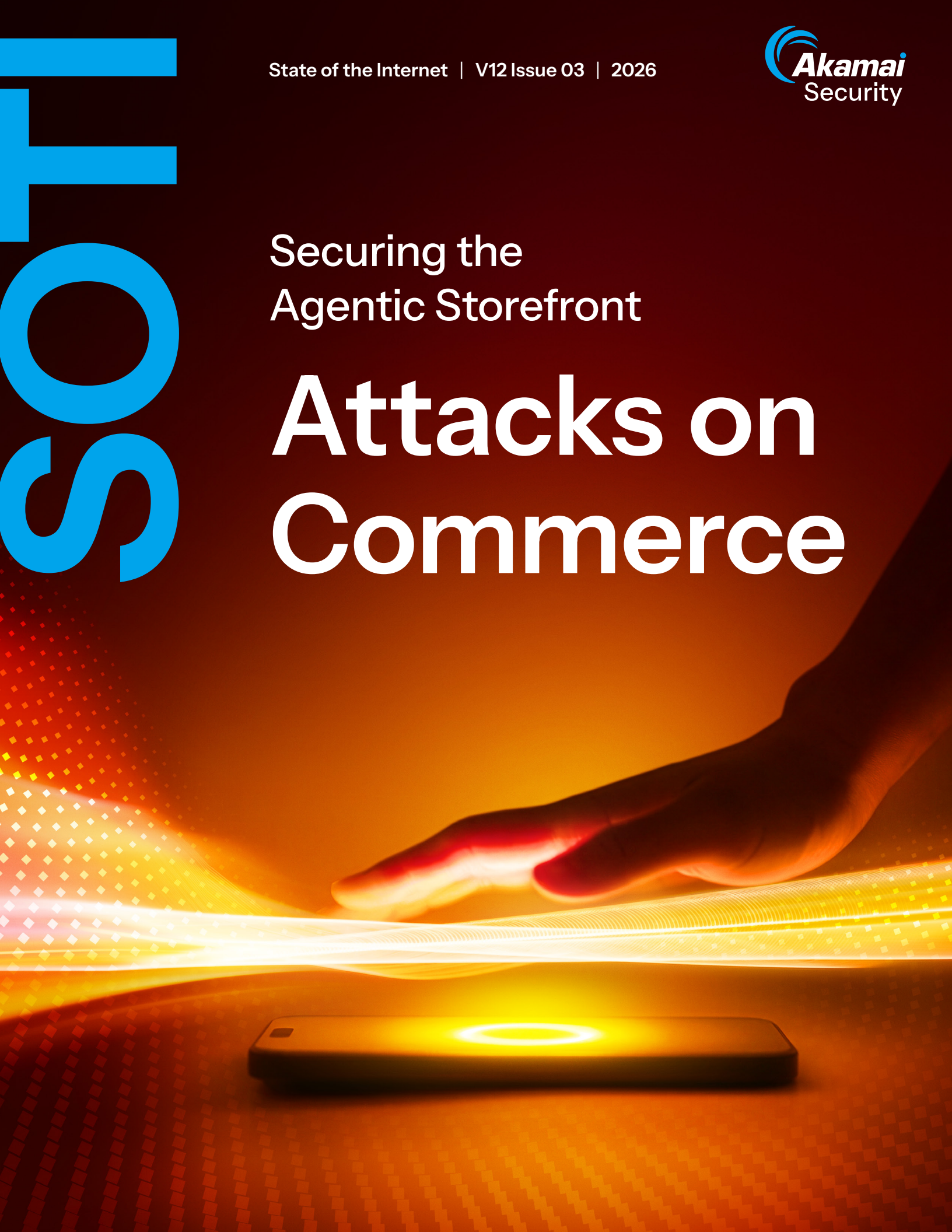
State of the Internet | V12 Issue 03 | 2026

Akamai Security

SOTI

Securing the Agentic Storefront

Attacks on Commerce



Contents

Akamai Security

Introduction

The commerce industry is entering a sophisticated new chapter — one in which the interaction between brands and consumers is increasingly automated, and the line between legitimate activity and malicious exploitation has never been harder to discern. Three years have passed since a State of the Internet/Security report took a comprehensive look at the commerce landscape, and the environment has shifted fundamentally from traditional digital transactions to what is now known as agentic commerce — an ecosystem where AI-driven shopping tools, autonomous agents, and automated processes have become the new standard.

Although agentic commerce unlocks significant opportunities for growth and personalization, it also raises the baseline of resilience that organizations must achieve — consistently — to remain competitive. Commerce has become a high-interest target for application-layer distributed denial-of-service (DDoS) activity, user-targeted fraud, sustained web traffic anomalies — and, critically, these pressures are no longer seasonal. The threat window has expanded to be year-round, making uptime and reliability the ultimate currency.

This State of the Internet (SOTI) Security report examines the key factors that are shaping the commerce landscape.

- **The evolution of bot activity:** Beyond simple automation, sophisticated bot-driven processes are directly impacting daily economic stability, from inventory manipulation to checkout abuse.
- **The intersection of APIs and account security:** As organizations rely more on interconnected systems, the focus has shifted toward securing the API gaps that often serve as a bridge between a legitimate login and a fraudulent transaction.
- **The impact of generative AI:** From synthetic storefronts to AI-enhanced phishing, generative AI is reshaping how adversaries target both brands and their customers.
- **The proliferation of industrialized phishing and malware:** The growth of daily phishing attacks — coupled with specialized access tools like Remote Access Trojans (RATs) — fuels a highly monetized account takeover (ATO) pipeline targeting widely used identity and ecommerce platforms.

As security teams begin their holiday preparation, the goal should be to build a foundation of integrated situational awareness. Three years of rapid innovation have expanded the digital footprint, and protecting that footprint — reliably, at scale, and year-round — is no longer an operational goal. It is a strategic one.

This report is designed to serve as a strategic guide, and it includes a mitigation roadmap that helps commerce leaders balance the openness their customers expect with the steady, reliable protection business requires. Understanding these shifts is what separates organizations that successfully navigate the autonomous economy from those that are left managing its consequences.

Akamai Security

Guest column

How agentic commerce is rewriting the fraud playbook

The retail industry has always prioritized seamless customer experiences, a trait that modern cybercriminals are now exploiting with hypersophistication. As fraud evolves, individual retailers cannot afford to defend their digital perimeters in isolation. Resilience requires a unified front. At the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC), we facilitate this exact model of collective defense and industry-wide collaboration. This shared approach is more critical than ever as emerging technology introduces new vectors for exploitation.

Your shopping bot is a visibility gap

Agentic commerce (autonomous AI agents that browse, compare, and purchase on behalf of humans) is the latest hot retail trend. It has, however, introduced a massive signal masking problem. Historically, security systems relied on consumer digital fingerprints to distinguish humans from bots. AI shopping agents are now designed to mimic these human microbehaviors perfectly, rendering traditional detection methods obsolete.

This development has left retailers with a massive visibility gap. Beyond masking, we are also seeing the rise of agent hijacking; that is, fraudsters compromising users' legitimate AI agents and abusing preexisting trusted relationships and stored payment credentials with multiple retailers to execute a wave of unauthorized purchases before the customer or the retailer even notices.

Loyalty points are the new shadow currency

Criminal syndicates have shrewdly recognized the enormous opportunity in what some experts have labeled the shadow currency of loyalty programs. Account takeover rates have consistently increased year over year with the biggest single target being inactive accounts.

Because they are poorly monitored, inactive accounts are ideal environments for point laundering. In the hospitality industry, these stolen points are often quickly exploited by booking free hotel accommodation or buying costly retail items to be resold to a third party at a discounted rate.

Meet synthetic identity fraud

If that is not sobering enough news, there has been a rise in synthetic identity fraud, in which fraudsters use large language models (LLMs) to blend legitimate data (such as a real Social Security numbers) with fabricated elements to create "Frankenstein" accounts. These accounts are cultivated to appear as long-term loyal customers, effectively bypassing standard fraud detection. The danger scales further with hyper-realistic phishing and deepfake voice and video.

Cooperative resilience and the security loop

Static defenses cannot survive machine-speed attacks. Organizations must shift to a security loop model: a continuous feedback framework designed to transform a single organization's threat detection into an enterprise-wide, or better yet, industry-wide immune response.

- **Anticipate:** Focus on hardening defenses with Zero Trust architecture and passwordless authentication to eliminate exploitable vulnerabilities
- **Monitor:** Use behavioral biometrics to aid AI models in flagging anomalies
- **Respond:** Use automated kill switches to instantly freeze accounts if suspicious point-draining is detected, and step-up authentication to prompt users to re-verify their identity with stronger credentials (i.e., multi-factor authentication) to limit the fraud blast radius
- **Recover:** Go beyond root cause analysis to customer restitution and financial entanglements resolution
- **Share intel:** Share pre-incident anonymized telemetry data during the detection phase to provide early warnings to the community, and post-incident full forensic reports to help the industry understand the how and why of an attack

Intelligence-to-action velocity

Today, security is no longer measured by the height of your "high walls," but by the velocity of your intelligence-to-action cycle. As AI-driven fraud evolves quickly, most static defenses have become liabilities rather than assets. Success now depends on **cooperative resilience**, and the ability to protect your unique logic while participating in a global defense network.

The ultimate challenge for retail and hospitality leaders is navigating the friction paradox. How can we implement enough security to stop a synthetic identity fraud scheme or a hijacked agent without eroding the seamless, trust-based experience that our customers demand? The answer lies not in isolation, but in the collective strength of a shared defense. Through the RH-ISAC, companies have a platform to turn collective strength into actionable velocity, transforming individual threat telemetry into an industry-wide shield.

Pam Lindemoen
Chief Security Officer and Vice President, Strategy, RH-ISAC

Akamai Security

Expert insight

The economy of autonomous agents: Is your commerce security ready?

As the Executive Vice President and General Manager of Security Technology for Akamai, I am constantly in high-level discussions with CISOs about the unique volatility of the commerce sector. As one of the most exposed industries in the threat landscape, commerce is tasked with an incredibly difficult challenge: maintaining an open, frictionless experience for customer convenience while building a fortress around their data. And, today, the conversation is even more nuanced. We are now securing an entire ecosystem where the "customer" is just as likely to be an autonomous

Security leaders must navigate technical risks while ensuring agentic readiness. When I look at the current state of cybersecurity, a few specific shifts stand out as the most critical:

- The commerce exposure
- The rise of API abuse and account takeover
- Security priorities for CISOs
- AI as a tool for exposure governance
- The dangerous misconception: "We are secure"

The commerce exposure

Commerce organizations must operate within a unique set of pressures that other industries don't face at this scale:

- **Continuous value drain:** Scrapers constantly drain competitive value from ecommerce sites, siphoning pricing and inventory data in real time, and undermining competitive advantage before you even realize the data is gone.
- **Exploitation of peak events:** Attackers deliberately target high-traffic holiday windows, major sales, and large marketing campaigns, turning every outage into a crisis.
- **Generative AI (GenAI) phishing:** GenAI is now weaponizing brand identity through hyperconvincing fake storefronts and phishing campaigns that target customers.

The rise of API abuse and account takeover

API abuse has become the entry point of choice for a reason. APIs allow attackers to bypass traditional controls and access sensitive pricing, inventory, and loyalty data at a massive scale.

Account takeover compounds this directly. Once credentials are harvested through stuffing or phishing, APIs become the tools used to convert stolen identities into fraudulent transactions, chargebacks, and loyalty point theft. The impact on brands and fraud rates erodes customer trust and profitability.

Akamai Security

Security priorities for CISOs

In this environment, we cannot rely on a single gatekeeper. A defense-in-depth strategy is the only way to build true resilience. I recommend a layered approach that prioritizes the following security capabilities:

- **Manage and mitigate bots:** Implement a strategy that protects your sites from malicious bots while remaining available and understood by legitimate GenAI shopping agents.
- **Discover and secure APIs:** Get visibility into your APIs, understand if they are secure, know what kind of data is on them, and protect them from abuse.
- **Manage and mitigate vulnerability risk:** Ensure that your ecommerce site is patched. In environments where this isn't possible, ensure that your web application firewall (WAF) is up to date and can protect you.
- **Segment networks:** Minimize the impact of an attack by segmenting your network to contain lateral movement and protect valuable assets.

AI as a tool for exposure governance

Commerce organizations have an opportunity to use AI to transition from static defenses to adaptive protection and manage exposure in a rapidly evolving operating environment.

Project Glasswing, a new class of AI capability, can potentially discover and exploit software vulnerabilities at a pace and depth that no human team, regardless of skill, could match. History suggests commerce and finance will be the most targeted industries for these emerging capabilities. However, this capability also unlocks autonomous validation for defenders, providing teams with a head start to find and fix weaknesses faster. AI allows junior security operations center (SOC) analysts to use natural language queries to perform research that previously required a decade of experience.

The impact of AI for defenders extends beyond vulnerability management. For example, security tools that have been infused with AI-powered capabilities can apply policy enforcement in real time, allowing defenders to move as fast as attackers.

The dangerous misconception: "We are secure"

The most dangerous thing a commerce leader can say is: "Our perimeter is secure, so we aren't too concerned about ransomware or malware in our network … and we'd *know* if we were breached."

Relying on perimeter defense alone is a gamble that can lead to a business-ending catastrophe. Attackers may already be inside the environment, dwelling silently while they escalate privilege. Resilience is less about the architecture and more about integrated situational awareness to alert on and block unsanctioned activity.

A CISO's strategic roadmap

If you are leading a security organization, especially in commerce, I believe you should operate from a position of strength. To do that, your strategy over the next 18 months needs to evolve in three specific ways:

1. **View performance as security:** Your security tools cannot be a bottleneck. Demand that your vendors prove they can maintain performance and protection during peak traffic. Reliability is a requirement, especially when events like Black Friday, Cyber Monday, Singles' Day, or Boxing Day determine if you hit your revenue goals for the year.
2. **Adopt agentic readiness:** Treat every byte of site traffic as suspect. Block malicious bots, serve only legitimate users, and start architecting for agentic commerce. Ensure that your site is discoverable and navigable by AI-driven shopping tools.
3. **Stop lateral movement:** Implement microsegmentation to deny ransomware the ability to move through your network. By containing a breach to an isolated zone, you ensure that a security incident remains a manageable event rather than a headline-grabbing disaster.

The question is no longer whether you are secure. It is whether you are ready to drive growth, customer trust, and competitive advantage in an economy of autonomous agents.

