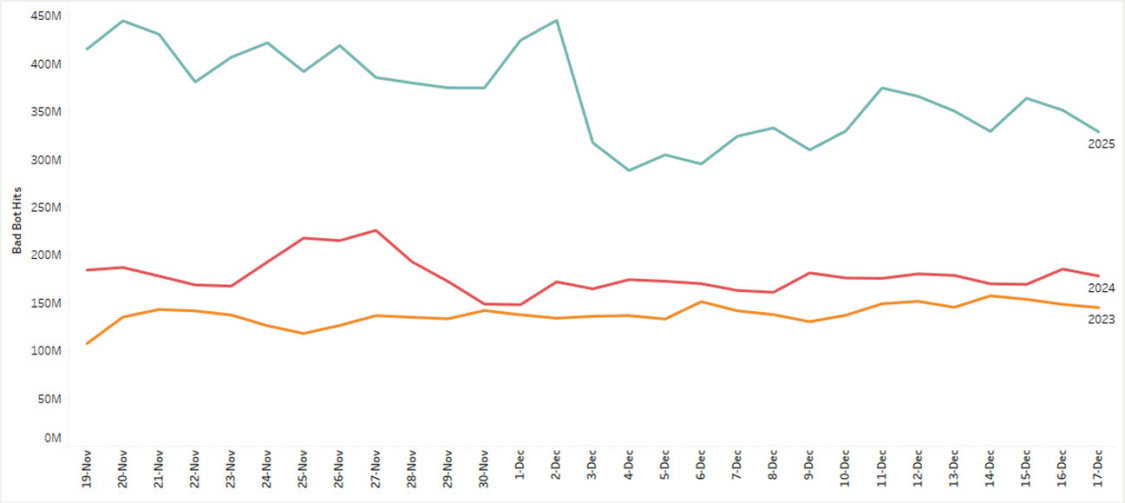
The strategic implication here is that advancement of AI not only brings a larger base of attackers online who adopt AI-based tooling (as seen this year), it also enables attackers to enhance the sophistication of their attacks with minimal skill and effort.

The Attack Timeline

Radware research shows that bad-bot threats built up ahead of key sales events, peaked during Cyber 5 events and then dropped almost as fast as they rose.

Figure 4:

Bad bot traffic trend at a large e-retailer during the holiday shopping season (2025 vs 2024 vs 2023)

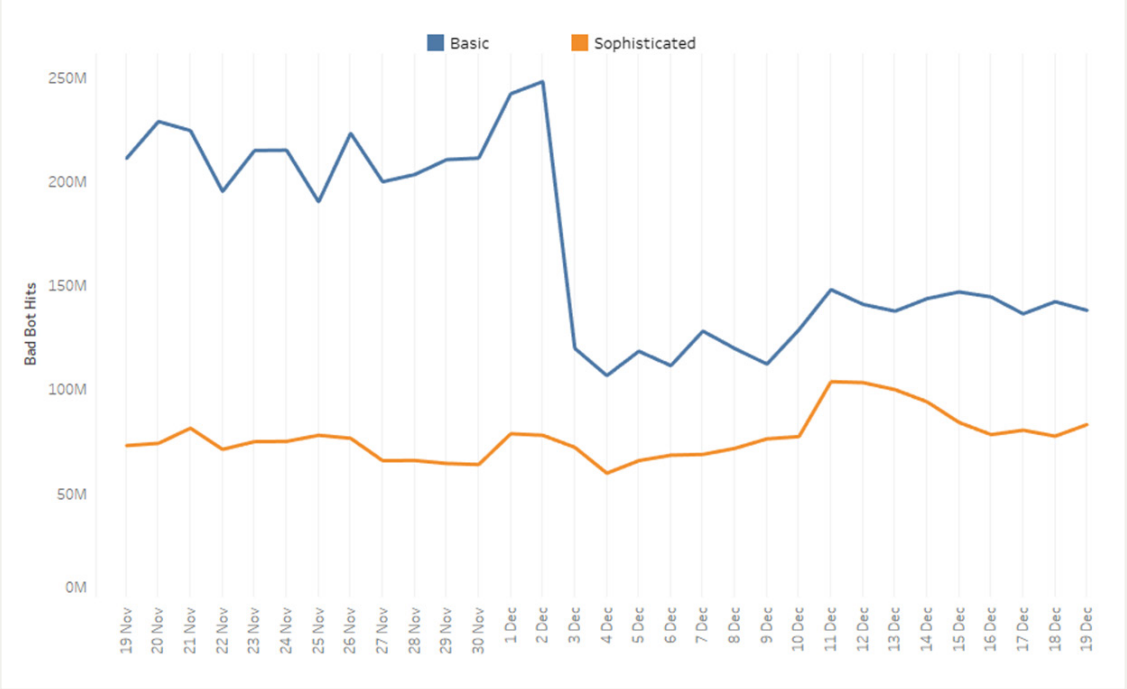


The clearest view comes from a large multinational retailer, where we tracked bad-bot volume across three consecutive holiday seasons (Figure 4). In 2025, the line spiked sharply through the Cyber 5, the highest point of the entire period, then dropped steeply in the days after Cyber Monday. It then settled into a mild daily climb that never again approached the peak. The 2024 trendline for the same retailer rose around the Cyber 5, too, but far more gently and with little movement on either side. The contrast indicates that attackers are increasingly concentrating high-volume attacks onto the few days where it pays off the most, then pulling back the moment the window closes.

