NETACEA

Netacea Bot Management

Netacea @Netacea_AI www.netacea.com hello@netacea.com

Contents

What is Netacea Bot Management?

All websites, mobile apps and APIs are now a target for malicious attacks by automated bots, putting profits, customers, data and reputation at risk. Without specialist bot protection in place, attacks such as credential stuffing, carding, fake account creation, scraping and scalping will succeed or go undetected.

On average, it is estimated that between 10% and 40% of traffic on a typical web-facing system is malicious bots.

These bot attacks are becoming ever more sophisticated and can appear human, bypassing many defenses that have been put in place to identify them.

Netacea Bot Management takes a new approach to bot detection, spotting known and evolving attacks to ensure that the maximum number of bots are detected with a minimum number of false positives.

Netacea protects your customers, data, brand and infrastructure from the threats posed by sophisticated bots and other automated attacks.

Monitor

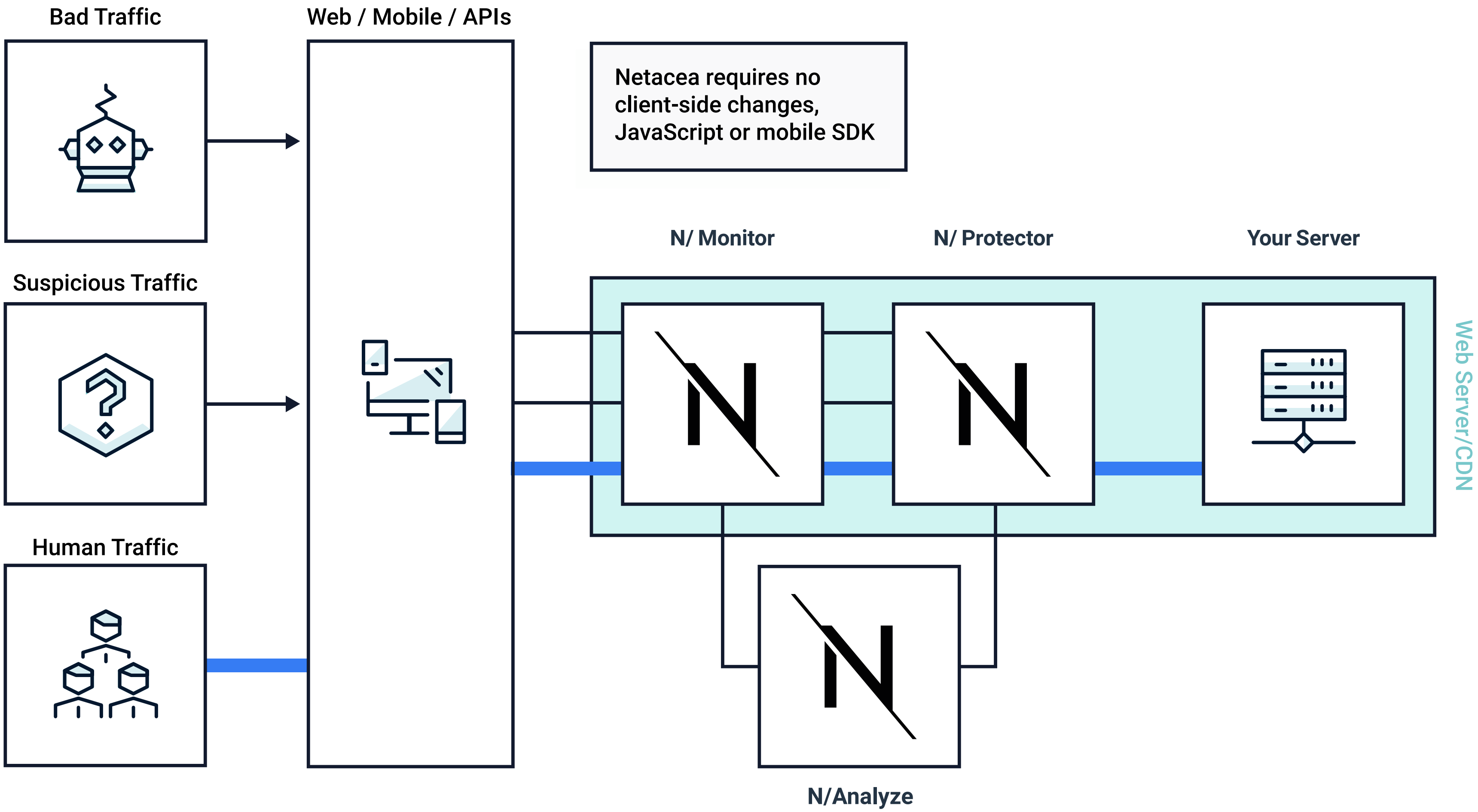
visitor activity across your website, mobile apps and APIs