Mani Sundaram
Executive Vice President and General Manager,
Akamai Security Technology Group

Akamai Security

Key insights of the report

Commerce remains the most heavily targeted industry for bot activity, experiencing a 19% year-over-year increase in 2025, with retail accounting for 61%. This momentum is expected to persist.

During 2025, bot activity among commerce organizations increased in each region, growing by 63% in Asia-Pacific (APAC), 48% in Latin America (LATAM), 16% in Europe, the Middle East, and Africa (EMEA), and 7% in North America (N. Amer.), reflecting differences in market maturity, existing bot adoption, and activity within the retail, travel, and hospitality verticals.

Between July 2025 and December 2025, among all verticals in all industries, the retail vertical in N. Amer. had the most AI bot activity at 33 billion AI bot counts (nearly 16% of all AI bot activity), followed closely by retail in EMEA at 26 billion (12.4% of all AI bot activity).

Commerce recorded the highest volume of AI bot traffic between July 2025 and December 2025, accounting for 48% of all activities.

Web attacks on APIs rose by 9% year over year between Q4 2024 and Q4 2025, surpassing attacks on applications, and underscoring attackers' shift toward APIs as preferred initial entry points.

A prominent pro-Iraqi and Iran-aligned hacktivist group has been leveraging a multi-vector approach, combining AI-assisted Mirai-derived Internet of Things (IoT) botnets, browser impersonation, and complex DDoS attacks to target ecommerce APIs.

The retail vertical accounts for 84% of all application-layer DDoS activity in the commerce industry.

The persistent rise of bot traffic in commerce

The commerce industry attracts the highest volume of automated bot traffic. These bots are often focused on trends, pricing, and customer behavior, and they (particularly AI bots) imitate customer interactions through popular categories like online shopping and travel booking. Commerce sites feature vast numbers of unique pages, frequent content updates, and seasonal surges that further draw bot traffic.

We observed an increase of 19% year over year in commerce bot activity in 2025 (Figure 1), and we expect this trend to continue. The retail vertical dominates this activity, accounting for 61% of commerce bot detections over 2025 (Figure 2).

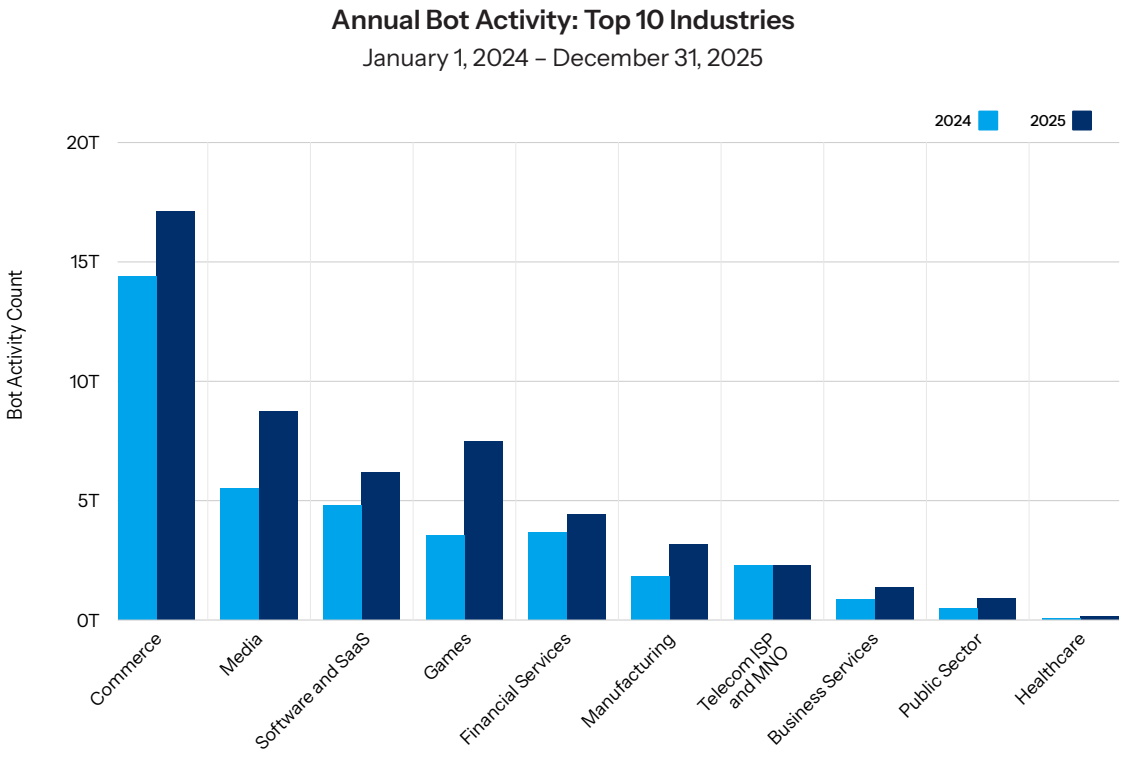


Fig. 1: Commerce remains the most active industry for bots, and that activity continued to increase with a total count of more than 17 trillion for 2025

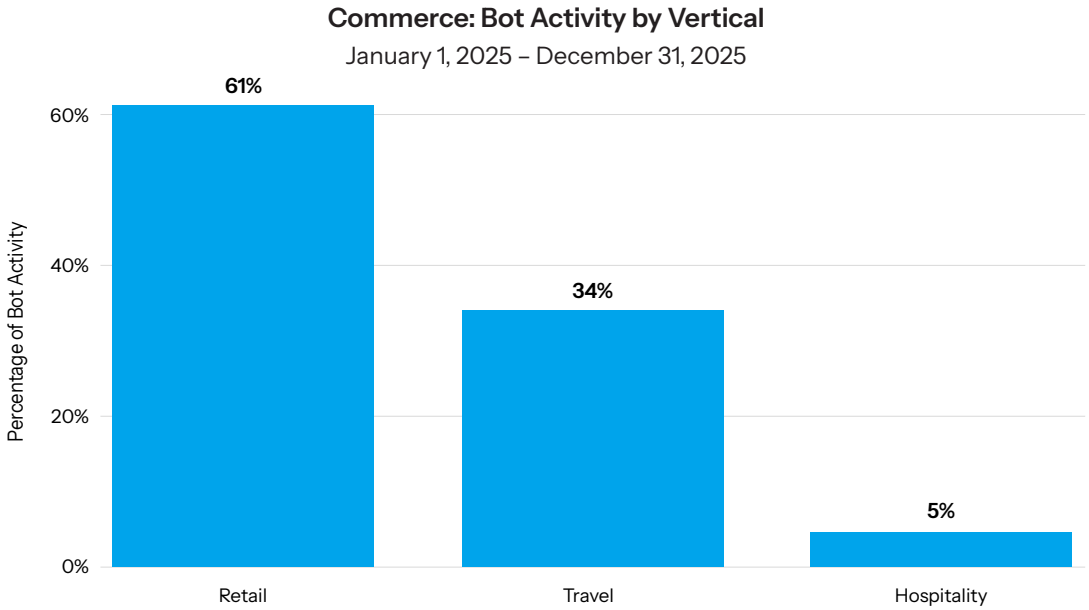


Fig. 2: Retail still leads the other two commerce verticals with 61% of bot activity for 2025

Bots weekend drop-off trend

Analysis of our daily data from July to December 2025 reveals a consistent and significant weekend drop-off trend in bot performance. While this cyclical dip is expected, the precision of the correlation is notable in that almost every dip in activity occurs on either a Saturday or a Sunday (Figure 3). The main exception occurs on Thursday, December 25, which stands out as the most significant decline in the subset, surpassing the typical weekend decline. The data confirms that these bots, while automated, remain tethered to human business cycles. Their activity levels mirror the typical market, tapering off during weekends and some holidays when human oversight is less active.

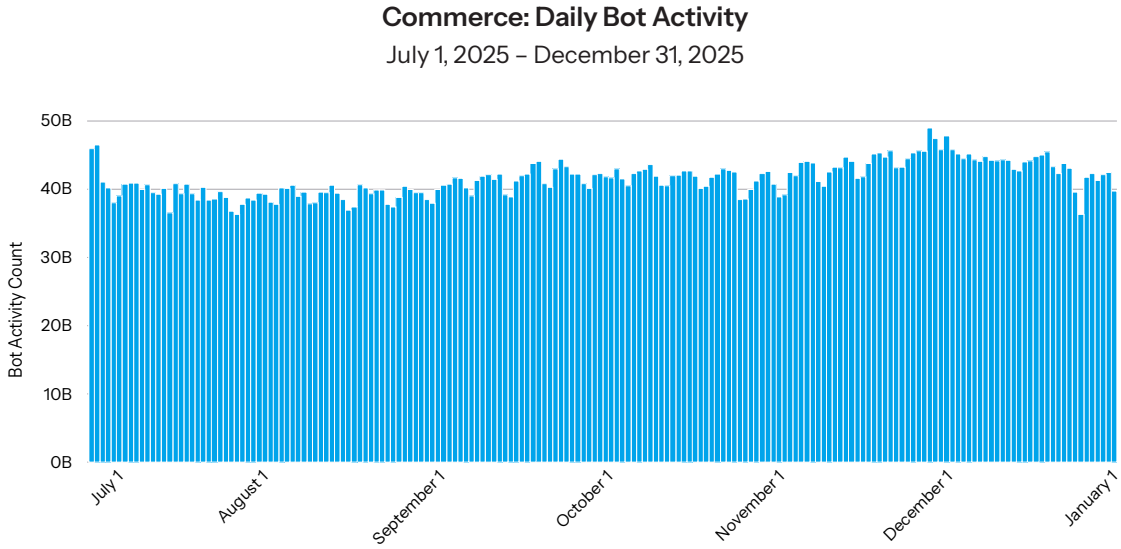


Fig. 3: This six-month subset of data shows that bot activity declines on most Saturdays and Sundays

Impersonation at scale

Online web crawlers play a vital role in commerce by connecting users with fresh and relevant content, helping users discover ecommerce sites and drive potential customers to businesses. Specifically, web search engines surface pertinent results for users by crawling the internet to gather site information. While these search engines rank among the top bot traffic vectors in commerce, a far more prevalent threat dominates our data. Browser impersonators now command a massive share of automated commerce traffic (Figure 4).

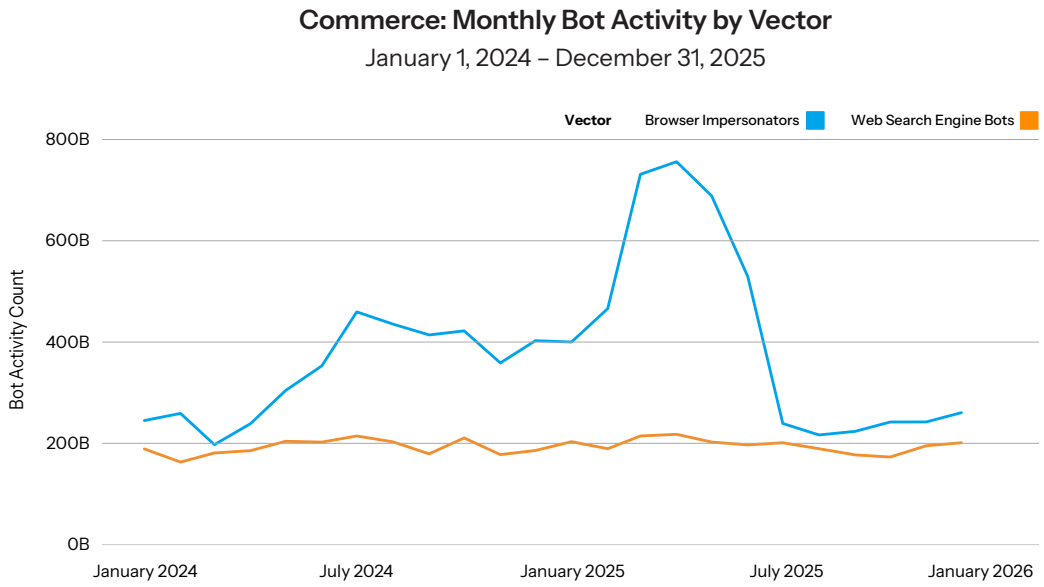


Fig. 4: Browser impersonator activity peaked in April of 2025 reaching more than 750 billion

Browser impersonators are automated bots or scripts that mimic legitimate web browsers to evade detection during scraping. In addition to serving legitimate functions (e.g., testing company privacy protection and web development), browser impersonators may also be used for purely malicious intentions, such as conducting fraud or DDoS attacks. These tools create fake HTTP headers, TLS fingerprints, and client hints that appear as real users on standard operating system web browsers (e.g., Chrome, Firefox, Safari, etc.). Yet, browser impersonators are often detected because many bots fail to fully replicate authentic browser signals (e.g., proper header presence, version formats, and signature consistency).

The surge in web browser impersonator traffic shown in Figure 4 was driven by one large-scale attack in the beginning of 2025 (get more details in the next section on regional trends). Nevertheless, browser impersonation remains a top vector for commerce bot traffic.

Regional trends: Bot activity expanded despite market differences

In 2025, bot activity among commerce organizations increased across all regions, although growth trends varied due to differences in market maturity, existing bot adoption, and activity within verticals. More mature regions such as N. Amer. and EMEA, saw modest increases in activity of 7% and 16%, respectively, while less mature regions experienced faster growth as online commerce expanded, with activity in APAC and LATAM rising 63% and 48%, respectively.

Consistent with the global trend of retail leading travel and hospitality with 61% of all bot activity in 2025, retail also experienced the most bot activity in each region. In N. Amer., bot count in retail reached 4.9 trillion (53% of all bot activity) in the region, followed by EMEA at 2.7 trillion (80%), APAC at 2.1 trillion (58%), and LATAM at 724 billion (82%). However, in N. Amer. and APAC, travel was a close second to retail (Figure 5).