The composition of the surge tells the same story, coupled with that of AI enabling the launch of more bot attacks. Across our e-commerce customers, basic bot volume ran consistently higher than sophisticated bot volume through the season, but its defining feature was a sharp drop right after Cyber Monday (Figure 5). Sophisticated bot volume, by contrast, stayed roughly flat throughout. The cheaper, high-volume automation is what floods in for the peak and drops once it passes. Advanced attackers maintained a steady presence throughout.

Figure 5:

Trend of bad-bot sophistication during the 2025 holiday shopping season



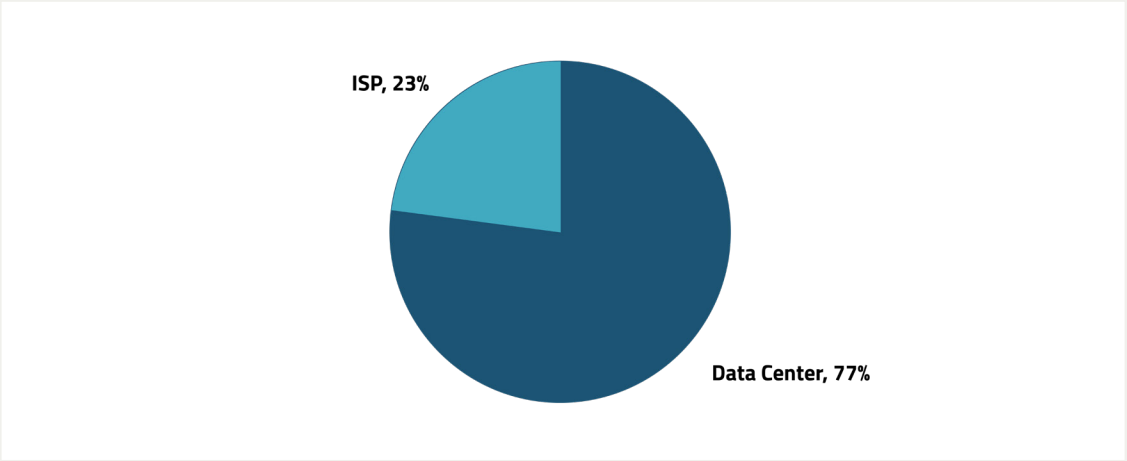
Across attack types, the most aggressive activity often occurred before the sale, not during it. This pre-sale window is when shoppers reactivate dormant accounts, load digital wallets, and refresh stored payment details, increasing the value of those accounts. The key sales events themselves drew the transactional attacks, as card-testing and denial-of-inventory bots tried to blend in when checkout traffic would be the highest.

Bad Bot Evasion and Origin

During the 2025 holiday shopping season, 77% of bad bot traffic originated from data centers and 23% from ISP networks, broadly unchanged from a year earlier. That stability is worth noting, as ISP share might have been expected to fall given the flood of low-sophistication, data center-based bots. It held instead, indicating that sophisticated attackers continued investing in residential and ISP-based routing to disguise their traffic and evade defenses.

Figure 6:

Bad bot origin during the 2025 holiday shopping season

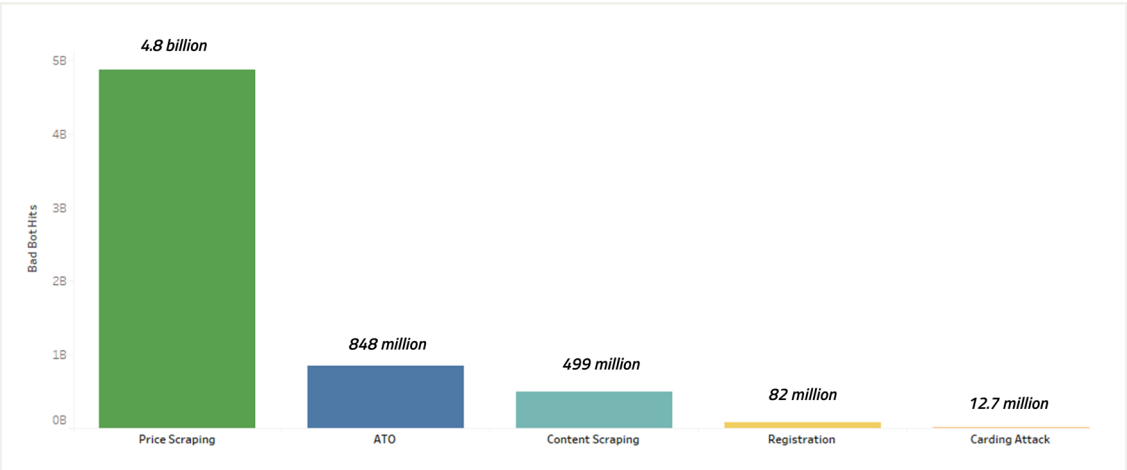


Primary Bot Attack Types

The clearest measure of the increased scale of this season's attack comes from a large multinational e-commerce customer, where price scraping dominated by sheer volume, rising to 5 billion detected attacks this year (Figure 7). ATO grew dramatically, by more than 5x from last year to around 900 million attacks this year. Carding rose to roughly 12 million, a 15x jump in the most financially direct attack of all. Fake registrations climbed to roughly 80 million, while content scraping held broadly level at around 500 million compared to last year.