Detect

automated threats with unparalleled speed and accuracy

Protect

your customers and platforms from attacks with real-time mitigations



Netacea requires no client-side changes, JavaScript or mobile SDK

Key benefits

Most accurate

Netacea's multi-layer approach and ability to detect evolving attacks ensures that there is maximum accuracy and minimum false positives and/or negatives.

Low maintenance, backed by expert service

Netacea's auto-detect technology backed by proactive bot experts ensures that any threats to your platform are automatically identified and mitigated. There is no requirement for complex configuration or ongoing creation and management of rulesets.

Easy to integrate

Ease of integrations with existing systems is one of Netacea's core values. You can leverage your existing platforms and skillsets to build a low friction integration with the full Netacea platform, without deploying changes to your applications or installing any physical or virtual hardware.

Bots cost the average enterprise 3.6% of their annual online revenue. For 25% of the businesses we surveyed, this equates to $250m.

The Netacea difference

Maximum accuracy, maximum speed

Many bot management tools focus on speed of detection over reduction of false negatives. Although we usually identify bots before any requests have reached your server, only Netacea's layered detection maximizes speed while maximizing accuracy.

Continuous detection

Other bot detection tools only check a visitor on first arrival. Instead, Netacea reassesses every user after every request to ensure bots are detected even if they appear human on first contact.

Crowdsourcing malicious threat mitigation

We process billions of requests and identifiers across the full range of countries and industries we're able to identify and add novel bot threats to our shared Active Threat Feed - giving you and all our customers immediate protection.

Zero maintenance and proactive support

Using machine learning and data science, our technology learns what normal behaviour looks like for your platform, and ensures that we're always able to apply protection in line with your attitude to risk. You don't need to regularly log in to respond to alerts, configure rules or manage settings.

Low risk to your customers or developers

Relying on client-side JavaScript and mobile SDKs to perform security is putting your defenses into the hands of the attackers to develop bypasses, so no client-side application changes are involved in deploying our product.

Multiple protection modes

Whether you want instant inline mitigation of threats or a stream of data to augment existing defense mechanisms, Netacea Detector can pass mitigations or recommendations to your systems in a manner that suits you.

Purpose built for modern bot detection

Bots can't hide their intent at the server level. Netacea Bot Management has been designed to handle the level of data, and complexity of analysis required to identify bots at this layer.

Detects automated OWASP threats including credential stuffing, web scraping, carding and fake account creation

Protects websites, mobile applications and APIs in one solution

Deploying Netacea Bot Management

Salesforce Commerce Cloud

All Netacea functionality will be enabled by integrating the Netacea cartridge into your application. This cartridge will provide streaming of request data to Netacea and connect to Netacea's service to determine whether connections should be allowed, or mitigations applied.

Fastly

Data is streamed to Netacea using Fastly's Real-Time Log Streaming facility to Netacea's S3 bucket. Netacea will provide documentation on the data fields that need to be included. Mitigation is carried out within the Fastly VCL. Netacea will provide a VCL snippet to deliver functionality for connecting to the Netacea service to retrieve recommendations for each new visitor.

Cloudflare

All Netacea functionality is provided within a single Cloud Worker that Netacea will supply for you to upload into your Cloudflare configuration. This Cloud Worker will provide streaming of request data to Netacea asynchronously and connect to Netacea's service to determine whether connections should be allowed, or mitigations applied.

N/ Plugins

To speed up the integration process, Netacea has a pre-built range of plugins for the most common technology platforms.