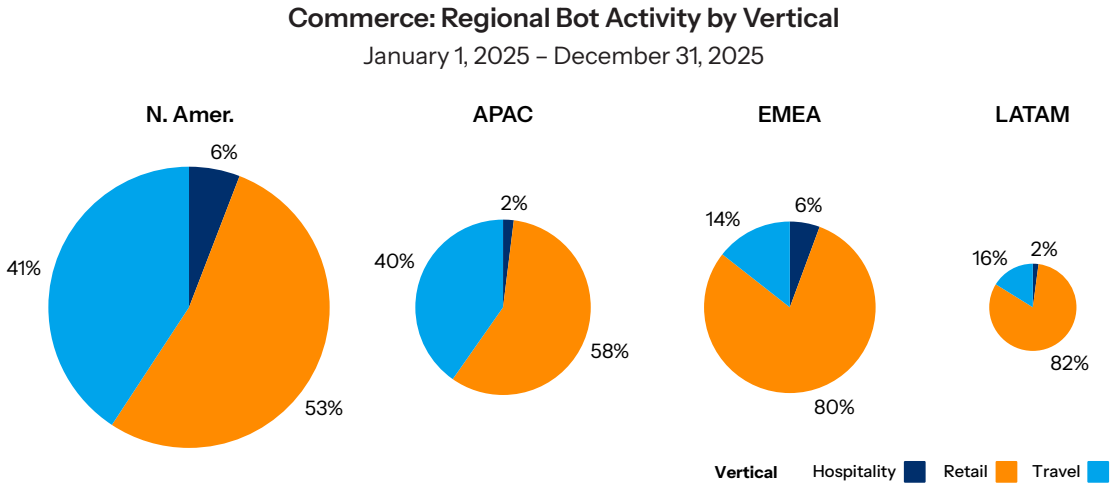


Fig. 5: Retailers experienced the most bot activity in each region, with travel a close second in N. Amer. and APAC

Driven by a customer-first mindset, retailers have been at the forefront of developing chatbots, which makes them an attractive target for potentially malicious bot activity and requires retailers to adjust their traditional business models. In N. Amer. and EMEA, where bot activity is comparatively high, major drops of limited products continued to generate spikes in bot activity for inventory hoarding. However, Akamai experts observed new challenges for retailers, including threat actors using bots that blend in with normal traffic, wait until fast-moving products are released, and then buy-up inventory to resell at a profit. Although this is not a revenue issue for retailers, it causes reputational harm and erodes customer loyalty.

In this environment, retailers must continually evolve their strategies to mitigate risk while embracing bots as a proactive tool to enhance customer experience — for example, by offering memberships that provide customer benefits and hamper opportunistic attacks, and by closely monitoring bot activity to understand the impact and opportunities as they prepare for the broader use of agentic AI.

Although absolute bot counts were lower in LATAM and APAC, Akamai researchers observed significant growth in each region. In LATAM, online retail is developing and gaining momentum at a compound annual growth rate of 20.5%, driven by digital wallet penetration. Meanwhile in APAC, the leading region for online shopping in terms of volume, retailers are already pivoting to agentic commerce in which bots are used to hyperpersonalize the shopping experience and reduce cart abandonment.

Bot impact on travel

In 2025, the travel vertical rivaled retail as a major market for bot activity in APAC and N. Amer. The reasons behind the numbers vary and highlight the double-edged nature of bots: as a tool to drive value to businesses *and* an opportunity for threat actors.

Three years ago, we reported that the travel vertical was a particularly attractive target for web attacks in APAC when compared with other regions. At the time, the region was the fastest-growing market for online travel booking.

We attribute the elevated bot activity in 2025 to a combination of market dynamics, consumer behavior, and seasonality surges. APAC, with the largest share of the online travel market, is also the fastest growing chatbot market, and travel providers in APAC are very fragmented, which results in more platforms and more bot use. Travel loyalty programs are extremely popular in APAC where points have huge monetary value, escalating account takeover and credential stuffing activity. Additionally, travel surges based on seasonal events like Lunar New Year, Golden Week, and Diwali, as well as regional sporting and entertainment events, increase bot activity by various groups of users.

In contrast, in N. Amer., where 41% of bot activity in commerce targeted travel, the surge was due to a large-scale attack attempt against travel companies in the region. The intent was to steal customer credentials across a vast ecosystem of partners by using bots for browser impersonation to enhance and accelerate phishing and fraud.

The high stakes of AI bots in commerce

AI bots are boosting efficiency, increasing conversion rates, lowering customer support costs, and reshaping how commerce organizations engage customers. Shoppers are also shifting away from traditional web search and turning to AI to find products or gift ideas. Adobe reports that generative AI–driven traffic to U.S. retail sites surged by 4,700% year over year from July 2024 through July 2025.

This growing reliance on automation has also made the commerce industry a primary target for AI bot–driven activity. Nearly 50% of AI bot traffic across Akamai's network targeted commerce organizations from July 2025 through December 2025 — more than any other industry globally (Figure 6).

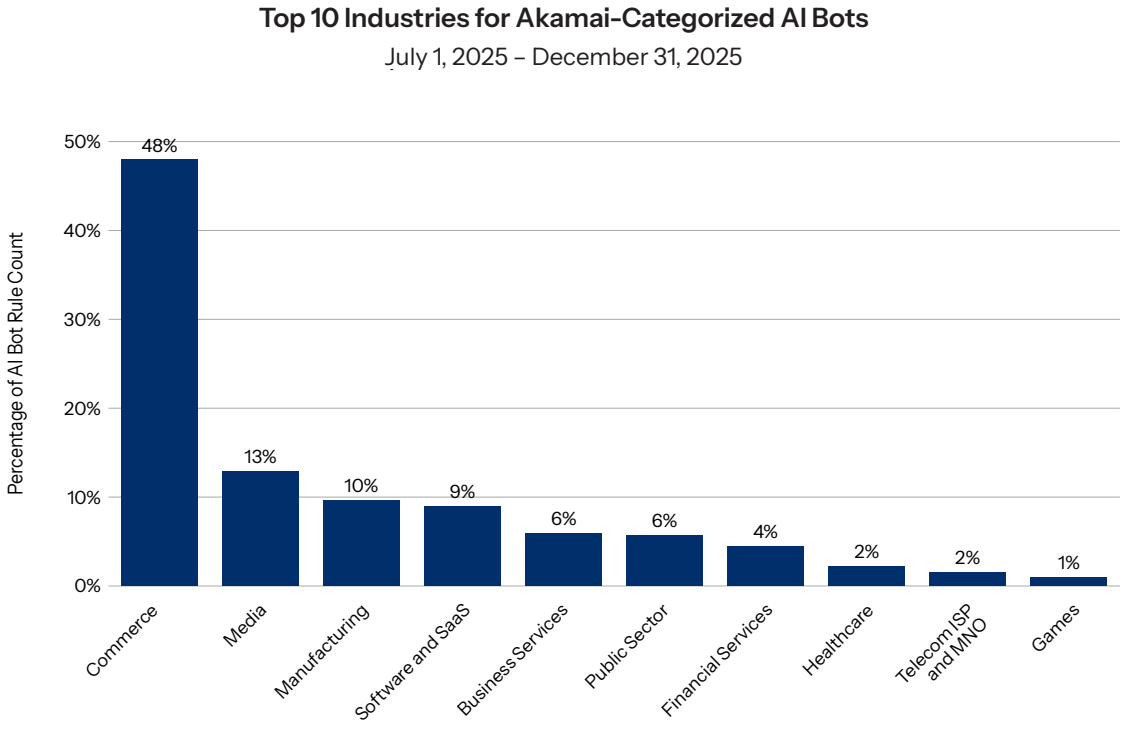


Fig. 6: Commerce has experienced more than three times the volume of Akamai-categorized AI bot triggers as the second-most-targeted industry (media)

Commerce companies prioritize customer experience, often choosing to accept increased risk rather than block legitimate users, which can leave security as a secondary concern. This mindset has accelerated the early adoption of customer-facing technologies like chatbots, but it has also introduced new attack surfaces (see The vulnerable interface: Chatbots, agents, and tokens for detailed coverage of the expanded attack surface).

Akamai-categorized AI bot types

Akamai monitors a vast array of bot types, and AI bots currently account for a small fraction of the total volume across our network. Within this specific subset, we further categorize AI bots based on distinct behavioral patterns: AI training crawlers, AI search crawlers, AI fetchers, and AI agents.

Between July 2025 and December 2025, AI crawlers dominated the commerce landscape, followed by AI fetchers and AI search crawlers (Figure 7).

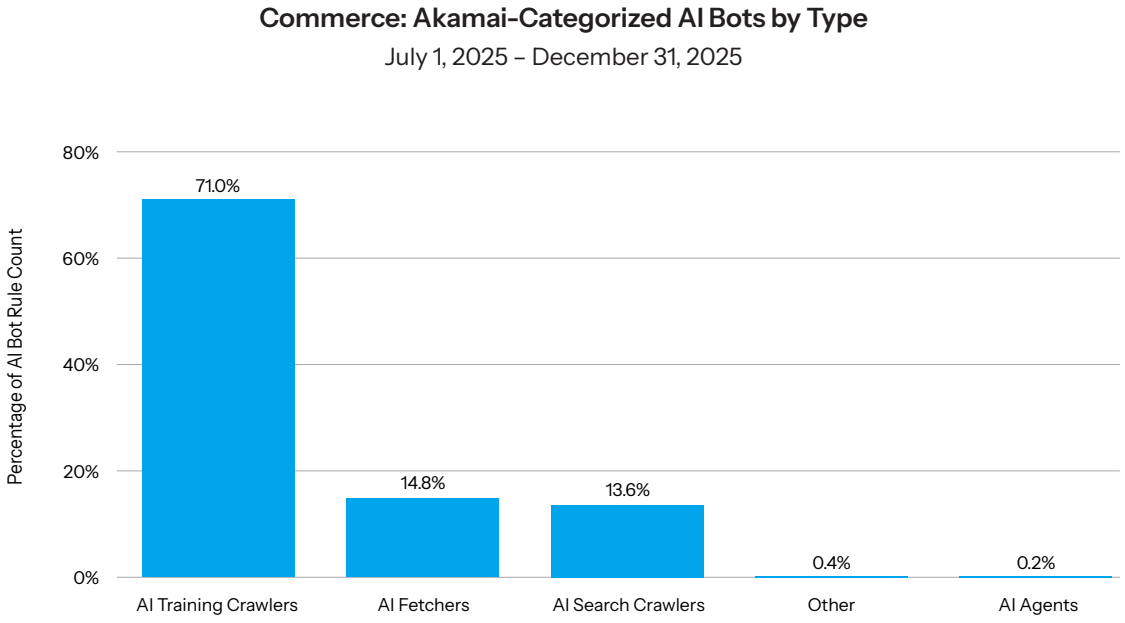


Fig. 7: Training crawlers account for more than 70% of Akamai-categorized AI bot triggers, followed by AI fetchers, and AI search crawlers

Training crawlers that automatically scan and collect large volumes of website data for LLM development often scrape product descriptions, pricing, and other proprietary content. This practice can erode competitive advantage, as rivals may use near real-time data to adjust pricing or monitor inventory. It can also degrade site performance and distort analytics, since distinguishing bot traffic from human users remains difficult.

At the same time, broadly blocking these crawlers carries trade-offs. Reduced access may limit a company's visibility in AI-driven product recommendations and shopping assistants, ultimately reducing digital storefront discovery and brand visibility.

In 2025, OpenAI, ByteDance, Anthropic, Meta, and Perplexity remained the most common AI bots (Figure 8), which is consistent with our previous AI bot research.

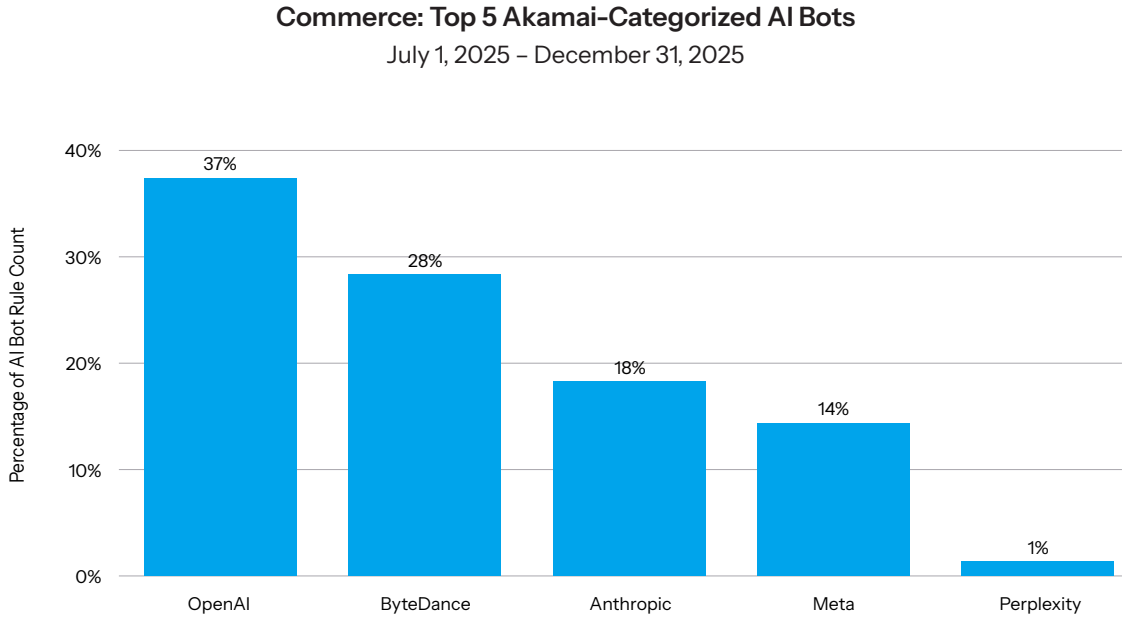


Fig. 8: OpenAI tops the list of specific Akamai-categorized AI bots in commerce, followed by ByteDance and Anthropic

A balancing act

AI bots continue to represent one of the most prolific and unpredictable bot types and as AI bot traffic continues to rise, the traditional "block vs. allow" binary no longer suffices. Organizations need to consider solutions that help mitigate risks without blanket-blocking AI bots, which can cause them to miss out on the potential benefits of those bots.

According to Akamai research data from a six-month period, commerce organizations, like most other industries, placed more than 90% of their Akamai-categorized AI bot activity in the "monitor" category to use more behavior-based assessments on these bots. As shown in Figure 9, commerce organizations allow three-quarters of the *remaining* activity to pass unrestricted, while other industries are more strict. While this permissive approach prevents the accidental blocking of legitimate consumers, it exposes platforms to significant underlying risk, recognizing AI bots as potential revenue drivers, and are actively investing their impact.

