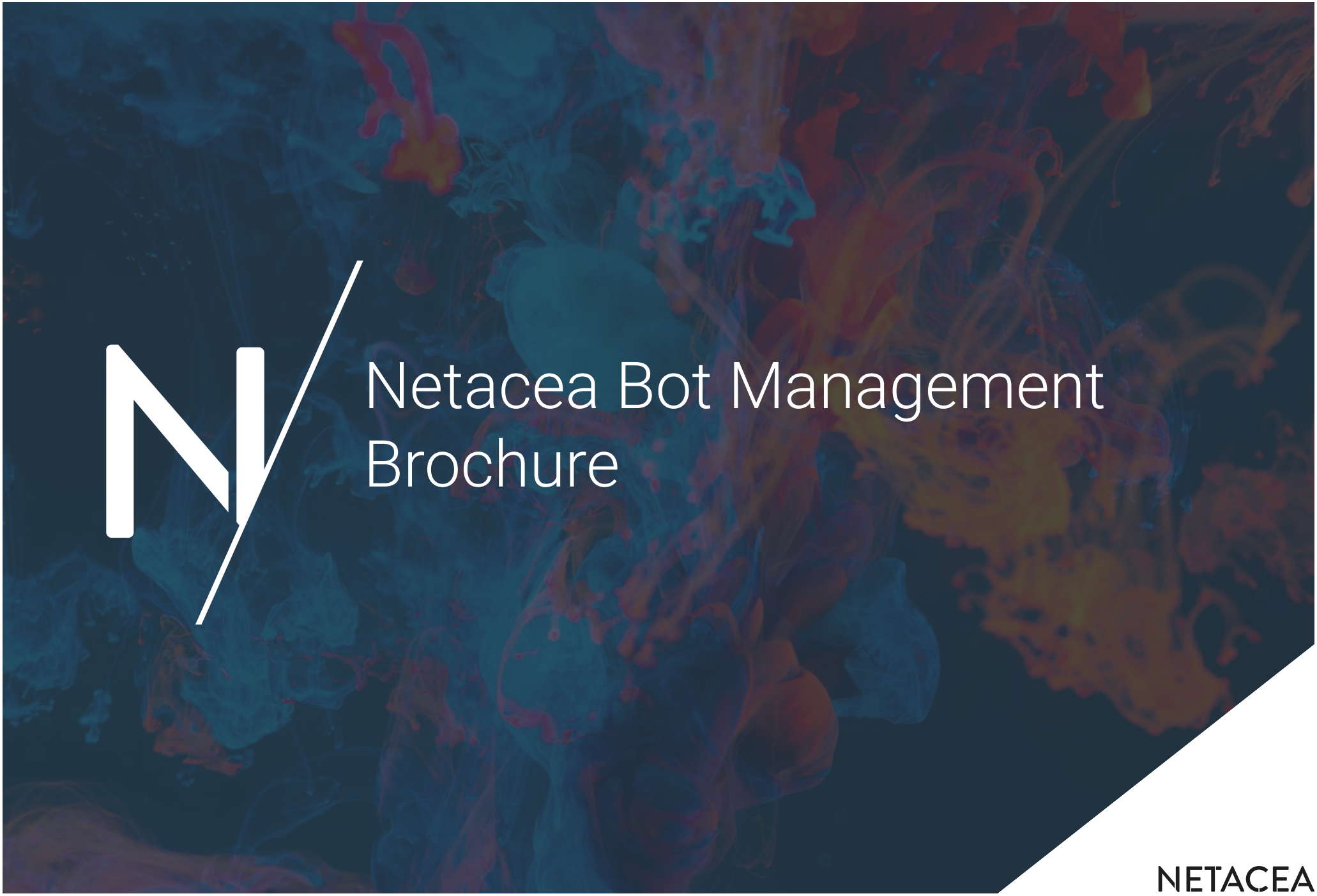


Netacea Bot Management Brochure

NETACEA

NETACEA

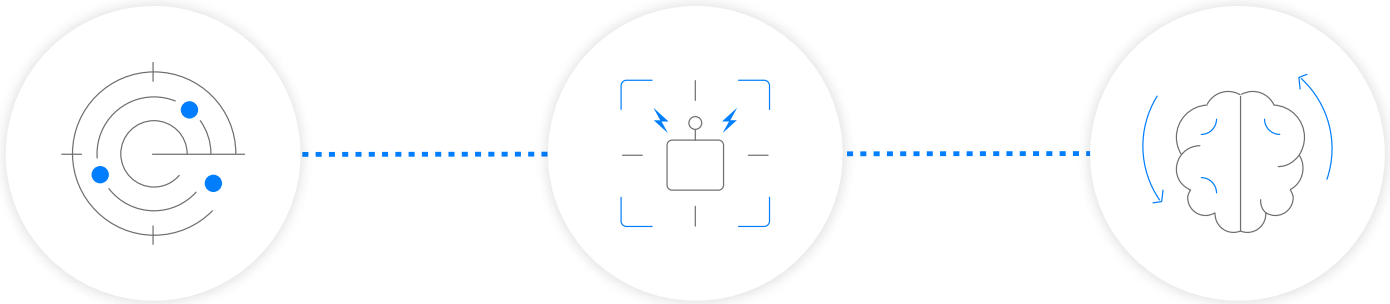
WHAT IS NETACEA BOT MANAGEMENT?