Figure 7:

Bot attack types detected at a large multinational e-retailer during the 2025 holiday shopping season



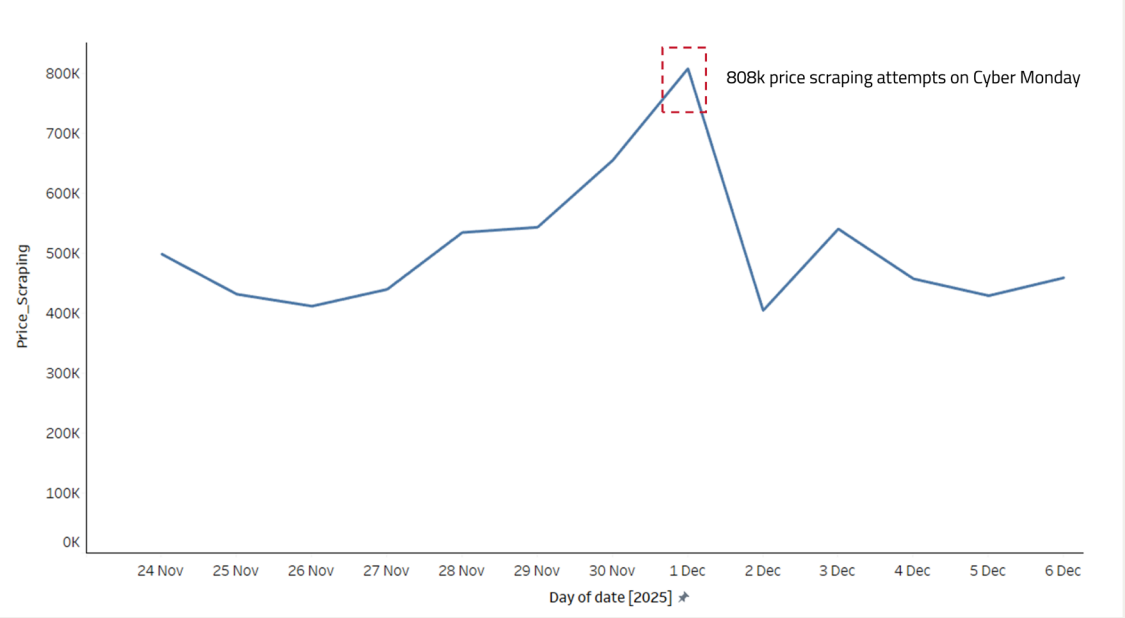
The following sections take each attack type in turn, with evidence drawn from across our e-commerce customer base.

Price Scraping

Price scraping is the systematic extraction of product pricing from e-commerce websites, typically by competitors or third-party aggregators chasing real-time competitive intelligence. During the holiday shopping season, when pricing is at its most dynamic, the incentive to scrape continuously is at its highest.

Figure 8:

Price scraping attacks detected at an e-retailer during the 2025 holiday shopping season



Holiday observations: At one retailer, price scraping climbed roughly 70% through the Cyber 5 period, peaking on Cyber Monday—a pattern of sustained monitoring. The timing fits the season's logic, with rivals scraping harder to keep pace with retailers adjusting promotion pricing through the key sales events.

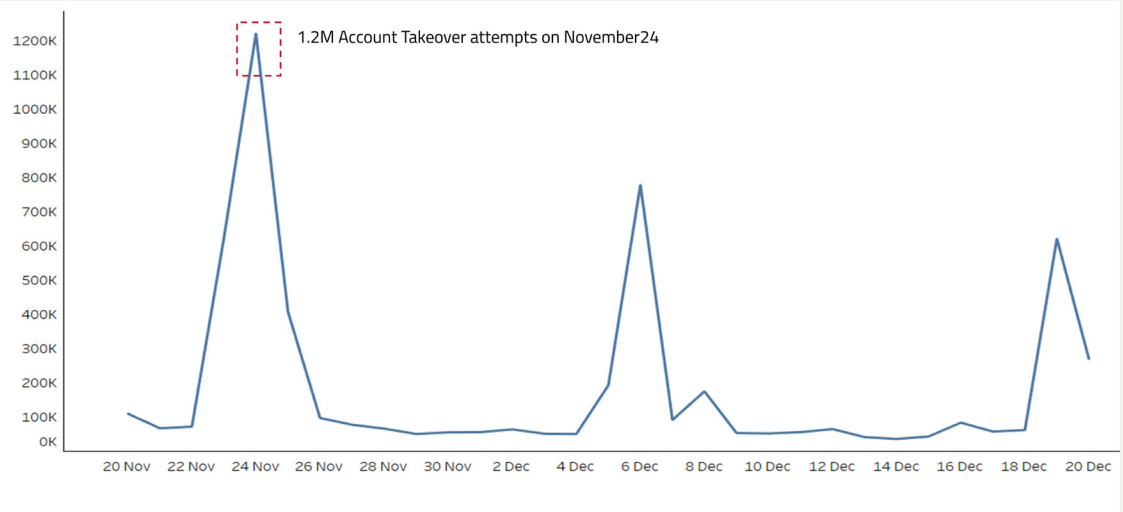
Business impact: Real-time visibility into a retailer's pricing lets competitors undercut promotions the moment they launch, neutralizing the advantage a carefully planned sale event is meant to create. At scale, scraping also imposes a rising infrastructure cost, consuming capacity, degrading site performance for genuine shoppers during peak load and distorting the analytics that retailers rely on for business decisions.

