Netacea for Security Teams

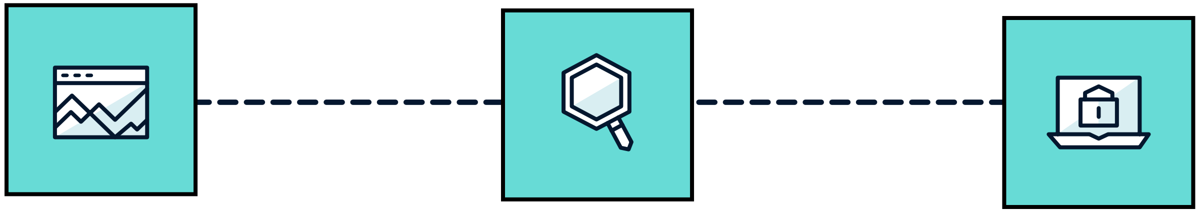
All websites, mobile apps and APIs are now a target for malicious attacks by automated bots, putting profits, customers, data and reputation at risk. Now making up over 40% of web traffic, malicious bots are sophisticated enough to appear human. Without specialist bot protection, attacks such as credential stuffing, carding, fake account creation, scraping and scalping are impossible to detect or prevent.

How Netacea helps

Netacea Bot Management takes a new approach to bot detection, using machine learning to spot known and evolving attack vectors on the server side. This maximizes the number of bots detected whilst protecting genuine customers.

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

How it works



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

Server-side monitoring

- **Every request and transaction captured across web, mobile and API**
- **Invisible protection that can’t be detected by bots**
- **Highly scalable platform analyzes billions of requests daily to detect malicious behavior**

Machine learning-based detection

- Predictive protection that adapts to new attacks, enriching data for better decision making
- Flag and mitigate bot traffic in real time
- Adept at detecting the most sophisticated and distributed attacks

Bot expertise

- Bot Intelligence Service augmenting your security team, freeing up time and resource
- Dedicated threat research team infiltrating criminal forums for new attacks
- Bot expert team delivering deep insights into mitigated threats

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

NETACEA

Stop a wide range of bot attacks

Netacea combats bot attacks as described in the BLADE Framework™*, including:

Credential stuffing

Aggressive credential stuffing bots hit login screens millions of times in short succession. Netacea removes this strain from your infrastructure and protects your customers' accounts from unauthorized access or sale on the dark web.

Account takeover

By securing accounts, we stop bot operators making a profit from selling your customers' credentials, payment details and private information, or by redirecting transactions and loyalty points to other accounts.

Scalper bots

We ensure your stock goes to legitimate customers rather than being scalped by bots and sold on secondary markets as soon as items become available.

Web scraping

Some scraper bots are useful and wanted, such as SEO tools and aggregator partners. Others are malicious or too aggressive. Netacea classifies each kind and blocks only the bad bots.

Carding attacks

Stop bots testing stolen card details against your system, eliminating unnecessary verification costs and chargebacks for fraudulent purchases.

Fake account creation

Stop bots from creating new accounts en masse to prevent costly attacks like scalping limited stock items and abusing bonus and welcome offers.

Gift card and voucher abuse

Stolen gift card and voucher balances are a popular commodity on dark web forums. Cut down on customer complaints and reimbursement of lost balances by protecting these valuable assets.

*Learn more about the BLADE Framework™ at www.bladeframework.org