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 defences 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

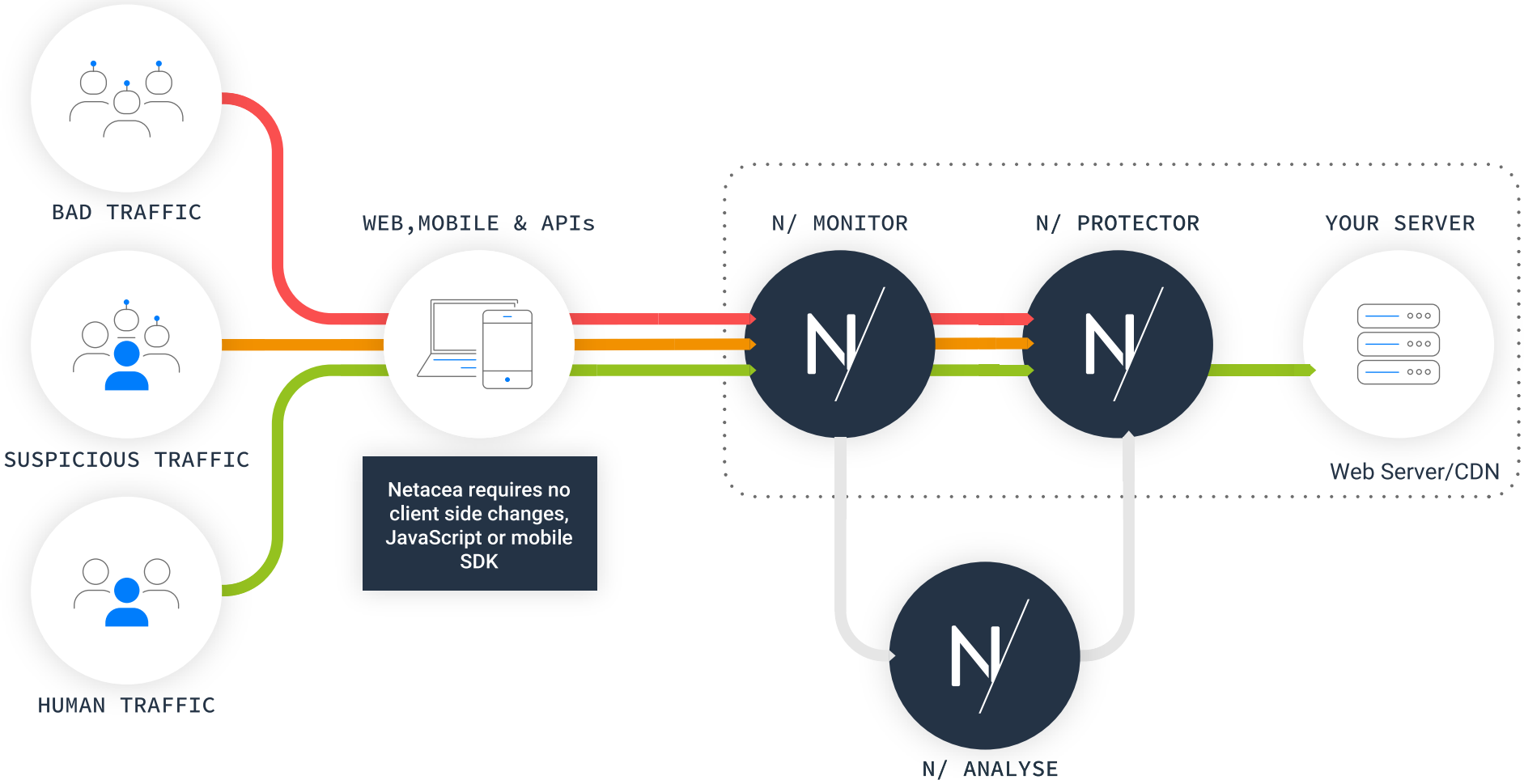
visitor activity across your website, mobile apps and APIs

DETECT

automated threats with unparalleled speed and accuracy

PROTECT

your customers and platforms from attacks with real-time mitigations


BAD TRAFFIC
SUSPICIOUS TRAFFIC
HUMAN TRAFFIC
WEB,MOBILE & APIs
Netacea requires no client side changes, JavaScript or mobile SDK
N/ MONITOR
N/ PROTECTOR
YOUR SERVER
Web Server/CDN
N/ ANALYSE

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.

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 is 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.

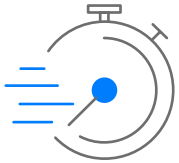
N/ API

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.

