

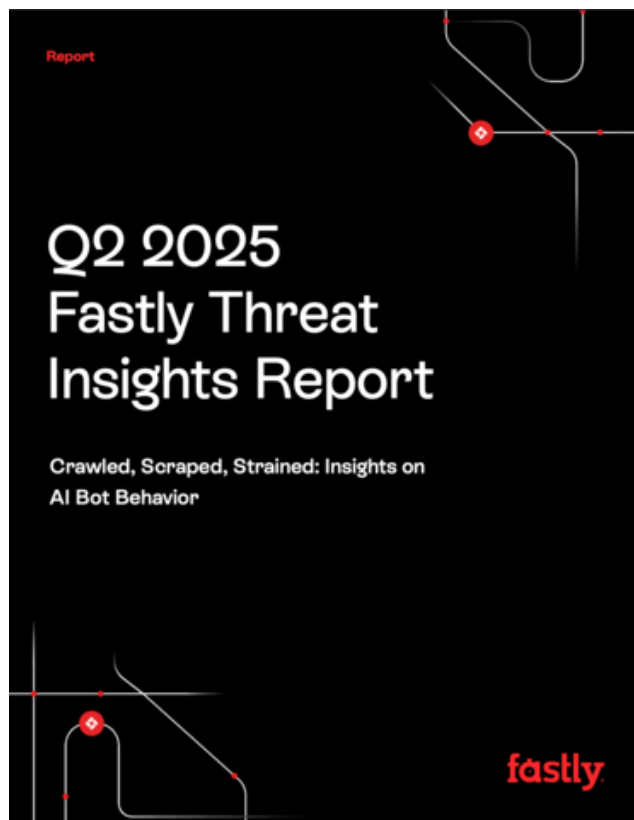


New Fastly Threat Research Reveals AI Crawlers Make Up Almost 80% of AI Bot Traffic, Meta Leads AI Crawling As ChatGPT Dominates Real-Time Web Traffic

August 19, 2025

AI bots are driving increased content scraping, operational load, and high-frequency access patterns, revealing emerging risks from unverified automation traffic.

SAN FRANCISCO--(BUSINESS WIRE)-- [Fastly, Inc.](#) (NYSE: FSLY), a leader in global edge cloud platforms, today released its [Q2 2025 Threat Insights Report](#), exposing a striking shift in the nature and scale of automated web traffic. Analysis of traffic from mid-April to mid-July shows that AI crawlers made up almost 80% of all AI bot traffic observed, with Meta generating more than half and eclipsing both Google and OpenAI combined.



Fetcher bots—those that access website content in response to user actions—including those used by ChatGPT and Perplexity, are also driving massive real-time request volumes. In some cases, fetcher request volume exceeds 39,000 requests per minute. This surge is putting pressure on unprotected origin infrastructure, consuming bandwidth, overwhelming servers and mimicking the effects of DDoS attacks, even without malicious intent. North America receives a heavy skew of AI crawler traffic, accounting for nearly 90% of observed activity. Every other region, including Europe, Asia, and Latin America, sees a significantly smaller share, signalling a growing geographic bias in LLM training datasets and raising questions about the long-term neutrality of AI model outputs.

Fastly's [Q2 2025](#) report found that automated bot traffic already represented 37% of observed activity across Fastly's global network. While previous concerns centered on the volume of automated traffic, the Q2 data highlights the nature of that traffic, with AI bots now presenting a more complex challenge to security, performance, and operational resilience.

Drawing on 6.5 trillion monthly requests¹ across Fastly's [Next-Gen WAF](#) and [Bot Management](#) products, the findings offer a detailed view of how AI-driven automation is reshaping online traffic. With visibility into over 130,000 applications and APIs² across a wide range of industries including e-commerce, media, financial services, and technology, Fastly's insights shed light on the

evolving battleground for web security and control.

Additional findings include:

- Meta's AI bots alone generate 52% of AI crawler traffic, more than double that of Google (23%) or OpenAI (20%).
- Commerce, media & entertainment, and high-tech sectors face the highest levels of scraping for training AI models.
- ChatGPT generates the most real-time traffic to websites, with 98% of fetcher bot requests attributable to OpenAI's bots.
- Lack of bot verification persists, making it difficult for security teams to distinguish between legitimate automation and malicious impersonation.

"AI Bots are reshaping how the internet is accessed and experienced, introducing new complexities for digital platforms," said Arun Kumar, Senior Security Researcher at Fastly. "Whether scraping for training data or delivering real-time responses, these bots create new challenges for visibility, control, and cost. You can't secure what you can't see, and without clear verification standards, AI-driven automation risks are becoming a blind spot for digital teams. Businesses need the tools and insights to manage automated traffic with the same precision and urgency as any other infrastructure or security risk."

The report calls for more transparent bot verification, clearer signalling by bot operators, and smarter [bot management strategies](#). Without them, organizations face growing exposure to shadowy automation, attribution gaps and escalating infrastructure costs.

To read the complete report, visit <https://learn.fastly.com/Security-Threat-Insights-Report>.

About Fastly, Inc.

Fastly's powerful and programmable edge cloud platform helps the world's top brands deliver online experiences that are fast, safe, and engaging through edge compute, delivery, security, and observability offerings that improve site performance, enhance security, and empower innovation at global scale. Compared to other providers, Fastly's powerful, high-performance, and modern platform architecture empowers developers to deliver secure websites and apps with rapid time-to-market and demonstrated, industry-leading cost savings. Organizations around the world trust Fastly to help them upgrade the internet experience, including Reddit, Neiman Marcus, Universal Music Group, and SeatGeek. Learn more about Fastly at <https://www.fastly.com>, and follow us [@fastly](#).

¹Trailing six-month average as of April 22, 2025.

²As of April 22, 2025

Source: Fastly, Inc.

Media Contact
Alex Klepel
press@fastly.com

Investor Contact
Vernon Essi, Jr.
ir@fastly.com

Source: Fastly, Inc.