Account Takeover

Account takeover (ATO) uses credential stuffing, credential cracking and brute-force techniques to gain unauthorized access to customer accounts. Attackers gather credentials from prior breaches in the weeks before the season, then deploy bots against login workflows during the peak days of the sale, when account activity and the value locked inside those accounts is at its maximum.

Figure 9:

Account takeover attacks detected at an e-retailer during the 2025 holiday shopping season



Holiday observations: ATO showed the most aggressive pre-sale timing of any attack type this year. At one retailer, ATO attempts surged roughly 1,100% just four days ahead of Black Friday. The window just before the sale is when shoppers reactivate dormant accounts, top up digital wallets, and refresh stored payment details, making it the period with maximum returns for attackers. The more than quadrupling of ATO attack volume year over year at the large multinational customer example described earlier reinforces that this is becoming a highly preferred attack type during the holiday season.

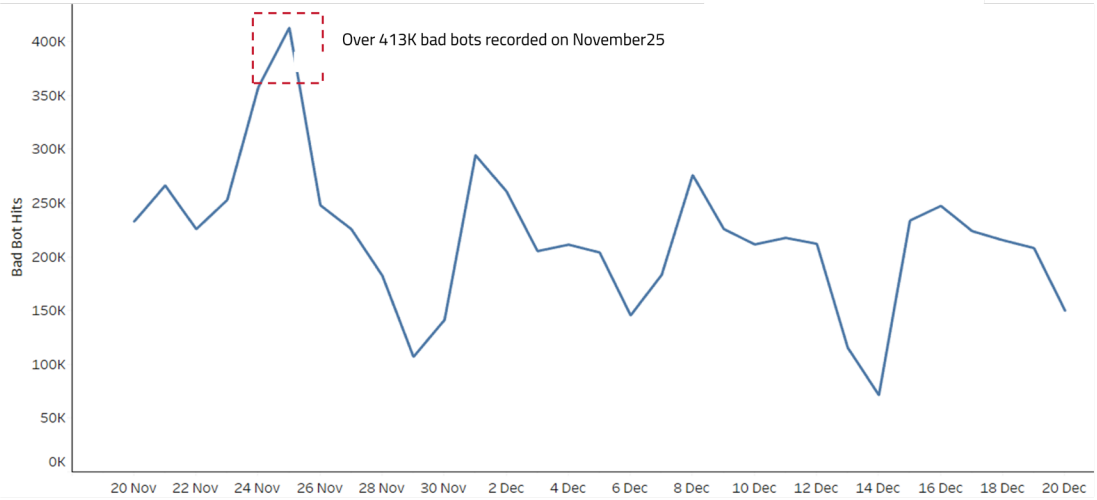
Business impact: ATO is among the costliest attacks a retailer can suffer, with chargebacks, refunds, investigation and remediation costs, customer-service load, and the regulatory exposure that follows any breach of stored payment or personal data. Also the reputational damage from customers learning their accounts were compromised during the holidays can outlast the season itself.

Content Scraping

Content scraping extracts a retailer's proprietary content such as product descriptions, photos, specifications and customer reviews, for reuse on competing sites. Beyond the extraction itself, duplicated content can erode the original retailer's search rankings and dilute the value of marketing investments made.

Figure 10:

Content scraping attacks detected at an e-retailer during the 2025 holiday shopping season



Holiday observations: Content scraping mirrored the pre-emptive timing seen in ATO. At one e-commerce customer, content scraping rose roughly 70% three days before Black Friday, consistent with competitors and aggregators moving to capture catalog content before promotional changes rolled out.

Business impact: The impact is both competitive and reputational. Scraped product content lets rivals replicate cheaply, and duplicate content can trigger search engine penalties that reduce organic traffic. When shoppers encounter the same listings across multiple sites, they lose confidence in the original brand.

Fake Account Registration

Fake registration uses automation to create large volumes of fake customer accounts, typically to exploit new customer promotions, referral bonuses and other acquisition incentives. They are also used as a launchpad for further fraudulent activities.

Holiday observations: This was one of the fastest-growing attack types of the season. At the large multinational retailer referenced earlier, fake registrations increased 7x year over year. Growth at that scale suggests attackers are shifting resources to registration abuse, likely because it has proved effective. Fake registrations tend to cluster around the launch of holiday promotions, when new-customer offers are most generous.