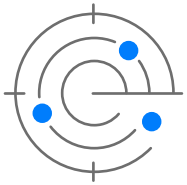
THE NETACEA DIFFERENCE



Maximum accuracy, maximum speed

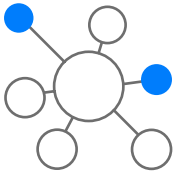
Most of the time Netacea will identify bots at the point of first contact, before any requests have reached your server. However, Netacea involves multiple layers of defence, allowing reduction in false negatives by running additional analysis of visitor activity.

Many bot management tools focus on speed of detection over reduction of false negatives. Only Netacea's layered detection maximises speed while maximising accuracy.



Continuous detection

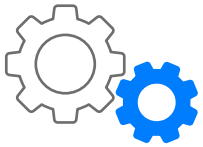
Bots attempt to bypass your defences and masquerade as legitimate human users. Ultimately, however, they are not undertaking legitimate activities. Many bot detection tools will only check a visitor on first arrival. Netacea re-assesses every user after every request to make sure bots are detected even if they appear human on first contact.



Protected by the power of the Netacea customer network

Netacea's network handles billions of requests and identifies bots across the full range of countries and industries.

Netacea analyses these bots and when they are identified as a threat to the wider network, they are instantly added to our shared Active Threat Feed and all customers receive immediate protection.



Low maintenance with Netacea Auto-Protect

Netacea is built to detect bots. Our detection modules, combined with our bot experts, will learn normal behaviour for your platform and ensure that Netacea is optimally configured to apply protection in line with your attitude to risk.

There is no need to regularly log in and respond to alerts, configure rules or manage settings.

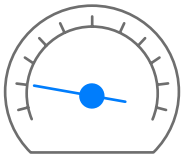
Proactive expert support

Netacea's team of customer success managers and bot experts work proactively to understand your site, typical traffic and attitude to risk. This allows them to proactively monitor your site activity to ensure that Netacea Bot Management is optimally configured and providing maximum protection with minimum impact to your customers.

Protecting all your web-based systems

Your web presence is about much more than just a website and attackers will often target other channels that are less well protected.

Netacea provides the same level of protection to all your web-facing systems including website, mobile apps, APIs and web-based applications out of the box.



Low risk to your customers or developers

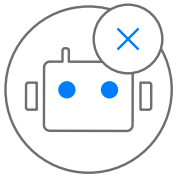
Client-side JavaScript and mobile SDKs can be a security and privacy risk to you and your customers. Relying on any client-side functionality to perform security is putting your defences into the hands of the attackers to develop bypasses.

Netacea believes that the risk of asking customers to deploy client-side changes far outweighs any benefit so no client-side application changes are involved in deploying our product.

Multiple protection modes

Some customers want instant inline mitigation of threats. Other customers have existing risk mechanisms and want Netacea detection to be a part of that.

Netacea can support both of these models (or a combination of the two) allowing customers to take full advantage of the power of Netacea Detector in a manner that suits them.



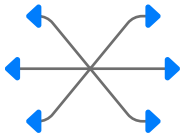
Purpose built for modern bot detection

Netacea identified that server-side analysis was the most effective approach when detecting bot activity. Netacea Bot Management has therefore been designed to handle the level of data, and complexity of analysis required to identify bots in this way.

Legacy products are unsuited to the server-side approach and the levels of complex analysis required for effective detection.

Breadth of bot detection

Netacea identifies and categorises the full range of automated bot attacks, including those identified by OWASP such as credential stuffing, web scraping, carding and fake account creation.



Easy to deploy across any platform

Netacea is easy to integrate by design, no matter the technology stack or platform you are using. Netacea has a range of pre-built plugins with all major technology stacks and platforms. If our range of plugins are unsuitable, Netacea can be integrated via our open API by providing a stream of data or by using our highly distributed, low latency cloud solution.

There is no need for application changes or physical or virtual hardware deployment.

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 for connecting to Netacea's service to determine whether connections should be allowed, or mitigations applied.

CUSTOMER SUCCESS STORIES:
Top 3 sports betting platform cleans up online traffic

Client challenge

A large global gaming and betting organisation 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

CUSTOMER SUCCESS STORIES:
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

NETACEA RANKED AS LEADER IN THE FORRESTER NEW WAVE™: BOT MANAGEMENT, Q1 2020

In 2020, top research organisation Forrester identified Netacea as a leader in its 2020 evaluation of the emerging bot management market.

The Forrester New Wave™: Bot Management, Q1 2020 Report evaluated the top 13 vendors in bot management and determined Netacea to have among the highest scores in the strategy category with a differentiated rating in 8 out of 10 criteria.

Netacea's differentiating server-side approach to bot management combines web log analysis with real-time and historic trends to analyse user behaviour and determine intent. The technology is uniquely equipped to detect sophisticated threats, combining an extensive signal collection with deep analysis and dashboards that address both security and business context in the enterprise environment.

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.