Case Study

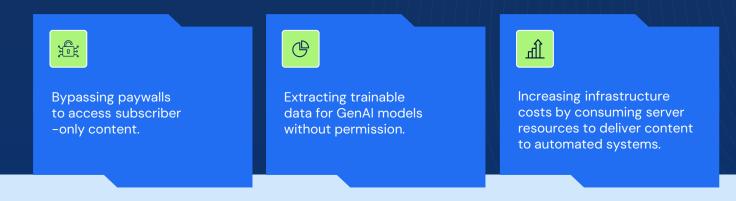
Newspaper Publisher Gains Control Over Content Theft with Netacea Bot Protection





NETACEA

One of the world's largest media publishers faced a growing problem with scraper bot activity across their extensive network of news websites. These bots facilitated content theft in multiple ways:



Despite having a rudimentary Web Application Firewall (WAF) in place, the client struggled with:

Limited visibility into bot traffic.



Inability to counter sophisticated, evolving bot tactics.

ۍ.

High utilization of their AWS infrastructure by bot traffic.

The executive leadership team prioritized solving this issue. The organization needed better visibility, control, and protection to combat content theft effectively, without having to manually block bots themselves.

The Solution



To tackle the issue head-on, the publisher partnered with Netacea, a leader in bot protection for a fully managed bot protection service.

STEP 01 Understanding the Bot Threat Landscape

Netacea's Threat Intel Center conducted extensive research across hidden marketplaces and forums to uncover content scraping configurations targeting the client's websites.

STEP 02 Data-Driven Detection

Netacea seamlessly integrated with the client's CloudFront CDN, ingesting web log data from key news sites. Using server-side analysis and machine learning algorithms, Netacea analyzed each web request's intent to differentiate between benign visitors and malicious bots.

This highly scalable and adaptive approach made it impossible for attackers to detect and bypass Netacea's defenses.



STEP O3

Automated Identification and Response

The detection models quickly identified that 24% of all website traffic came from malicious bots. Further investigation revealed advanced techniques employed by attackers, including:

Rotating IP addresses to evade detection.



Using spoofed user agents to mimic human visitors.

 \bigcirc

Netacea's machine learning algorithms automatically adapted to counter these evolving tactics, requiring no manual intervention from the publisher's internal teams.

The Outcome

Netacea's Bot Protection is now fully integrated across the publisher's news websites, delivering tangible results:

\$]



စ္

Reduced Infrastructure Costs

The publisher's infrastructure team reported a 24% drop in AWS usage, saving operational expenses. Visibility into Bot Traffic

Through the Netacea portal, the organization can now see and analyze every bot attempting to scrape their content.

Commercial Licencing of Ethical Bot Traffic

While malicious bots are automatically blocked, ethical scrapers that declare their identity can now be approached with financial agreements to license content access.

With Netacea Bot Protection, the publisher is not only addressing content theft effectively but also establishing new revenue opportunities in the era of generative Al.

By investing in robust bot protection technology, this organization has safeguarded its content assets, protected revenue streams, and positioned itself as a leader in managing the challenges posed by GenAl-driven content scraping.

Stop unwanted bot traffic with ease. Visit Netacea.com to book a demo

NETACEA