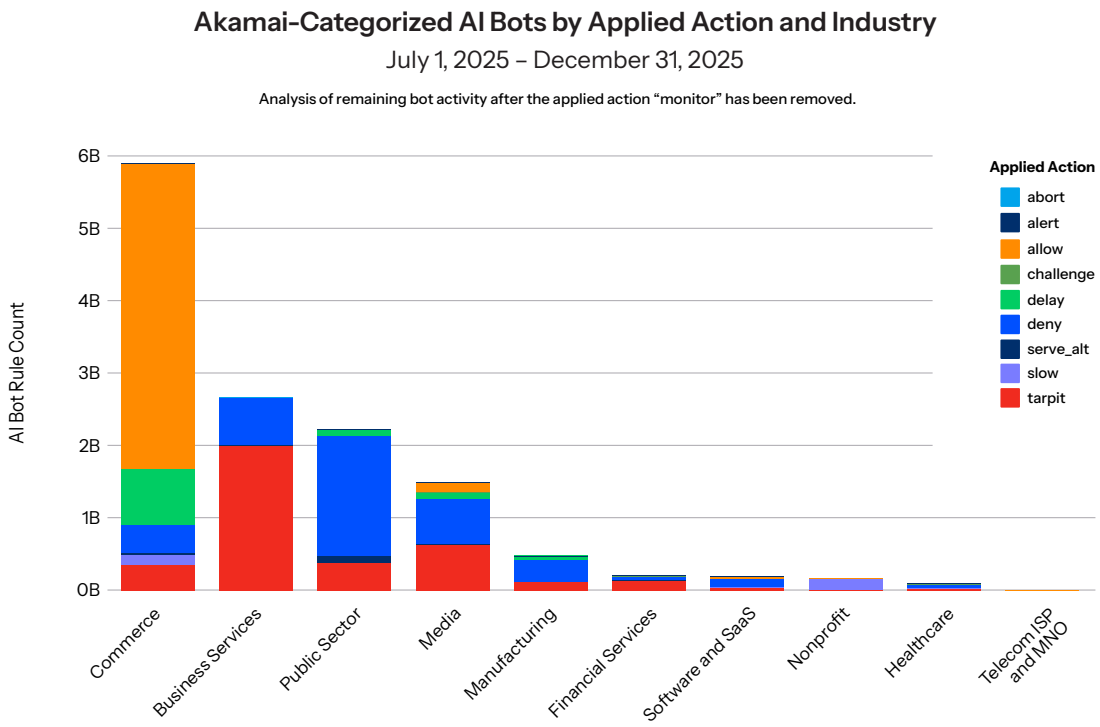


Fig. 9: After monitoring more than 90% of Akamai-categorized AI bot activity, most commerce organizations allow significantly more of the remaining activity to pass unrestricted than do other industries

Organizations are entering largely uncharted territory, and the decisions they make cannot follow a one-size-fits-all playbook. The right approach is often highly individualized; each organization must carefully evaluate which AI bots to allow, restrict, or monitor within their own environment, based on their unique business needs and risk tolerance.

Regional trends: Retailers led AI bot adoption

Within each region, a high level of AI bot activity in commerce compared with other industries reflects how AI bots are trending as a "go-to tool" for customer interaction. Between July 1, 2025, and December 31, 2025, commerce was the top industry for Akamai-categorized AI bot activity in each region, accounting for 54% of AI bot activity in LATAM, 53% in EMEA, 49% in N. Amer., and 38% in APAC.

The regions followed the global trend with respect to AI bots, with OpenAI, ByteDance, Anthropic, Meta, and Perplexity making up the top five in each region (Figure 10).

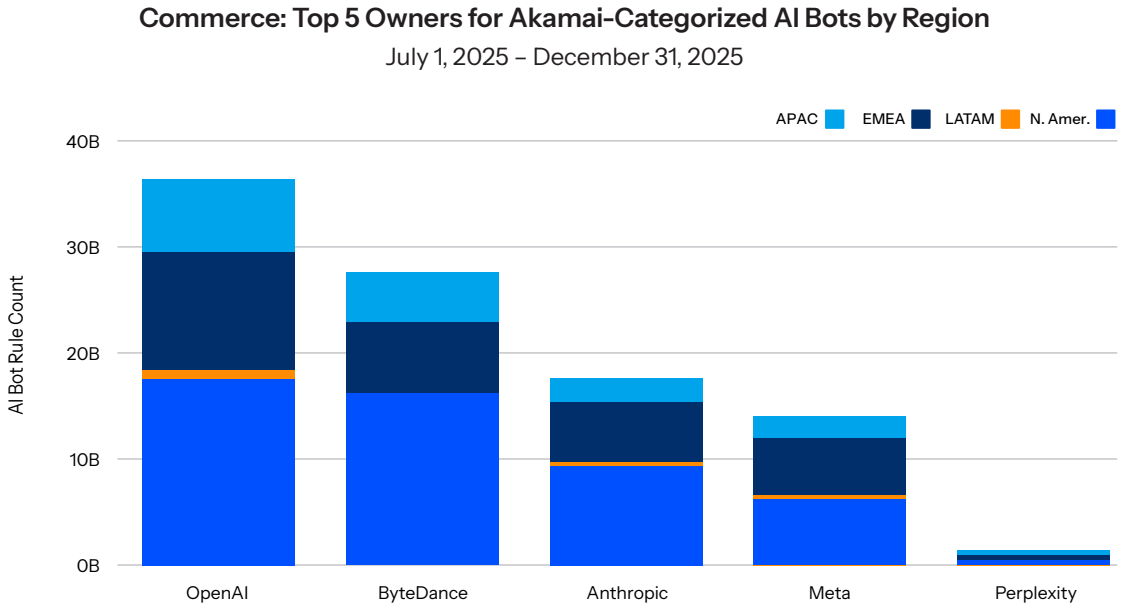


Fig. 10: The top five Akamai-categorized AI bots were consistent across each region

Also consistent with the global trend, AI training crawlers were the most active bot types in each region, with AI fetchers and AI search crawlers in second and third places, reflecting the massive influx of learning, agent/assistant, and scraping activity that commerce organizations experience (Figure 11).

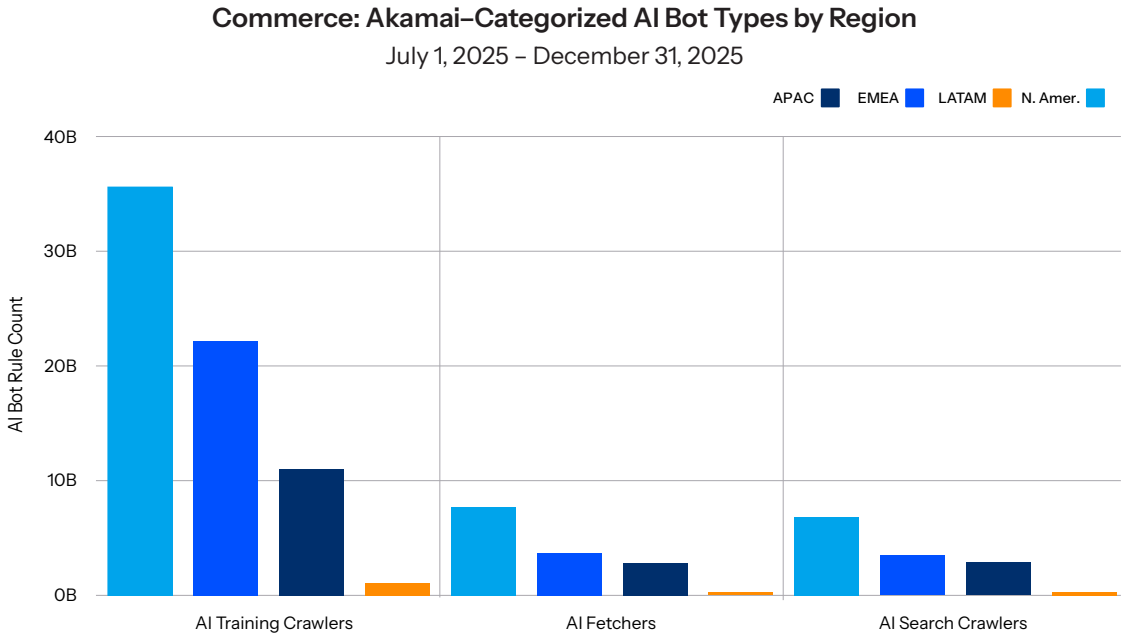


Fig. 11: Akamai-categorized AI bot type activity in commerce is similar across regions

One reason for similar activity across regions is the dual purpose of AI bots to drive value to organizations and to inflict damage, making them a ubiquitous tool for various groups of users.

Further analysis of Akamai-categorized AI bot activity across all verticals in all industries (e.g., media, finance, manufacturing, etc.), revealed that the retail vertical in N. Amer. had the most AI bot activity at 33 billion AI bot counts (nearly 16% of all AI bot counts), followed closely by retail in EMEA at 26 billion (12.4% of all AI bot counts). The travel vertical in N. Amer. ranked third in AI bot counts at 16 billion (7.5%).

The maturity and size of the bot market in these regions directly contribute to their prominence in AI bot activity. As an early adopter of AI, N. Amer. dominates the global chatbot market with a 39% share. And in EMEA, agentic commerce is becoming the shopping tool of choice; nearly two-thirds of consumers use it to inform shopping decisions.

The stage is set for AI bots to evolve beyond product discovery, comparison, and recommendations into fully autonomous shopping agents. As AI bot use advances and proliferates, it becomes easier for illegitimate bots to blend into normal patterns and more difficult for defenders to understand intent and protect their business and customers.

The vulnerable interface: Chatbots, agents, and tokens

Integrating artificial intelligence into commerce platforms has created a broad, complex attack surface. As organizations deploy intelligent interfaces to streamline service and automate workflows, threat actors are aggressively exploiting these systems across three tactical fronts: exploiting AI chatbots, manipulating conversational AI agents, and using AI token freeloading.

Exploiting AI chatbots

Consumer-facing AI chatbots are increasingly targeted by automated logic exploits. Rather than relying on traditional code vulnerabilities, attackers use structured text prompts to bypass safety rails — a tactic known as a "leaky faucet" attack. By methodically manipulating input parameters, threat actors trick these conversational interfaces into overriding business rules.

In commerce, this exploitation yields immediate financial damage. Attackers have successfully coerced retail chatbots into honoring expired promotional codes, authorizing fraudulent returns, and leaking proprietary inventory data. Because these interactions occur within legitimate, encrypted user sessions, standard signature-based security filters frequently fail to detect the malicious intent.

Manipulating conversational AI agents

The threat runs deeper with autonomous AI agents. These back-end models possess significant operational authority, including the ability to independently navigate site architectures, query databases, interact with APIs, and execute complex workflows.

This deep integration introduces systemic risk. Sophisticated threat actors deploy advanced prompt injection techniques and jailbreaks to subvert an agent's underlying instructions. Once compromised, an enterprise agent can be manipulated into executing unauthorized database queries, exposing proprietary pricing models, or overriding purchase limits — effectively turning an organization's own automation into an internal vector for data exfiltration and fraud.

An example of protection against this risk is the recent partnership between Akamai and Visa for identity verification for agentic commerce, which blends Visa's agent protocol with Akamai's bot defenses to secure payments for merchants while preserving trust and control.

Using AI token freeloading

The high economic cost of running LLMs has given rise to a specific form of resource theft: AI token freeloading. Processing natural language queries requires substantial back-end computational power, billed directly through token consumption. Attackers are actively hijacking this infrastructure for their own utility.

Through automated scripts and bot networks, threat actors route their own heavy processing workloads or external model-training queries directly through a retailer's public-facing AI endpoints. By offloading these resource-intensive tasks, attackers force target organizations to absorb massive infrastructure costs while degrading application performance for legitimate consumers.

Hacktivists leverage bots for multi-vector attacks on commerce

A pro-Iraqi and Iran-aligned hacktivist group known as the 313 Team has been operating under the Cyber Islamic Resistance (CIR) umbrella and exemplifies the convergence crisis described in Akamai's SOTI Security report, Apps, APIs, and DDoS 2026: Prepare for the Convergence Crisis: Mitigating API, AI, and DDoS Risks.

Rather than relying on a single proprietary botnet, the group functions as a resource aggregator, leveraging DDoS-for-hire platforms (capable of multi-terabit attacks), shared Mirai-derived IoT botnets, and open source tools coordinated through Telegram networks. Their 2026 operations increasingly favor Layer 7 DDoS for precise, strategic disruption. Although they are usually more focused on Layer 7, their campaigns are sometimes multilayered, blending application-layer attacks with volumetric DDoS (as a smokescreen to distract security and saturate the network). This is often enhanced by browser impersonation techniques, allowing the group to mimic legitimate traffic and evade traditional defenses. This flexible, multi-vector model enables both scale and precision, aligning with broader trends of AI-assisted, coordinated attack strategies.

313 Team recently expanded beyond Saudi Arabian, Israeli, and U.S. government targets into the commerce industry (including the retail and travel verticals), demonstrating a strategic shift toward economic disruption. High-profile attacks against many of these companies highlight the hacktivist group's increasing focus on Layer 7 attacks that target APIs, so they can disrupt critical back-end services like checkout systems or security update mechanisms without fully taking sites offline. This approach allows them to create targeted disruption that produces both immediate revenue loss and the potential for long-term exploitation.

Our recommended mitigation techniques to defend against these attacks are outlined in the Mitigation strategies section.

Commerce continues to face sustained high web attack volume

As threat actors shift seamlessly between automated bot campaigns and direct exploitation of application vulnerabilities, the volume of web attacks targeting commerce platforms shows no sign of decreasing. Organizations across the industry faced relentless attacks on both applications and APIs, with more than 200 billion attacks recorded between 2024 and 2025 — a volume that cemented commerce's position as the most targeted industry during the reporting period (Figure 12).