N/ Data Stream

Netacea can be deployed by sending a stream or regular batch of data for analysis. Netacea can provide a Detection Feed that enables you to apply your own mitigations.

N/ API

Full integration to Netacea can be easily created by calling our open API.

N/ Cloud

If our current integration methods are not suitable, Netacea's highly distributed, low latency cloud solution can be deployed to sit in front of your systems and provide full Netacea protection.

"Netacea has worked closely with us to help us understand the bot challenges we were previously unaware of, enabling us to significantly reduce infrastructure costs and fraud losses."

Head of Operations, Top three global sports betting platform

Customer success stories:

Top 3 sports betting platform cleans up online traffic

Client challenge

A large global gaming and betting organization was facing high levels of automated traffic on its website and recognised it had a problem with bots but wasn't aware of the full scale of the issue.

Bots were being used to scrape data and odds from the business's website. This large volume of unpredictable traffic was threatening website availability for legitimate customers while significantly increasing infrastructure costs.

This malicious activity increased in the lead up to and during peak sporting events. Worse yet, the scraped data was being used to exploit imbalances in the odds across multiple operators, leveraging arbitrage betting in an automated manner. This significantly increased the chances of the risk-free betting – a problem already estimated to cost the gaming and betting industry £12 million per annum.

Despite having several solutions in place such as WAFs, fraud and security tools, the business lacked visibility of bot traffic on its website and was dependent on manual analysis to block and mitigate attacks. This often led to false positives, resulting in legitimate customers being inadvertently blocked and the business' revenue taking a significant hit.

The solution: Netacea

Recommendations from Netacea Bot Management were sent to the internal SIEM solution, then depending on the risk of the threat and the aggressive nature of the scraping, the operator provided an automated response. Netacea identified that over 30% of all website requests were made by bots. This became the foundation to a business case that would demonstrate a five-month ROI, consisting of infrastructure, fraud, operational and security savings.

Results

- 20% increase in online capacity
- 85% reduction in unwanted bets placed by bots
- 40% reduction in total website requests
- Overall savings across infrastructure, fraud losses and staffing of £3 million
- Improved manageability and predictability of traffic patterns

Top 5 global retailer puts a stop to account fraud

Client challenge

In 2018, one of the world's largest retailers identified they were being frequently targeted by credential stuffing attacks.

Threat actors utilised breached usernames and passwords to access customer accounts and make fraudulent purchases to the tune of millions of pounds per month, before selling the validated account details on the dark web.

Threat actors typically used a combination of volumetric and sophisticated low and slow attacks to carry out the credential stuffing activity. The attackers were able to bypass the protection put in place by the retailer's existing WAF and DDoS vendor, and manual, reactive mitigation measures were required by the business's Security Operations Centre (SOC) team, putting strain on internal resources.

The retailer needed a specialist bot management vendor that could provide rapid detection and mitigation, using technology that would integrate with existing architecture to ensure they maintained visibility of all website, mobile app and API traffic.

The solution: Netacea

Netacea Bot Management accurately identified several credential stuffing attacks within 24 hours of implementation. Over the course of the next 30 days, the solution detected large volumetric credential stuffing attacks and highlighted continued low and slow attacks that were flying under the existing vendor's radar.

Results

- 650,000+ malicious login attempts mitigated per week
- Customer account fraud costs reduced by £1.4 million per month
- Internal product and security resources freed up to focus on business needs

Netacea received the highest score in the Bot Detection criterion in The Forrester Wave™: Bot Management, Q2 2022 report

Forrester, a leading research organisation that provides advice on existing and emerging technology, identified Netacea as a Strong Performer in its 2022 evaluation of the bot management market, despite being "among the smallest vendors in this Forrester Wave." Netacea also received the highest possible score for Threat Research.

The report, authored by Sandy Carielli, Forrester Principal Analyst, evaluated 15 top vendors in bot management and found that Netacea customers "applauded the product's effectiveness and the 'very attentive' support team."

To find out more about Netacea's unique approach to stopping sophisticated bot threats, visit www.netacea.com/why-netacea or talk to our team today at hello@netacea.com.