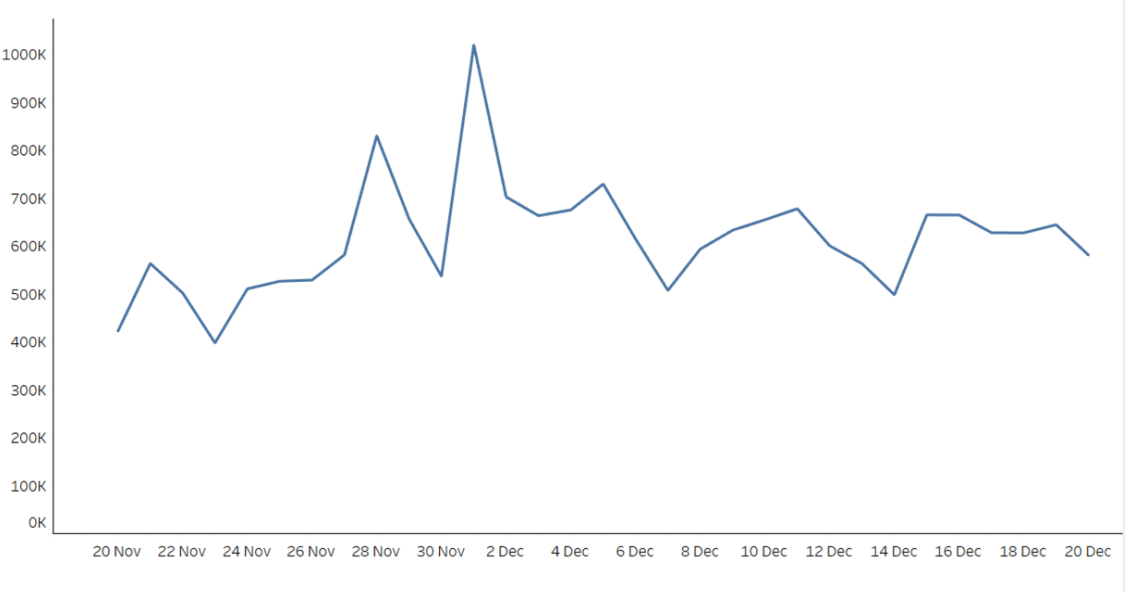
Business impact: Beyond the direct cost of abused promotions, fake accounts corrupt the business metrics retailers use, inflating user counts, distorting customer acquisition cost and conversion calculations, and leading to marketing decisions made on bad data. Each fake account is also used as a staging ground for downstream fraud, from promotion abuse to carding.

Carding

Carding tests stolen payment card data against a retailer's checkout to identify which cards are still valid. Validated cards are then used for larger fraud on the same site or elsewhere or resold. Modern carding distributes its attempts across many accounts to evade rate-based detection.

Figure 11:

Carding attacks detected at an e-retailer during the 2025 holiday shopping season



Holiday observations: From an overall attack volume perspective, carding is lower relative to other attack types like scraping, but the financial impact remains high. At one retailer, carding attacks spiked roughly 100% on Cyber Monday and roughly 60% on Black Friday, as attackers attempted to blend their card testing inside the season's heaviest legitimate checkout traffic.

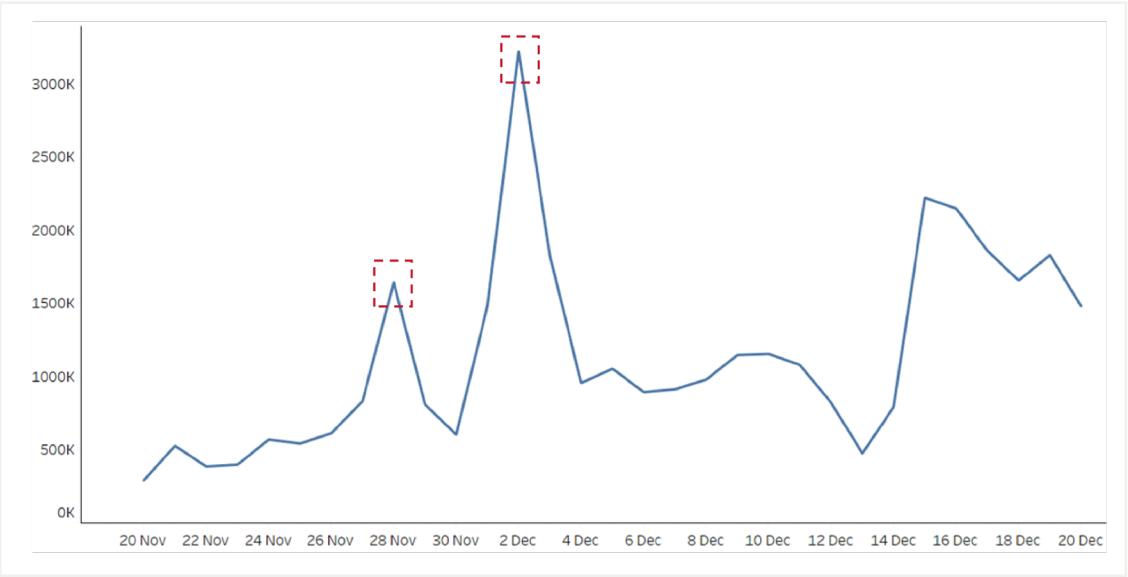
Business impact: Each validated card leads to losses far larger than the test transaction itself. The resulting impact can include fraudulent purchases, chargebacks, payment processor penalties, and potential breach of PCI DSS or related obligations. Businesses must deal with all of this along with the loss of customer trust that follows any payment compromise.

