FLEXIBLE API INTEGRATION

NETACEA DEEPER INSIGHT

FLEXIBLE API INTEGRATION

SEND THREAT INTELLIGENCE DIRECT TO YOUR EXISTING SECURITY LAYERS | AVOIDS LATENCY ISSUES | CUSTOM PROGRAMMATIC INTEGRATION INTO YOUR EXISTING CDN/WAF INFRASTRUCTURE

KEY BENEFITS

• Programmatic granular control so you can use the Policy API to apply the threat analysis to wherever it is needed in the enterprise.

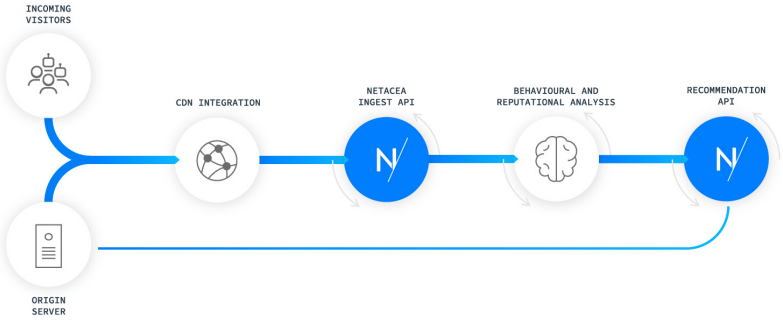
• The full API set allows you to customise the threat intelligence by behavioural type so you can fine tune policies programmatically at volume. This is essential to help mitigate against the 'slow and low' bot that hide just below the radar of rate limiting, disguised as normal visitors.

• Allows for a wide range of custom configurations to be deployed into a micro-service or in a particular set of legacy architecture.

• No need to login into yet another console

• Can handle very large volumes of data

• Threat analysis data feeds can be supplied in various formats so you can integrate the threat intelligence in the best way for your enterprise.



Visual Diagram To illustrate an API Integration

API INTEGRATION

Our adaptive API architecture supports a wide range of infrastructure from leading product vendors, allowing you to integrate our machine learning risk reduction into your existing platform of choice.

The adaptive data model and micro-services API approach gives huge power and flexibility to ensure that even the most complex of visitor requirements can be elegantly and reliable handled at volume, using the existing infrastructure that enterprise customers already maintain and own.

We complement existing controls such as WAF rulesets, rate limiting and threat databases, to provide deep analysis of all website visitors., through a practical use of A.I. to understand human and bot behaviours and adjust their website journey in real-time.

INGEST-LOG LEVEL ANALYSIS

The heavy processing needed to establish standard deviations of 'normal behaviour' v abnormal behaviour can all done out of line without affecting your site's visitors in any way via our Ingest streaming endpoint.

All the data is analysed by the machine learning engine, which is then able to provide a rich and detailed profile of who are the authentic versus the fake actors, browser emulators, and obvious bad actors, historical data is used to establish exactly what bots are doing on your site.

MACHINE LEARNING DATA LABELLING

Although you may not know what bots are actually hitting your web site, most businesses have very clear policies on how they want bot visitors to be handled once they know what the bot payload actually is.

For example, if you knew that bots were hitting your web site faking the behaviour of well known search engines, but were in fact competitive scrapers, you probably will know what policies you want to put in place to deal with these obvious fake search engines.

Once you set up the policies and key critical paths the machine learning then takes your input and builds up a custom threat score for your actual environment.

Everything is then automatic and the set-up for the original learning just takes a few minutes to complete.

As we identify new bot threats, you can guide the machine learning at any time by adding your feedback into how you want to treat bots. You can get as granular as you like, or just accept the default settings from your custom configuration list.

Classifications include:

- Fake Search Engine Bots
- Scrapers
- Shopping Cart Abuse
- Account Takeover

POLICIES API

The policy API will allow you to configure policies based on complex conditional statements and rules, to allow you to automate the mitigation of visitors, grouped by behavioural characteristics. The Policy API will allow you to create, edit and delete policies programmatically, updating in real time and integrating seamlessly with your estate.

EVENTS & RECOMMENDATIONS

Netacea carries out near real time analysis of the data provided and, based on the policies and configuration defined, provides recommendations as to how future requests should be handled.

Any actions that are taken (and reasons why) are provided to customers within the management interface delivering transparency and visibility into the performance of the solution. The facility to provide continuous feedback on any actions taken by Netacea is used to help eliminate false positives and to drive operational efficiencies that are tailored specifically to your traffic. These recommendations are provided by the Recommendations API.

The events API has several predefined channels for the output of this data and is typically implemented as a push based API.

The Recommendations API can pass Automated Actions directly to the Web Application Firewall, or push recommendations to the Origin Server or chosen SIEM engine to enhance intelligence and mitigate attacks. Through consultation with our development team custom integrations can be devised and supported.

Netacea provides advanced insight and visibility into your web traffic, allowing you to create powerful actions based on deep machine learning insight, using APIs. Visit Netacea.com to find out more.