Top 10 Web Attacks by Industry

January 1, 2024 – December 31, 2025

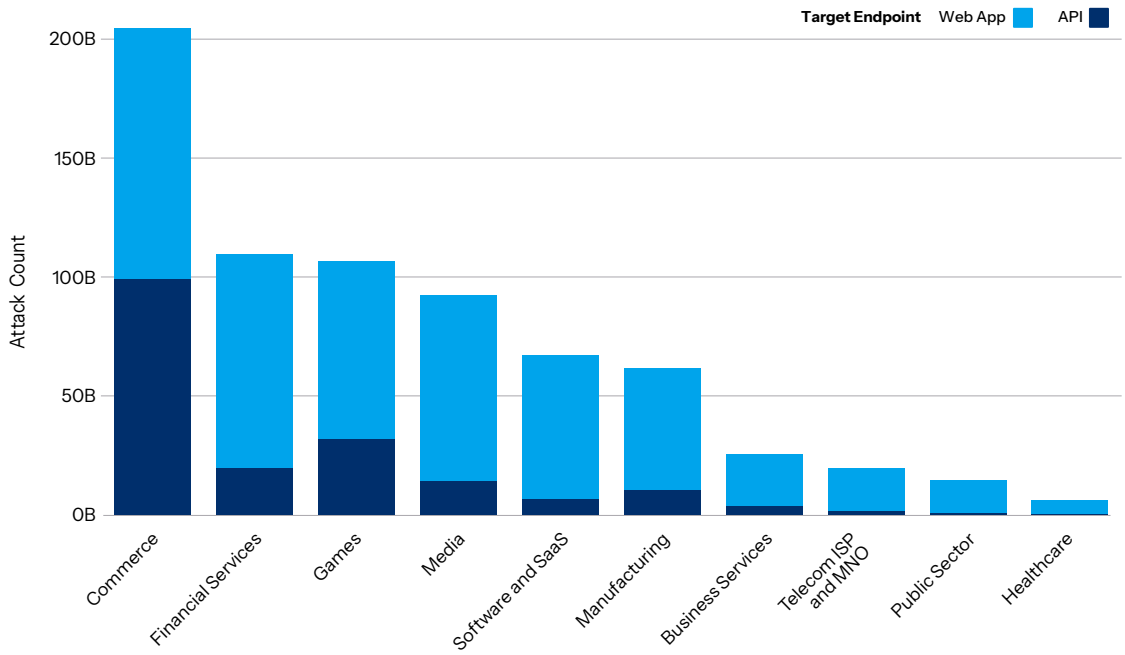


Fig. 12: The commerce industry has consistently recorded the highest number of web attacks across all industries

Between January 2024 and December 2025, the three commerce verticals dominated the top 15 web attack verticals across all industries, with retail leading the rankings, hospitality at number 5, and travel placing 10th overall (Figure 13).

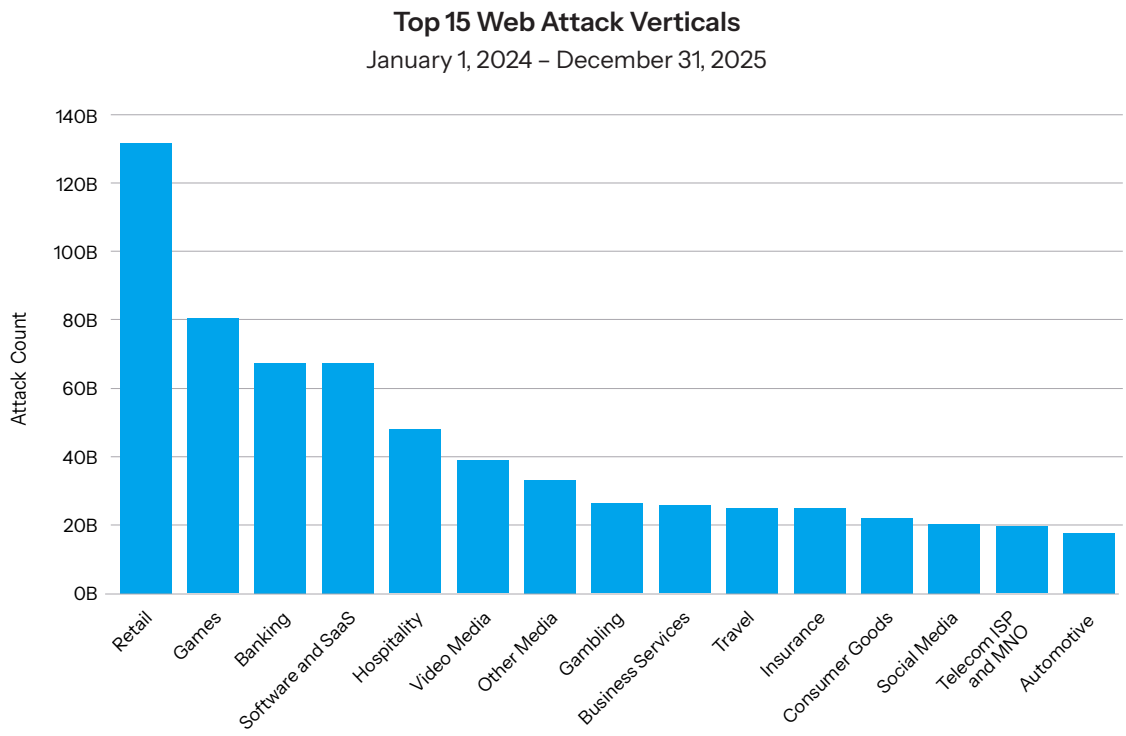


Fig. 13: All commerce verticals (retail, hospitality, and travel) rank in the top 15 web attack targets, highlighting the prevalence of this threat

The commerce industry's higher exposure to web attacks is not surprising. Retailers and ecommerce sites store some of the most profitable data in the threat landscape, such as payment card records, personally identifiable information (PII), and transaction histories that can be peddled on underground marketplaces. A successful breach can yield substantial returns, with stolen datasets fueling everything from card fraud to identity theft campaigns.

Compounding the risk is the industry's inherently complex digital architecture. Modern commerce environments rely heavily on web applications, APIs, and sprawling third-party vendor ecosystems — each integration point represents a potential entry point for threat actors. The result is an attack surface that is broader and more difficult to defend than those found in less interconnected industries.

Notable vulnerabilities

Web attacks remain among the most effective tools in an attacker's arsenal. Ecommerce platforms built on widely adopted technologies like WordPress and WooCommerce are frequent targets because of their open source nature and user base. CVE-2025-0366 and CVE-2025-39391 demonstrate how attackers use well-known web attack methods to compromise ecommerce infrastructure, obtain sensitive data, and gain unauthorized control over servers.

- CVE-2025-0366: A critical local file inclusion (LFI) vulnerability in the Jupiter X Core WordPress plug-in, publicly disclosed in 2025, placing an estimated 90,000 websites at risk. The flaw carries significant implications for the ecommerce sites, given the plug-in's widespread adoption across WooCommerce-powered storefronts. Security researchers found that the vulnerability enables threat actors with contributor-level privileges or higher to upload malicious SVG files and trigger arbitrary PHP code execution. When successfully exploited, the attack chain could grant unauthorized access to sensitive data, which could be detrimental to online retailers handling payment information and customer records.
- CVE-2025-39391: Another crucial LFI vulnerability affecting the Checkout Field Visibility for WooCommerce WordPress plug-in. When successfully exploited, attackers can read sensitive files from the WordPress installation, potentially exposing valuable information such as database credentials, API keys, and other configuration details stored on the server. Additionally, when combined with other attack techniques, it can lead to remote code execution, thus compromising the security of the server.

As attackers increasingly exploit web application vulnerabilities, commerce organizations must adopt web and API protection strategies that reduce the time between zero-day discovery and widespread exploitation to prevent disruptions that can lead to system downtime and significant financial losses.

API attack trends

The rapid integration of global merchants, shippers, social media platforms, and payment systems has fueled API sprawl, significantly expanding the digital attack surface for ecommerce, particularly for retailers.

Although historical data shows a wide gap between application and API-targeted web attacks, that margin is narrowing. For instance, web attacks targeting APIs increased by 9% year over year between Q4 2024 and Q4 2025 (Figure 14). During this period, API-directed attacks exceeded those against traditional web applications, indicating a shift by threat actors toward APIs as initial entry points.

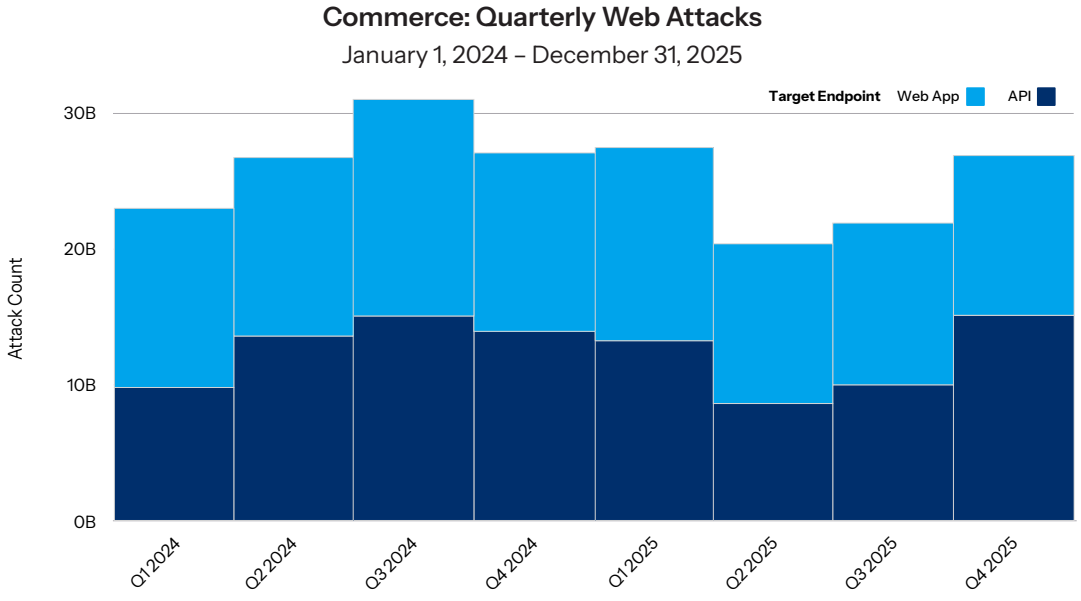


Fig. 14: Web attacks targeting APIs outpaced application attacks, showing 9% year-over-year growth from Q4 2024 through Q4 2025

This shift likely reflects threat actors' growing focus on APIs as primary entry points, given the sensitive data they expose, including PII and financial account information. This trend may be further heightened during the holiday shopping season when transactions (or purchases) and API activities surge.

Additionally, commerce recorded the highest number of web attacks against API endpoints of any industry, with 49% of commerce web attacks between January 2024 through December 2025. Within the commerce industry, retailers accounted for 58% of web attacks against API endpoints, followed by organizations in the hospitality (33%) and travel (9%) verticals.

API security challenges

Consistent with trends across other industries, commerce organizations faced significant API security challenges over the previous 12 months. The 2026 Akamai API Security Impact Study found that 85% of respondents in the commerce industry experienced at least one API-related incident in the past 12 months, underscoring the persistent nature of these attacks.

Some of the key drivers behind these API incidents included API misconfigurations, poor inventory of API estate (e.g., shadow APIs), and lack of additional API solutions on top of WAFs. Moreover, the top three API incidents experienced by the commerce organizations surveyed for the report are exploitation of insufficient access controls, unmanaged APIs, and attacks against APIs related to AI technologies.

The report also reveals critical visibility gaps. Although 77.7% of commerce respondents said they maintain a complete inventory of their API estate, only 22.3% of those 77.7% know which APIs expose sensitive data. This disconnect highlights a growing risk: Unmanaged APIs can become exploitable visibility gaps for attackers.

How API security incidents affect commerce

Successful API attacks can have significant consequences for organizations, including those in the commerce industry, and financial losses are among the most immediate impacts. However, respondents in the same security impact survey also identified longer-term damage such as loss of customer trust, diminished goodwill, and increased account churn as prominent outcomes of API-related incidents.

Addressing these risks requires a dedicated API solution paired with a WAF, giving commerce organizations real-time visibility into and detection of web attacks and behavioral risks.

Regional trends: Business dynamics and peak events shaped web attack patterns

Driving forces in N. Amer. and EMEA

From January 1, 2024, through December 31, 2025, commerce was the most targeted industry by web attacks in N. Amer. (125.8 billion) and EMEA (40 billion). Attacks on these regions drove the global attack trend of deliberately targeting holiday periods and APIs (Figure 15 and Figure 16).

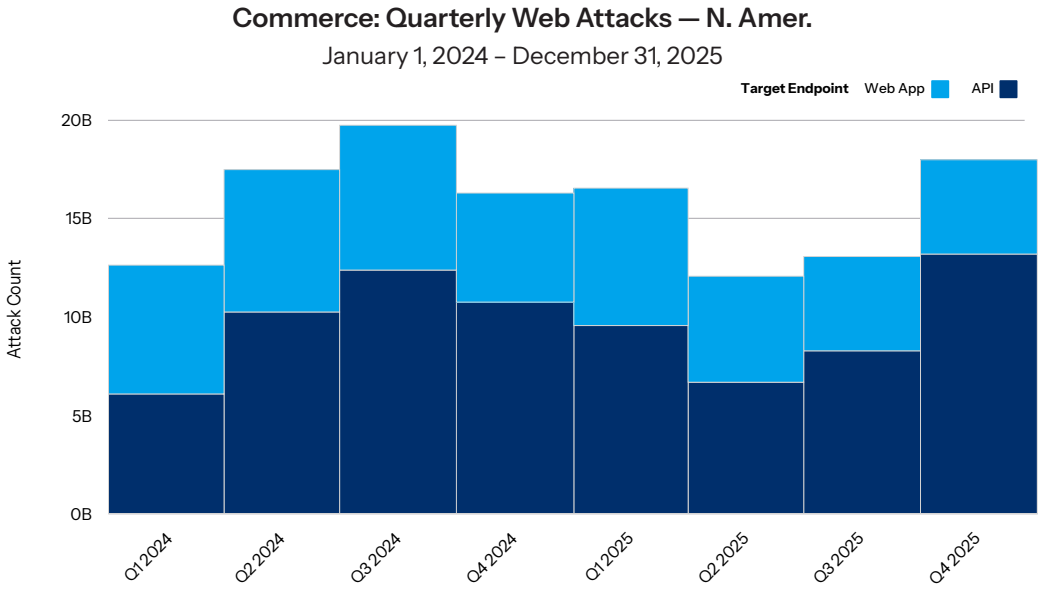


Fig. 15: Attacks during peak holiday windows and against APIs dominated the threat landscape for commerce businesses in N. Amer.