Cart Abandonment/Denial of Inventory

Cart abandonment attacks, also called denial of inventory or inventory hoarding, use bots to add high-demand items to carts at scale with no intention of buying, locking real shoppers out of stock during peak sale periods. Sophisticated variants of this attack can defeat session-based cart timeouts by revisiting and re-adding items to cart.

Figure 12:

Cart abandonment attempts detected at an e-retailer during the 2025 holiday shopping season



Holiday Observations: This type of attack strikes hardest on the peak days. At one retailer, cart abandonment attacks rose 500% on Cyber Monday and roughly 200% on Black Friday, with attackers hoarding inventory on the days of peak demand.

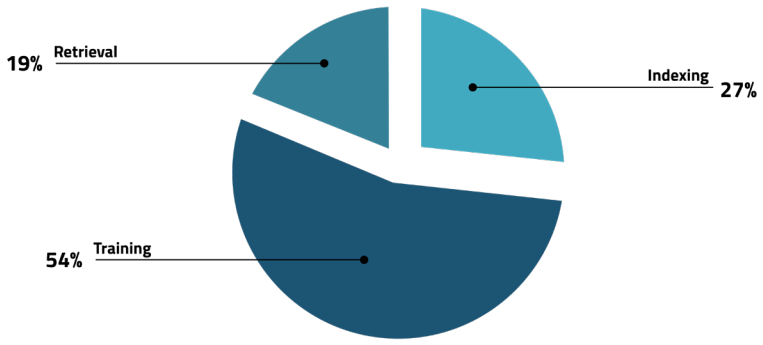
Business Impact: The losses are immediate: genuine shoppers abandon for competitors when items show as unavailable, conversion and abandonment analytics are corrupted, distorting analysis on real consumer behavior, and false demand signals can misguide inventory forecasting and supply-chain decisions. For retailers spending heavily to drive traffic to specific promoted products, inventory hoarding can waste marketing investments.

The AI Crawler Dimension

AI crawlers—the new, third class of automated traffic—fit neither the “good” or “malicious” label cleanly. Operated by AI platforms, they fall into three functional types, and across the holiday shopping period we observed them in the following proportions: AI-training crawlers at 54%, AI-indexing crawlers at 27% and AI-retrieval crawlers at 19% (Figure 13).

Figure 13:

Split of AI crawling activity by intent, detected during the 2025 holiday shopping season

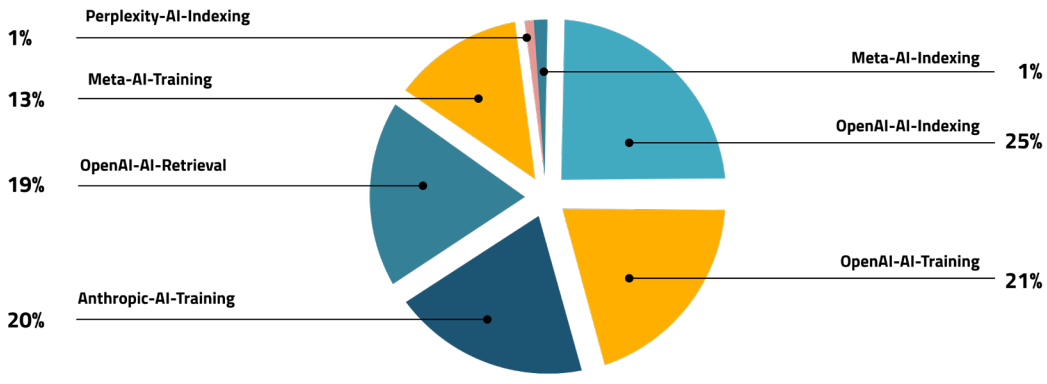


The purpose of each is well established: Training crawlers such as OpenAI’s GPTBot and Anthropic’s ClaudeBot collect web content to train and improve LLMs. Indexing crawlers gather content to surface in AI-powered search. Retrieval crawlers fetch live information in real time to answer a specific user query.

By operator, the breakdown across these crawlers was led by OpenAI and Anthropic. OpenAI’s crawlers alone made up 65% of all crawling activity. Anthropic’s training crawler was observed at 20% of all crawling activity, while Meta’s training crawler was observed at 13% (Figure 14).

Figure 14:

Split of AI crawling activity by source platform and intent, detected during the 2025 holiday shopping season



What makes AI crawlers a genuinely new problem is that they are neither malicious, like ATO, carding bots, etc., nor straightforwardly beneficial. Each AI crawler consumes infrastructure and harvests commercially valuable data, while the benefit returned to the retailer ranges from real (visibility in AI search) to negligible (content taken to train a commercial LLM model). This makes them a new management problem. The right response is intent-dependent, and retailers without advanced bot management lack the tooling to distinguish one crawler's intent from the other's, let alone the capability to manage them based on business context.

