NETACEA

How Netacea uses machine learning to stop new bot attacks

Ditch rules-based bot management and keep up with attackers with Intent Analytics

Key benefits of Intent Analytics®

Netacea's Intent Analytics is a suite of technologies that powers our threat detection capabilities:

- Adapts to new threats in real time 24/7 without you needing to lift a finger
- Attackers can't reverse engineer our agentless detection technology
- Learns and gets better with each request analyzed
- Industry leading 0.001% false positive rate across wide range of attack types:
  - High volume / 'low and slow' traffic patterns
  - Narrow / distributed attack origins
  - Attacks focused on a specific area / spread across many areas

Rule-based bot detection can't keep up with attackers

Many security products provide a generic solution, using block lists of known bad actors to protect you against the most obvious attacks.

However, attackers adapt their methods to bypass defense policies. Client-side detection solutions are especially susceptible because attackers can decipher your code, see which offensive signals you are looking for and build their attacks accordingly.

And so, the never-ending 'cat and mouse' chase begins as you scramble to react and update your block lists across endpoints, only for multiple attackers to change their tactics within hours. This wastes significant time and resources, yet still misses emerging attack types.

Stay ahead with Intent Analytics

Netacea's Intent Analytics engine detects both known and unknown threats using machine learning, a subset of artificial intelligence (AI) that analyzes huge amounts of data faster and more efficiently than humans whilst becoming more accurate and efficient over time.

Intent Analytics uses supervised and unsupervised machine learning and anomaly detection to stay ahead of new threats by analyzing behaviors that are impossible for attackers to spoof.

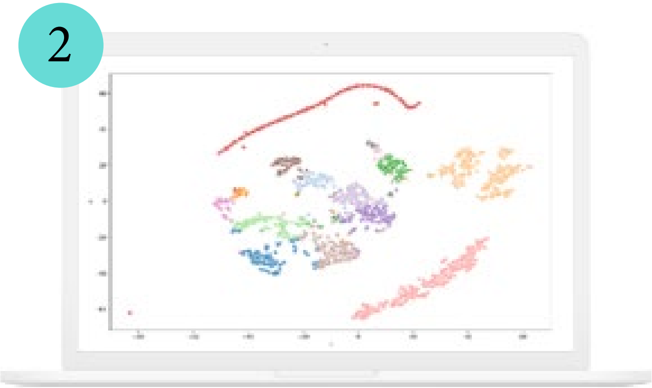
How Intent Analytics detects evolving threats

1

Supervised machine learning:

Trained to detect specific attacks, even from new threat actors.

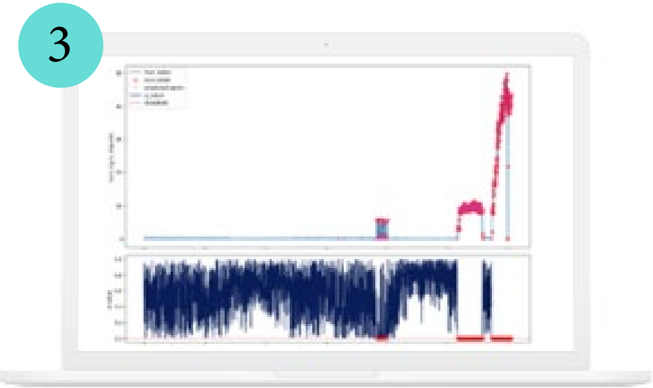
2



Unsupervised machine learning:

Spots rapidly changing and emerging threats within huge volumes of data, grouping behaviors together automatically.

3



Anomaly detection:

Detects unusual behavior within expected traffic patterns to highlight even highly distributed or low volume attacks quickly.

Combining machine learning with human expertise

Findings are inspected by our dedicated team of bot experts, who enrich outputs with data analysis and tune models for your use cases. This data also helps our threat research team tackle cybersecurity trends and allows our data scientists to build new models for your business.

About Netacea

Netacea received the highest score in the Bot Detection criterion in The Forrester Wave™: Bot Management, Q2 2022. Its Intent Analytics® engine analyses web and API logs in near real-time to identify and mitigate bot threats. This unique approach provides businesses with transparent, actionable threat intelligence that empowers them to make informed decisions about their traffic. Visit netacea.com for more information.