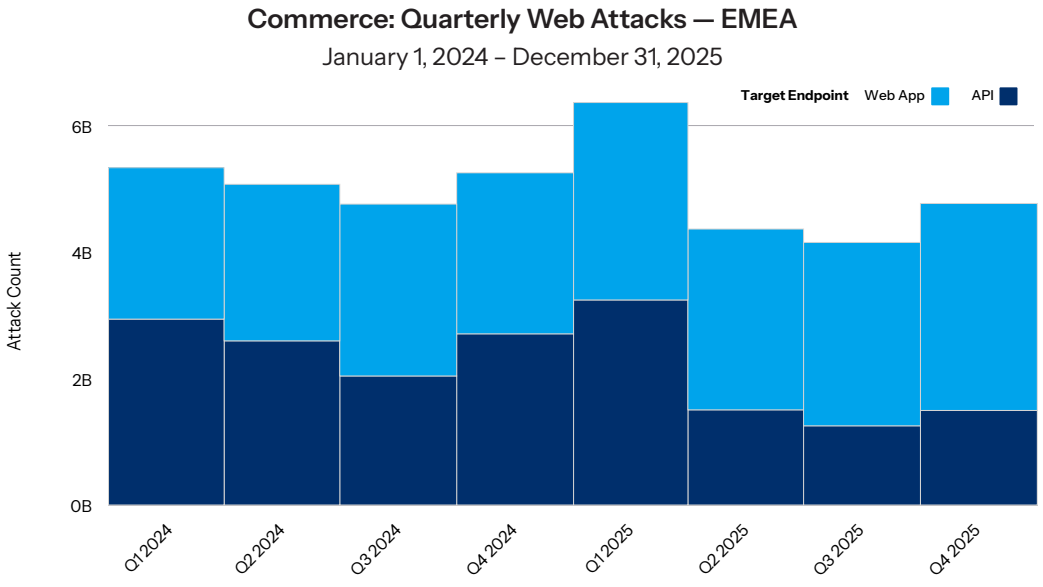


Fig. 16: Holiday periods and APIs were significant targets for web attacks against commerce organizations in EMEA

API-targeted web attacks in N. Amer. exceeded those targeting web applications in every quarter and composed 61% of all web attacks in the region over the two-year period. Although the gap between web app and API attacks was wider in EMEA, API attacks exceeded web application attacks in half the quarters and accounted for 44% of all their web attacks during the reporting period. In both regions, web attack activity increased during holiday periods, but other consumer-driven factors also elevated attack activity.

In N. Amer., consumerism is a driving force in API attack activity. The perceived need for hot ticket items sparked by influencers, general media attention around events, and competitors' actions can have a cascading effect. Any event that captures consumers' attention is an opportunity for cybercriminals to target APIs to get into the revenue stream through inventory hoarding and ticket scalping or to attack customers through fraud and data theft campaigns.

In EMEA, commerce traffic surges in continuous waves — spanning early-year sales and holidays, regional cultural and sporting events, and an end-of-year holiday rush that begins as early as October. Against this backdrop, websites are increasing in size, complexity, and traffic volume, spurring more API development. Meanwhile, commerce models are evolving from a monolithic architecture to a microarchitecture, contributing to API sprawl and shadow APIs and increasing abuse opportunities. According to the 2026 Akamai API Security Impact Study, 84% of commerce respondents in EMEA experienced at least one API-related incident in the past 12 months, with 24% reporting more than five incidents, underscoring the risk from lack of API visibility and hygiene.

Business model differences in APAC and LATAM

In comparison, commerce organizations in APAC and LATAM experienced significantly fewer web attacks targeting APIs, composing 15% and 23% of all their web attacks during the two-year period, respectively. This is primarily due to the prevalence of digital-native retailers that do not require integrations to legacy systems and business models that leverage ecosystem consolidation.

In APAC, the widespread use of super apps such as Grab, Gojek, and Paytm — an app with a marketplace of services and offerings, delivered via in-house technology and through third-party integrations — means most services (e.g., digital finance, food delivery, ride-hailing, and retail) are baked in with fewer integrations (APIs) required. Popular commerce platforms that focus on vertical integration, such as Alibaba, Amazon, and JD.com in APAC, and Mercado Libre, Amazon, and Walmart in LATAM, also reduce the attack surface for retailers.

A vertical view

While retail remains the top targeted vertical in the industry, in N. Amer. 31% of web attacks focused on the hospitality vertical, and, in APAC, travel companies faced 22% of web attacks (Figure 17). Additionally, a whopping 82% of attacks against hospitality in N. Amer. targeted APIs, and a significant 25% of attacks against travel in APAC targeted APIs.

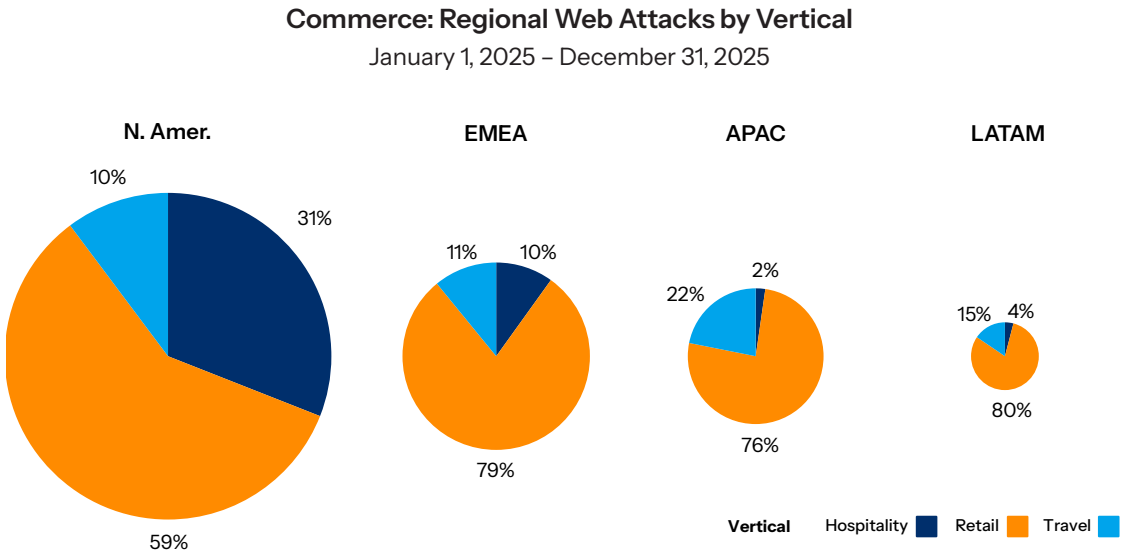


Fig. 17: In addition to retail, in N. Amer. and APAC, the hospitality and travel verticals, respectively, sustained high web attack volumes

Fraud is a huge factor for attacks on hospitality in N. Amer. Gamification of promotions, loyalty abuse, and carding attacks are surging for quick-service restaurants because low-cost transactions can bypass fraud detection. However, sometimes the intent of attacks is more subtle. Akamai researchers observed an attack on an online ordering system aimed at tracking orders that leveraged a programmatic flaw in the API to extract intelligence, likely for competitive purposes.

In APAC, the travel sector is a significant target for web attacks. Major travel peaks usually occur during big holidays like Lunar New Year and seasonal events like year-end holidays when people can get extended time away from work. With some of the highest digital and mobile penetration rates in the world, consumers in APAC are accustomed to reserving and buying travel services online. To capture this market, travel companies have ramped up their digital services and integrations, which in turn has increased the attack surface.

Commerce is the industry most targeted by Layer 7 DDoS attacks

In addition to the rise in bot traffic, web application vulnerabilities, and API exploits, commerce platforms must also withstand a relentless barrage of application-layer (Layer 7) DDoS activity. The commerce sector remains the primary target for these disruptive attacks, with API endpoints accounting for 31% of the total volume (Figure 18).

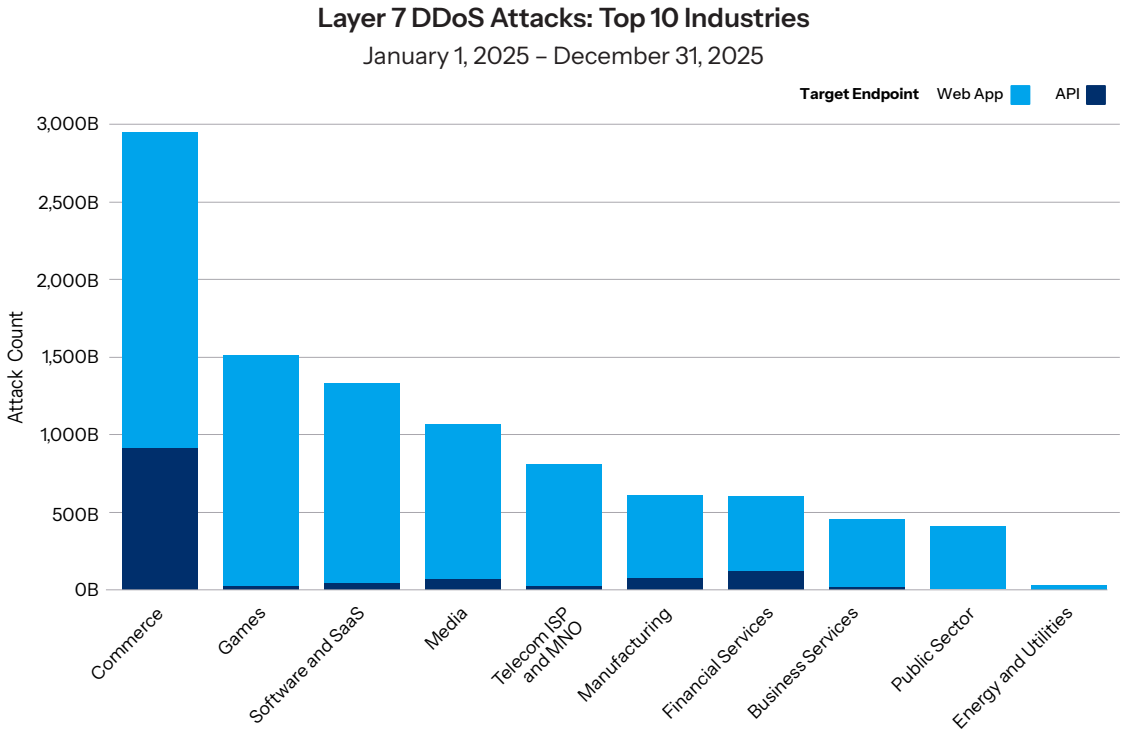


Fig. 18: Commerce was targeted by application layer DDoS attacks almost 3 trillion times in 2025, with 31% of those targeting APIs (Note: An outlier was removed from this figure to accurately represent overall trends)

The retail vertical experienced the largest percentage of these commerce attacks by far (Figure 19).

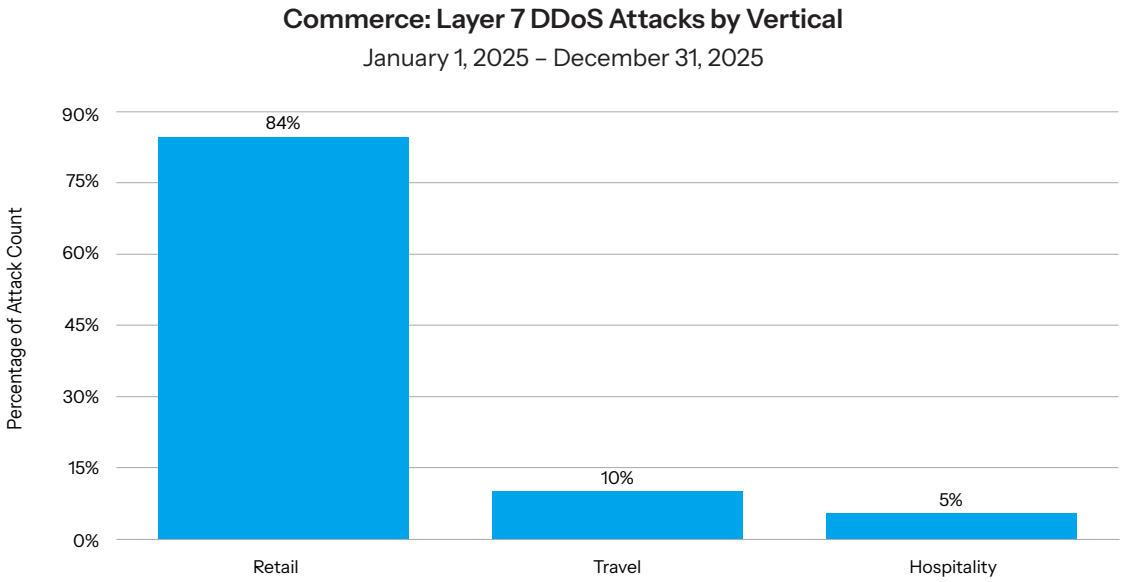


Fig. 19: Retail accounted for 84% of all Layer 7 DDoS attacks on commerce in 2025

Retail companies face elevated DDoS risks due to their massive ecommerce scale and surging financial stakes during peak shopping periods, such as holidays. This includes handling extremely high volumes of traffic, transactions, inventory, and orders while attempting to maintain consistency and efficiency in their operations while keeping expenses in check. Revenue often grows much faster than operational overhead, requiring advanced automation, robust infrastructure (e.g., cloud scaling), and third-party services.

Ecommerce retail outages are frequently caused by Layer 7 DDoS attacks that flood APIs. Attackers often execute this via HTTP botnets that produce seemingly legitimate requests that evade volumetric defenses, blending into real-shopper surges to exhaust app servers and halt sales. These attacks often target well-known brands because of the trust and household recognition tied to their products and services, which enhances disruption impact. Attacks over holiday seasons further deepen the harm, with damages peaking from the U.S. Black Friday shopping day through year-end, as revenue potential soars but is undermined by downtime.

Regional trends: Layer 7 DDoS attacks escalated, focused on APIs

Layer 7 DDoS attacks escalated rapidly across key regions: APAC witnessed a 39% increase — surging from 260 billion to 361 billion events (see Shopping for Weak Spots in APAC) — while N. Amer. experienced a 36% upward trajectory, culminating in 1.89 trillion targeted infrastructure strikes.

As discussed in our Apps, APIs, DDoS 2026 SOTI Security report, Layer 7 DDoS attacks are a primary attack vector, in part because automation, AI, and botnets for hire make these disruptive and costly attacks easier to launch. As such, attack activity against the commerce industry remained relatively consistent throughout the year, with spikes in the fourth quarter correlating to holiday shopping. Seasonality and cultural differences, including bank holidays, festivals, and peak travel periods, contributed to an ebb and flow of attacks in each region (Figure 20). In addition to disrupting the customer experience, application-layer DDoS attacks were also used to abuse APIs and steal customer data and for hacktivist strikes against brands.

