NETACEA

Unified Bot Protection That Effortlessly Secures Your Websites, Apps & APIs

Netacea enhances bot threat intelligence, detection and response. Used by leading InfoSec teams to reduce risk, fraud and prevent attacks in real-time by mitigating threats across the kill chain.

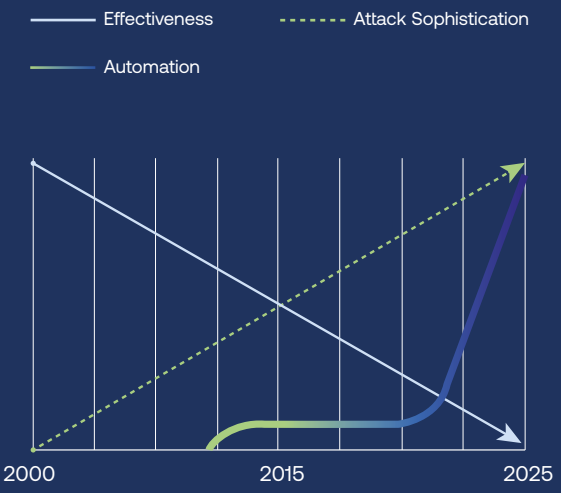
Traditional Bot Protection Is Broken

Legacy Solutions Miss Over 90% Of Attacks

Built for a previous generation of automated attacks, traditional tooling is no longer fit for purpose.

Enhanced technology, consumer adoption and the rise of Offensive AI are accelerating the sophistication of attacks, to dramatically outpace conventional control measures.

Netacea's unique approach makes us the only vendor that identifies, predicts and stops attacks across the entire attack lifecycle at machine speed.



83% Of Attack Tactics Are Not Solved By Existing Tech

Traditional tools focus on defence bypass, missing 83% of tactics deployed by adversaries.

90% of Attacks Missed By Leading Providers

Bot operators are bypassing defences and exploiting the gaps existing solutions can't cater for.

Limited, Complex Attack Surface Protection

Unable to protect at the edge, deployment challenges and complexity enables exploitation by bots

Secure Your Business With A Platform Built To Address Risk Across The Full Automated Attack Lifecycle

Mix and match services to deliver the threat coverage you need

Model

Understand the scale of the problem with bot cyber threat intelligence feeds and services.

- Netacea Sentry
- Threat Research

Harden

Boost your baseline protection and visibility of automated attacks based on years of curated, known threats.

- Business Attack Intelligence

Detect & Respond

Effortless AI-driven bot protection. Real time mitigation from sophisticated and dynamic automated attacks.

- Netacea Bot Protection

bitwarden DOMĚSTIKA OFFICE LUISAVIAROMA Dr. Martens AirWair Backblaze

Only With Netacea Can You Address 100% Of The Attack Tactics Used By Automated Adversaries

BLADE

Netacea pioneered the industry standard BLADE Framework for identifying and managing business logic and automated attacks

1. Resource Deployment
Attackers acquire the skills and knowledge to start an attack

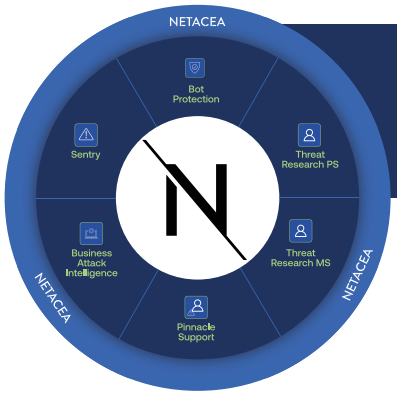
2. Reconnaissance
Attackers start to understand your weaknesses and what they can exploit

3. Defence Bypass
Attackers develop techniques or tools to bypass your defences

4. Attack Execution
Attackers undertake the bot attack

5. Actions On The Objective
Attackers exploit the data or privileged access they have achieved

6. Post-Attack
Attackers reap the awards



33x
more bots blocked vs competitors

36 Billion
signals analyzed daily

3,000+
active threat groups monitored

Netacea Products		1. Resource Deployment	2. Reconnaissance	3. Defence Bypass	4. Attack Execution	5. Actions On The Objective	6. Post Attack
		Automated Attack Cycle					
Netacea Sentry	Netacea AI-driven insights to see what your adversaries have done and have planned	✓	✓	✓			✓
Threat Research	Access to industry leading threat intelligence reporting	✓	✓	✓			✓
Business Attack Intelligence	Shareable dataset of known sources of malicious automated attacks				✓		
Netacea Bot Protection	Real-time, inline AI-driven protection against all automated attacks		✓	✓	✓	✓	
+ Pinnacle Support	AI-driven bot protection tailored with dedicated data science expertise		✓	✓	✓	✓	

See How Netacea Can Help You Automate Your Bot Protection

Uncover threats and block bots with Netacea.
Visit Netacea.com to book a demo

FORRESTER®
WAVE LEADER 2022
Bot Management