AI crawlers are also not just background noise in web traffic. At one retailer, AI crawling activity spiked three days before Black Friday (Figure 15). At another, it jumped more than 300% on specific days in December, driven primarily by training crawlers from Anthropic and OpenAI (Figure 16). And at a third retailer running a dedicated sales event between November 14 and 20, it drew a clear lift in crawling alongside the traffic surge.

Figure 15:

Split of AI crawling activity by source platform and intent, detected during the 2025 holiday shopping season

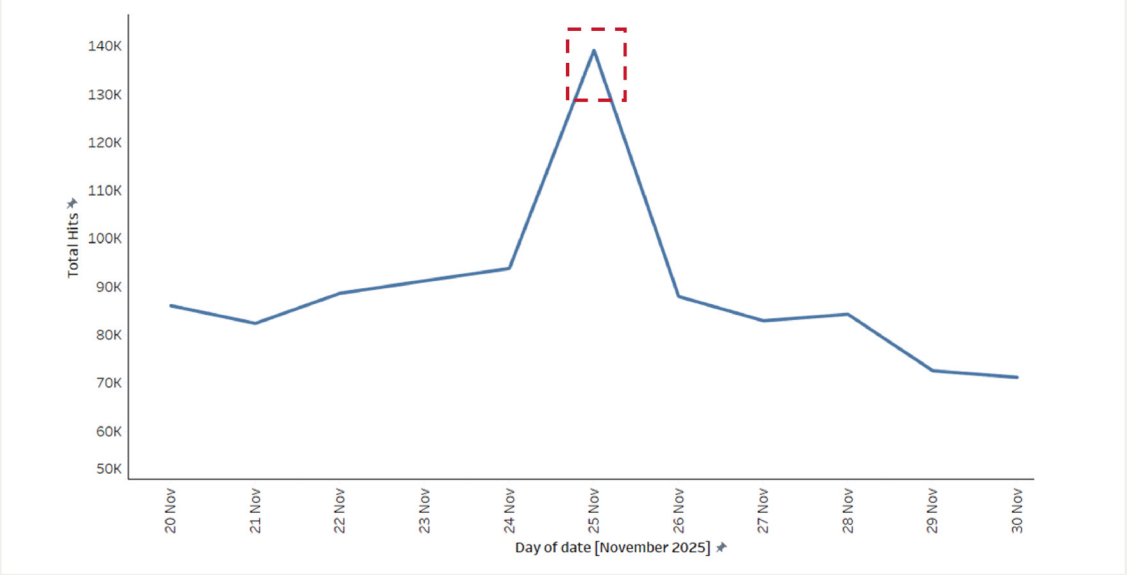
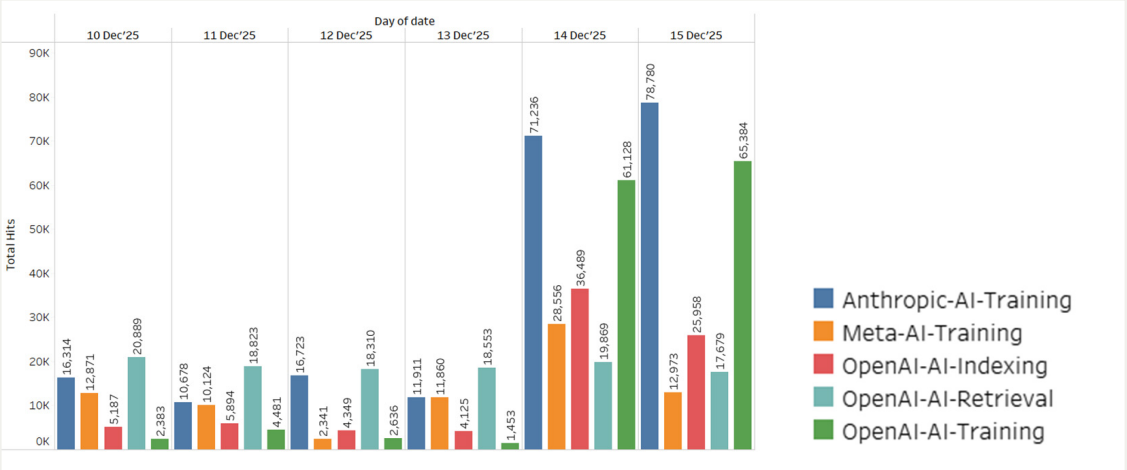


Figure 16:

Surge in AI crawling activity at an e-retailer, detected during the 2025 holiday shopping season



A 300% surge in the middle of sales events competes for the very capacity a retailer needs to serve revenue-generating customers. A second concern is data exposure, with training crawlers forming a major share of crawling activity. Retailers' proprietary content and pricing are being gathered at scale to train LLMs, with no real benefit in return, while also being used for commercial purposes.

Business Impact of Holiday Shopping Attacks

Reduced Revenue and Conversion: When bad bots approach human traffic in volume, and when denial of inventory and ATO attacks peak around critical sales events, revenue and conversion rates are directly affected. Genuine shoppers who find items out of stock or abandon a platform after a compromised-account experience will take their potential payment to a competitor on the highest-stakes days of the year.