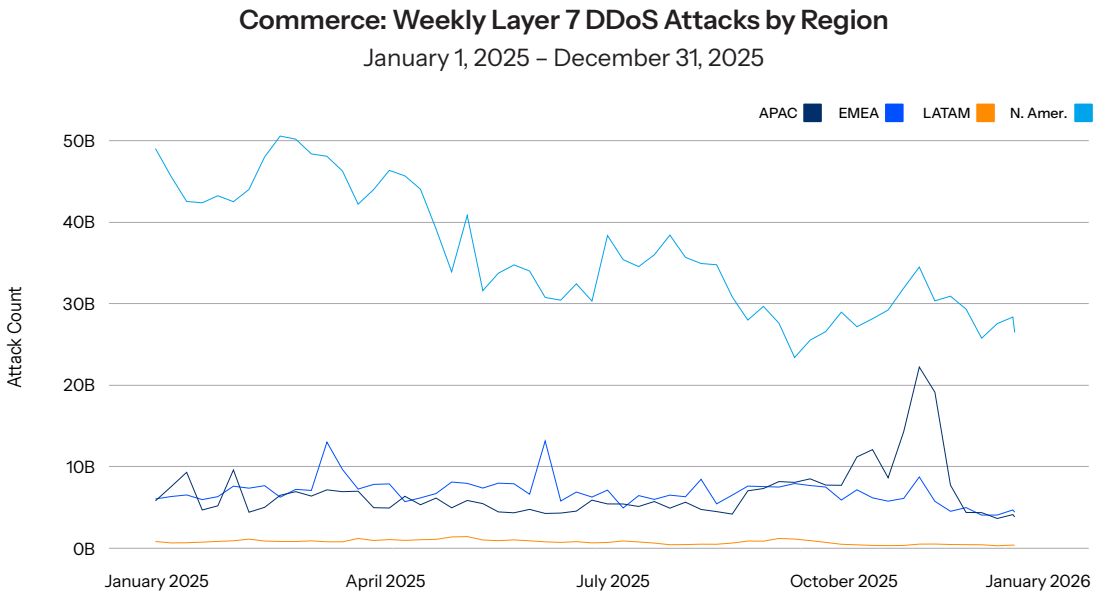


Fig. 20: Layer 7 DDoS attacks peaked in Q4 2025

Across all regions, retailers were the most targeted by Layer 7 DDoS attacks and experienced the largest percentage of Layer 7 DDoS attacks against APIs (Figure 21). In N. Amer., 39% of Layer 7 DDoS attacks against retailers targeted APIs; in EMEA, that number was 34%.

Commerce: Regional Layer 7 DDoS Attacks by Vertical

January 1, 2025 – December 31, 2025

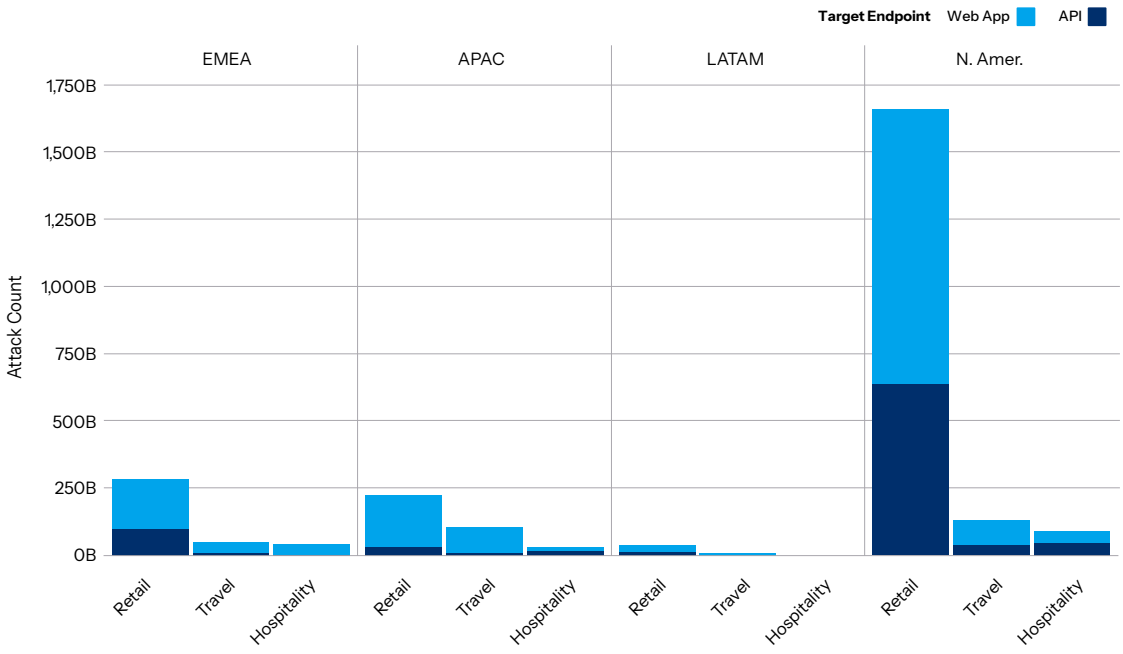


Fig. 21: Across all regions, retailers were the most heavily targeted by Layer 7 DDoS attacks against APIs

Retail operates in a large ecosystem consisting of store fronts, suppliers, merchants, logistics, payment providers, and other partners. These systems are all connected by APIs, which creates API sprawl. Additionally, retail is less restricted than highly regulated industries, such as financial services. In a very competitive market, new technology adoption to elevate the customer experience is high. When combined with the pressure of small margins and tight deadlines, development cycles shrink to remain competitive. As a result, shadow APIs and AI-assisted coding (aka, vibe coding) proliferate, expanding the attack surface and creating a prime opportunity for API abuse.

Given the huge focus on APIs in retail, and the industry's consistent activity throughout the year, attackers' primary motivation is likely financial — the monetization of attacks through stolen payment credentials, compromised customer accounts, and sensitive PII.

Shopping for weak spots in APAC

During 2025, APAC faced a unique situation when it came to Layer 7 DDoS attacks against API endpoints: The distribution among commerce verticals was much more even. Just over half (51%) of API attacks in APAC targeted the retail vertical, 28% targeted hospitality, and 21% targeted travel (Figure 22).

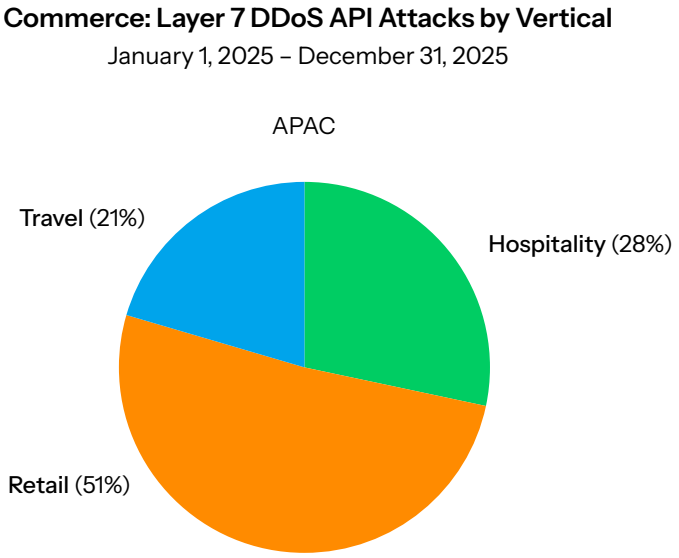


Fig. 22: In 2025, the combined hospitality and travel verticals in APAC experienced nearly half of all API attack attempts

We attribute this trend to various market dynamics and technology factors in the region. Retailers' reliance on super apps and major commerce platforms with built-in services reduces the need for APIs, which makes retailers less attractive targets. Meanwhile, the online purchasing of travel and hospitality in the region is driving a surge in digital services and integrations among a massive and fragmented ecosystem of providers which, in turn, has increased the number of targets for attackers. We discussed these factors in greater depth in the Regional trends: Business dynamics and peak events shaped web attack patterns section of this report.

Akamai Security

Security in depth

How CISOs can prepare for peak event commerce attacks

For modern commerce organizations, major online retail events have evolved from predictable traffic surges into high-stakes operational resilience exercises during which cybersecurity, fraud prevention, and customer experience are tested. Whether it is a major sale with heavy advertising like seasonal clearances, a holiday event like Black Friday or Cyber Monday in the United States, or a cultural event like Singles' Day in China, the combination of infrastructure and security preparation is intense.

For many companies, these events will have a substantial impact on revenue goals, so preparation and collaboration are imperative to success. That means leadership needs to minimize the risk of disruption, so companies have freezes for infrastructure changes that includes security.

This intense operational pressure is further compounded by the fact that fraud and phishing remain the top threats facing the commerce industry during the holiday seasons. According to Bolster AI, during the 2025 holiday season, scammers shifted their phishing and scam tactics from discount-based promotional lures to urgency-driven ones (e.g., fake delivery alerts, package tracking updates, account verification) with higher-value outcomes.

Phishing and scams both grew substantially across the specified lure categories, but scams saw even more significant increases. By optimizing their approach with these urgency tactics, scammers successfully manipulated victims into reacting without hesitation, which ultimately led to much bigger payouts for the attackers.

While companies focus on profit, so do the cybercriminal groups that are innovating at the same pace as retailers. They have evolved from simple stolen credit card shopping to takeovers of both the shopping account and the loyalty reward point accounts. They are no longer just using "bots"; they are leveraging agentic AI and attacks like supply chain poisoning. For example, by poisoning a trusted software library to trigger a malicious prompt injection, attackers can hijack an autonomous AI agent's decision-making power, leading to unauthorized financial transactions and severe operational chaos. This attack innovation requires close integration of cybersecurity and fraud capabilities to keep pace.

Another challenge: Criminals are using fake retail sites and spoofed login portals to harvest customer credentials that are later used in account takeover (ATO) fraud. Detecting these brand impersonation sites is crucial. By continuously monitoring domain registries and using computer vision to detect unauthorized, cloned login portals, organizations can proactively dismantle phishing infrastructure and neutralize credential-harvesting threats before ATO can occur.

Finally, during peak commerce events, large-scale GenAI-driven scraping campaigns must be detected and mitigated as they can overwhelm infrastructure and extract pricing and inventory.

CISOs: Follow the customers' online journey

As CISOs determine what needs to be protected, it is important for them to follow the customers' online journey. Some customers will use traditional web pages, others will buy via an app, and others will make purchases directly through AI platforms. This diversity of experiences requires a number of controls, including WAFs, API security tools, and AI firewalls.

- Infosec teams must have integrated monitoring across all these capabilities; that is, they must have one security platform that is able to rapidly respond to incidents.
- Companies also need DDoS protection across applications (Layer 7), infrastructure (Layers 3 and 4), and Domain Name System (DNS).
- Finally, companies need to fortify the back-end systems with monitoring and segmentation. This will minimize any threats that get into the enterprise and will keep attacks like ransomware or data breaches from creating a major crisis.

Microservices and mobile-first experiences are critical today — and, consequently, APIs are the new storefront. Because of this, companies must be able to address attacks like the leaky faucet attacks that bypass traditional rate limiting to scrape inventory or leak customer data.

Additionally, security teams must be able to classify automation into categories in order to conduct analysis of the trends across their environment. These categories may include:

- Search crawlers
- Carding tools
- Accessibility tools
- AI shopping agents
- Partner integrations
- Scrapers
- Scalpers
- Credential stuffing tools
- Fraud bots
- DDoS botnets

The customer experience environment has become so complex that security teams are moving from asking “How do we stop bots?” to “How do we govern automation?” This means that security must have optimized capabilities before the freeze. Teams must validate configurations and best practices, test surge traffic peaks, and run discovery exercises for new technical and organizational capabilities. Additionally, they must test third-party integrations like DDoS protection and review the crisis management plan with key stakeholders.

To accomplish all of these tasks, CISOs must identify mission-critical customer functions like:

- APIs
- Third parties
- The checkout path
- Mobile paths
- Loyalty flows
- Promotion engines
- Inventory lookups
- Third-party payment processors

Next, security teams need to treat peak commerce events as an operational discipline rather than a last-minute security exercise. The following checklist will help ensure the fundamentals are in place.

Map the revenue chain (visibility and governance)

- ☐ Identify “crown jewel” systems and APIs (including loyalty and gift card flows)
- ☐ Review third-party software as a service (SaaS) mapping (to prevent Magecart-style supply chain attacks)
- ☐ Identify “shadow AI” tools (AI tools leveraged by internal employees without approval or oversight) and establish agentic policy (frameworks that define the decision-making boundaries, permissions, and goals for autonomous AI agents)

Classify and govern automation (the bot strategy)

- ☐ Stress test scraper defenses
- ☐ Test credential exposure monitoring
- ☐ Ensure bot mitigation is tuned against credential stuffing, scraping, and inventory abuse
- ☐ Review AI-powered commerce services and APIs for abuse and data leak risks

Minimize the blast radius (resilience and segmentation)

- ☐ Verify that microsegmentation protects all customer data touchpoints (e.g., systems and apps)
- ☐ Enable risk-based multi-factor authentication for high-value actions
- ☐ Conduct DDoS drills for Layers 3 and 4, Layer 7, and DNS

Establish operational discipline (the human element)

- ☐ Establish freeze exception protocol and escalation paths
- ☐ Validate crisis communication tree

Drive executive alignment (the boardroom)

- ☐ Define "tolerable fraud" goals and security metrics
- ☐ Pre-authorize emergency actions for specific threat activities

Finally, being ready for peak commerce events isn't about surviving the surge in attacks; it's about controlling the edge. This means readiness must be framed around business outcomes. Organizations that perform best are not simply blocking attacks faster — they are building commerce environments that can absorb disruption, govern trusted automation, contain fraud, and maintain customer confidence even under sustained pressure.

For CISOs, readiness is now a business continuity strategy tied directly to revenue protection, brand trust, and digital resilience.

Deep dive on malware

Commerce threats focus on monetization

Akamai is a Common Vulnerabilities and Exposures Numbering Authority (CNA) that sees and tracks established and emerging malware. Two areas of malware that impact commerce are phishing and account takeover (ATO).

According to threat events observed in our commerce customer traffic, commerce organizations are facing a focused criminal threat on monetization through credential theft, ATO, fraud enablement, and persistent access. Malware remained the dominant threat category during the reporting period of November 2025 to April 2026. Malware represented 56.5% of observed activity, phishing accounted for 37.6%, and command and control (C2) communication represented 5.9% of total activity during the reporting period (Figure 23).