Higher Infrastructure Costs: Large-scale scraping and surging AI crawler activity both consume real capacity. Serving non-human, malicious traffic at this scale means provisioning and paying for infrastructure that returns no sales, costing the hardest during peak load when capacity is most expensive.

Competitive Disadvantage: Price and content scraping hand competitors real-time intelligence, while AI training crawlers gather product and pricing data into systems beyond the retailer's control. Each of these negatively impacts the proprietary advantage that a retailer's competitive business strategies are meant to provide.

Loss of Customer Trust and Data Integrity: Bot attacks such as ATO and carding directly impact customer trust and carry regulatory consequences. Other attacks such as fake registrations and denial of inventory distort the analytics that guide crucial business decisions, so the damage outlasts the attack.

Radware's Recommendations for E-Commerce Organizations

Establish complete visibility into non-human traffic.

The ability to see and classify any and all types of bot traffic reaching applications is the key to every advanced defensive capability. With the modern bot threat landscape consisting of malicious bots, AI crawlers and the first wave of AI agents, effective defense begins with granular classification of all non-human traffic, supported by analytics that reveal how each class behaves across applications.

Counter AI-driven bot threats with AI-powered defenses.

Gen AI has enabled attackers to both enhance the sophistication of attacks, with bots closely replicating human behavior, rotating identities and iterating at machine speed, while also arming a large population of low-skill attackers to generate functional bad bots from simple prompts. Traditional defenses cannot keep pace. Organizations need AI-powered, behavior-based detection layered with preemptive blocking of known threats and real-time mitigation. And it's important to sustain that accuracy at scale, even on the highest traffic days when both legitimate demand and attack volume peak together.

Govern AI crawlers based on business context.

AI crawlers need to be managed deliberately, rather than blocked by default. Indexing crawlers may deliver value through visibility in AI-powered search, while training crawlers may extract proprietary data while returning nothing to the retailer. With AI crawling activity now a mainstay of the AI era, acting on that distinction requires the ability to classify crawlers by operator and declared purpose and to apply different actions at a per-crawler level.

Prepare for the AI agentic shift & agentic commerce.

The next class of AI-powered actors is already here: AI agents that browse, compare and transact on a genuine customer's behalf. These actors break the human vs. bot binary entirely. They are non-human, yet they may be acting on behalf of a customer with genuine purchase intent. The defining defensive capability in upcoming seasons will be the ability to distinguish a trusted agent acting for a real customer from an untrusted one, when both are automated. Retailers that prepare for this shift now, rather than blocking all automation and turning away legitimate, AI agent-driven revenue, will be best positioned to capture the benefits of agentic commerce while containing its risks.

Deploy advanced, low-friction mitigation techniques.

Effective defense depends not only on accurate detection, but on the way a retailer responds once a malicious bot is identified. Traditional interactive challenges have lost much of their effectiveness with the widespread availability of CAPTCHA-farm services, while these same challenges continue to cause friction for legitimate customers and degrade the shopping experience. Modern bot mitigation requires a flexible range of response options with an emphasis on techniques that remain invisible to the genuine user. Non-interactive methods such as cryptographic challenges can effectively counter sophisticated bots without affecting legitimate shoppers, while the more traditional challenges are best reserved for high-risk traffic rather than as a blanket first line of defense.

Adopt an integrated, cross-layer application defense.

Attackers increasingly combine automated bot campaigns with other application-layer attacks such as API business logic exploitation, probing multiple defensive layers at once. They do so when security teams are most stretched thin, during the highest traffic days of the year. Retailers must onboard an integrated protection approach that correlates threats across bot management, WAF, API security, etc., supported by managed security services that extend the security team's capacity through continuous monitoring and rapid response.

The Outlook Ahead

The 2025 holiday season marked a threshold. For years, the headline was that the web was growing more automated; this year it is that malicious bots alone drew nearly level with human shoppers during the peak season. On the current trajectory, bad bots will soon cross from near parity to outright majority of holiday traffic. It is now a question of when—not whether—they will take the lead.

> The trends shaping the 2026 season are clear: AI will continue to lower the barrier to entry and sophistication, and the defense that responds to this will need to be increasingly AI-powered itself.

The bigger shift is in the changing humans-vs-bot distinction itself, which has been the baseline of bot defense up until now. AI crawlers already occupy an ambiguous middle ground, and AI agents will widen it further with automated traffic that has a genuine user behind it, carrying genuine purchase intent in an agentic commerce use case.

> As the grey zone grows, the defining question shifts from “human or bot?” to “trusted or untrusted?” for organizations.

The retailers best positioned for the upcoming shopping seasons are the ones that can govern the full spectrum of web traffic. They must distinguish the genuine shopper, malicious bot, useful crawler and trusted agent apart while applying the right response in real time and at peak scale. That capability will be what separates the protected from the exposed in 2026.

Get the statistics and storylines behind the threats.

For a broad analysis of cross-industry global network and application attack trends based on Radware’s 2025 threat intelligence, read Radware’s 2026 Global Threat Analysis Report.

RWI6385 | 06.16.2026