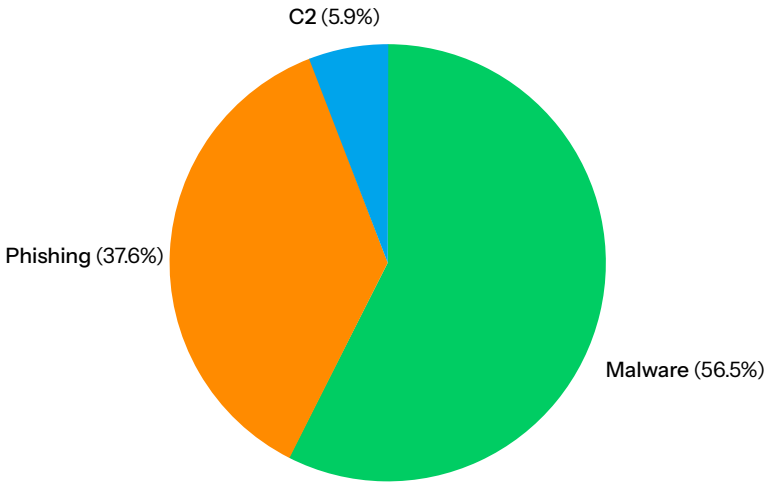


Fig. 23: Between November 2025 and April 2026 malware was the dominant threat category, followed by phishing and C2.

Phishing activity saw spikes in March and April, indicating large-scale credential harvesting campaigns. The persistent C2 communication suggests ongoing postexecution attacker activity within a subset of environments. The overall threat activity was operationally structured and campaign driven, unlike the past unmanaged or isolated attack patterns. Data further suggests that credential theft is not simply one attack objective — it is the operational center of modern commerce attack campaigns.

The dominant tools used within malware were execution activity loaders and postdelivery tools. Within phishing, the dominant tool was user-targeted compromises at scale, specifically engineered for credential theft. Unlike some of the findings from our SOTI about the financial industry, which showed politically motivated attack campaigns, commerce-focused attacks were primarily aligned with monetization objectives, including fraud, identity theft, and ATO.

The two malware threats facing commerce

There are two different malware threats facing commerce. The first is cryptojacking, which dominated the named malware family set and accounted for 65.7% of the observed malware family activity. This attack impacts infrastructure resources and could degrade performance and increase costs. While cryptojacking primarily targets infrastructure resources and operational capacity rather than customer identities directly, large-scale abuse can still affect service performance, operational costs, and customer experience. Consequently, it is not a direct threat to brand and customer trust but it's still worth tracking because of its possible impact.

The second threat that commerce organizations are consistently facing are access-enabling malware families, such as GoatRAT, MysterySnail RAT, AsyncRAT, and Sality, which create more direct business risk by enabling credential theft, unauthorized account access, and compromise scenarios that can impact customer trust and brand reputation. These threats indicate that the malware layer is driven primarily by opportunistic resource abuse, with a smaller but still important set of access-enabling and phishing-linked tools. The observed activity relies heavily on commodity and reusable tooling rather than on custom or highly sophisticated frameworks.

Some specific tools and techniques that the access-enabling malware families are using include:

- Phishing-enablement infrastructure, such as Gophish (an open source multi-tool)
- Botnet and commodity C2 infrastructure (used by Necurs and EvilGnome malware)
- RAT-based access tooling (used by GoatRAT and AsyncRAT)
- Opportunistic abuse patterns

Although the number of phishing attacks is lower than the number of malware attacks, phishing serves as the primary user-targeted attack vector, acting as the main entry point for user-focused compromise. In commerce environments, this directly translates into fraud, transaction abuse, and account compromise at scale.

These phishing attacks include:

- The targeting of widely used platforms (financial and high tech services)
- Credential theft and account access as primary objectives
- The repeated use of phishing infrastructure across campaigns

The timeline shows a clear increase in phishing activity toward the end of the observed period. Average daily phishing volume observed across our commerce customers increased from approximately 56,600 in February to 121,500 in March and 134,600 in April, indicating a strong shift toward large-scale credential harvesting campaigns. This increase suggests sustained credential harvesting campaigns targeting widely used platforms and identity ecosystems.

These campaigns require companies to closely monitor for fake sites as part of their brand protection strategy. These surges of sustained credential harvesting activity can increase operational strain across fraud teams, customer support operations, and incident-response functions. It is clear that credential theft has become the raw material that's powering the commerce fraud economy.

Cybercriminals' growing focus on network persistence

The methodology that attackers are using is an abbreviated version of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. Initial access is primarily driven by phishing campaigns and user interaction, including fake update prompts and malicious content delivery. Execution is typically achieved through lightweight loaders and script-based mechanisms, enabling rapid payload initiation without reliance on complex vulnerabilities. Malware programs, such as AsyncRAT and GoatRAT, function primarily as access enablers by establishing initial footholds and enabling further activity.

Following execution, C2 infrastructure (e.g., such as Necurs, EvilGnome, MyloBot, and QSnatch) indicates continued outbound communication with attacker-controlled or malicious infrastructure providing persistence.

The combination of phishing, loaders, and RAT-based tooling suggests that commerce attacks are evolving into repeatable operational workflows built around credential compromise and persistence.

Phishing → execution → loader → C2 → persistence

Threat trends reflect a layered attack model in which social engineering through phishing enables initial access, malware supports execution and access establishment, and C2 infrastructure then sustains attacker operations. The observed trends also align with recent changes in the MITRE ATT&CK framework, which increasingly emphasizes stealth, persistence, and defense impairment as distinct operational objectives. The recent release of version 19.1 went from 14 to 15 tactics by splitting "defense evasion" into "stealth" and "impair defenses."

These changes reflect the cybercriminals' goal of long-term access. This change should help SOC teams and threat hunters better analyze these techniques. Additionally, the focus on persistence demonstrates that commerce organizations should increasingly focus on Zero Trust and postcompromise detection, like segmentation, rather than relying solely on perimeter defenses.

Current trends suggest that future commerce campaigns may increasingly emphasize operational scale, automation, and persistence across customer identity ecosystems rather than relying solely on more sophisticated malware techniques.

Mitigation strategies

As commerce transitions from traditional digital transactions to an environment increasingly dominated by agentic commerce, the "block vs. allow" binary security policy we've analyzed is not going to continue to work. Security leaders must recognize that blanket-blocking automated traffic may render their digital storefronts invisible to legitimate AI-driven product discovery, search engines, and shopping assistants. Cyber leadership should consider implementing a risk-based automation governance framework that categorizes bots based on intent, behavioral telemetry, and business value. This includes deploying edge native security capabilities that can differentiate between API abuse, data-scraping competitors, resource-draining AI training crawlers, and revenue-generating shopping agents.

Success starts with visibility. APIs have become the fabric of modern commerce, linking payment systems, loyalty programs, AI models, and back-end logistic systems. The 2026 Akamai API Security Impact Study found that only 22% of organizations know which of their APIs expose sensitive data. Security leaders should treat APIs as their digital storefront, prioritize continuous discovery, and close the gap on understanding which systems carry the most risk. The reality is simple: Organizations cannot secure what they aren't aware of.

Commerce organizations should embed security throughout the entire API and software development lifecycle and prioritize protection before production. From testing to documentation and implementation, oversight and accountability are critical as a single weakness can ripple across interconnected systems.

Equally critical is safeguarding the consumer experience, ensuring that security measures reinforce market trust and brand value. Credential theft and account takeover have also evolved into industrialized business operations for cybercriminals. Phishing campaigns, fake storefronts, browser impersonation, and Magecart injections are no longer isolated threats. Security teams should assume that credentials will eventually be exposed somewhere in the ecosystem and should focus on limiting operational impact. When attackers compromise loyalty accounts, payment systems, or customer sessions, they are ultimately diminishing brand confidence.

During major sales events, Layer 7 DDoS attacks, malicious bots, and API abuse are increasingly being used to create operational disruption — and these are the times when organizations can least afford downtime. Before major shopping events, cyber leaders should validate surge capacity (for both security monitoring and customer experience), rehearse crises operational plans, test integrated DDoS response processes, and ensure that edge protections can distinguish legitimate AI-driven commerce activity from automated abuse.

Hacktivists' flexible, multi-vector model enables both scale and precision. This mirrors a larger trend toward coordinated, AI-driven cyberthreats. Our recommended mitigation techniques to defend against hacktivists that leverage bots for multi-vector attacks on commerce include:

- Edge rate control and IP reputation for baseline protection from high distribution
- Edge caching whenever possible, even with short time-to-live values
- Operation runbook with crisis management protocols to ensure efficient and effective engagement of emergency actions

Finally, when security tools fail we need to minimize impacts. Although the Akamai Segmentation Impact Study notes that 92% of organizations apply basic network segmentation, only 35% have progressed to true microsegmentation. Addressing this maturity gap ensures that even if an attacker steals valid authentication tokens, their lateral reach is nullified. Safeguarding the digital storefront requires an operational discipline that frames seasonal traffic spikes as business continuity rather than incident response.

Akamai Security

Conclusion

The insights in this SOTI Security report establish an undeniable reality: The traits that drive the vitality of commerce — unrestricted public accessibility, rich transactional data, and a commitment to frictionless consumer experiences — are the precise features exploited by the modern threat landscape. Across every aspect of the threat landscape, including advanced bot automation, malicious web application exploits, vulnerable API interfaces, and volumetric Layer 7 DDoS assaults, commerce stands as the global epicenter of digital risk. This hostile pressure is no longer a seasonal operational hurdle; it is a permanent cost of doing business in a hyperconnected marketplace.

What we are witnessing is not a failure of security architecture, but the natural maturation of a highly automated ecosystem. The commerce landscape has transformed rapidly since 2023. Phishing has scaled into industrialized pipelines that feed automated account takeover ecosystems. API traffic has evolved into both the primary vector for brand innovation and the most heavily targeted conduit for data exfiltration. Simultaneously, the deployment of intelligent interfaces — consumer-facing chatbots to agentic storefronts — has redefined the attack surface, creating new vulnerabilities.

This is the core friction paradox of agentic commerce. The same open, frictionless architecture that welcomes autonomous AI shopping assistants and hyperpersonalized customer journeys demand an adaptive, comprehensive posture. Security must be ready to evolve to protect both infrastructure stability and long-term brand value and trust.

Ultimately, navigating this environment will require continued leadership and forward thinking from commerce organizations. True operational resilience hinges on situational awareness, integrated threat intelligence, and proactive governance. The mandate for cyber leadership is not to restrict digital growth in the name of safety, but to build a foundation resilient enough to enable continuous business execution. The autonomous economy is not the future state; it's our current everyday life online. The commerce organizations that will thrive are those that shift the question away from "Are we secure?" and instead ask "Are we ready for the year-long shopping season?"

Methodology

Web application and Layer 7 DDoS attacks and bot requests

This data describes application-layer alerts on traffic seen through our web application firewall (WAF) and bot management tool. Both tools monitor requests to protected websites, applications, and APIs. The web application attack alert is triggered when Akamai detects a malicious payload within a request. The Layer 7 DDoS alert is triggered when we detect volumetric anomalies in the number of requests. The bot alert is triggered when we detect any bot payload within a request. These alerts do not indicate the successfulness of an attack. Although these products allow for a high level of customization, the data analyzed here does not consider custom configurations of the protected properties.

The data was drawn from an internal tool for analysis of security events detected on Akamai Cloud, a network of approximately 340,000 servers in more than 4,000 locations on nearly 1,300 networks in 130+ countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

This data covered the 24-month period from January 1, 2024, through December 31, 2025.

Guest contributors

Mani Sundaram
Executive Vice President and General Manager, Akamai Security Technology Group

As General Manager, Mani oversees strategy and product direction for Akamai's security solutions and is responsible for the business unit's core functions of engineering, product development, and product management. In this role, he also oversees Akamai's internal Information Security organization. He is based at the company's global headquarters in Cambridge, Massachusetts.

Mani is responsible for guiding Akamai's next phase of innovation and growth in security, driving Akamai's position as the market leader in DDoS prevention, web application and API protection, and bot management, as well as generating additional growth through new solutions in Zero Trust Network Access, multi-factor authentication, secure web gateway, and Zero Trust segmentation. Through his many roles at Akamai, Mani has built a depth and breadth of technical knowledge and a unique understanding of our customers' needs within the fast-growing security landscape.

Pam Lindemoen
Chief Security Officer and Vice President, Strategy, RH-ISAC

Pam Lindemoen is the Chief Security Officer and Vice President of Strategy at RH-ISAC, where she leads security operations, strategy, and partner engagement. With 30 years of experience in cybersecurity, Pam has held key roles at Cisco as a CISO Advisor and at Anthem (Elevance Health) as a Deputy CISO, helping build global risk management and leadership programs.

Gal Kochner
Senior Data Analyst, Akamai

Gal Kochner is a Senior Cyber Analyst at Akamai specializing in threat intelligence, cyberthreat analysis, and internet-scale security research. She develops intelligence enrichment and threat analysis capabilities that improve threat visibility and help protect customers against the evolving cyberthreat landscape.

Steve Winterfeld
Advisory Chief Information Security Officer

Steve Winterfeld is Akamai's Advisory CISO. He has a strong background in building operational security programs that are compliant with industry regulations. Before joining the team, he served as CISO for Nordstrom Bank, Managing Director of Incident Response and Threat Intelligence at Charles Schwab, and Senior Technical Director Cybersecurity & Group CTO at Northrop Grumman. Before working in the commercial sector, he was an Airborne Ranger in the United States Army and built out the first regional emergency response center (today called security operations centers) for Southern Command.

Steve focuses on collaborating with Akamai's customers to enable them to be successful in defending themselves and their customers. He also helps determine where Akamai should be focusing its security platform's capabilities. Steve has published a book on cyber warfare and holds CISSP, ITIL, and PMP certifications.

Credits

Research director

Kimberly Gomez

Writing and editing

Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Review and subject matter contribution

Gal Kochner
Reuben Koh
Tony Lauro
Pam Lindemoen
Samy Makki
Richard Meeus
Jan Roemer
Mani Sundaram
Steve Winterfeld

Data analysis

Chelsea Tuttle

Promotional materials

Ellen O'Brien

Marketing and publishing

Georgina Morales Hampe
Kimberly Gomez

State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports.

Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research.

Akamai security research

Read the Akamai security research blog for a rapid response perspective on today's most important research.

Access data from this report

View high-quality versions of the graphs and charts shown in this report. These images are free to use and reference, provided that Akamai is duly credited as a source and the Akamai logo is retained.

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, and LinkedIn. Published 07/26.