NETACEA

API Security from Netacea

How Netacea delivers complete API security

Netacea captures all requests, including via APIs, by analyzing API usage using low friction integrations without deploying changes to your applications or installing any physical or virtual hardware.

Protect API vulnerabilities with Netacea's advanced AI

API attacks can be generic across targets or written specifically to attack individual APIs. Intent Analytics®, our real time threat detection platform, uses machine learning algorithms to continually analyze every single request and rapidly categorize both broad and highly targeted API attacks.

Netacea's powerful AI also detects new attacks, patching unknown vulnerabilities as quickly as adversaries uncover them. We continually assess how your APIs are being called and group every request into constantly changing clusters, highlighting malicious activity and taking corrective action.

Comprehensive coverage of API vulnerabilities

Netacea's API security platform provides a thorough layer of defense against API attacks in any environment. Every API is a potential entry point for attackers; Netacea provides total visibility of your full API inventory, including:

- Public APIs
- Internal APIs
- Partner & third-party APIs
- Composite APIs
- REST, JSON/XML RPC, and SOAP protocols

Netacea's server-side data ingest engine tracks and secures every single request coming from APIs at all stages in their lifecycle, from those in build through to production and even as they change, without intervention or reconfiguration.

API attacks are an increasing danger to information security

- API use is increasing, creating a bigger target for attackers
- Insecure APIs put data and infrastructure at risk
- API inventories are constantly shifting and getting more complex to defend
- Tools like WAFs and API gateways are ineffective against API attacks

Case study

A major US retailer was the target of a huge amount of malicious activity via its product listing API. Bad actors flooded the API with requests, intending to scrape data and scalp high-demand products for resale.

Netacea's API Security reduced daily requests to the API by 84% (over 10 billion requests) within weeks of implementation. Mitigating API attacks has protected the client against content and price scraping, and scalper bots, as well as reducing infrastructure requirements.

NETACEA

Features

API Inventory

Automatically maintains an up-to-date inventory of active and deprecated APIs for full visibility and protection

Automatic threat mitigation

Netacea's protection service can provide recommendations or apply instant mitigations without intervention

Continual analysis of anomalies and vulnerabilities

Machine learning engine constantly scans for malicious activity, whether high volume or 'low and slow'

Detailed reporting and support

Dashboards and reports provide analysis of attack behaviors and origins, e.g., location, datacentres, IP addresses, user agents, etc.

Use cases

Netacea API Security defends against a full range of API vulnerabilities, including the OWASP API Security Top 10:

Stop scraper bot activity
A drain on infrastructure and often the first step in a larger attack chain

Prevent account takeover
Keep user accounts safe from unauthorized access

Protect infrastructure availability
Mitigate malicious volumetric attacks

Stop 'low and slow' attacks
Data log analysis with machine learning exposes persistent low volume attacks

Block injection attacks
Prevent and analyze attempts to inject untrusted data into the system

Prevent third-party login abuse
Cut out attempts to gain access to systems via third-party API abuse

Secure stock, pricing and inventory APIs
Cut off common entry points for adversaries to carry out numerous attack types

About Netacea

Netacea is a leader in API security. Its Intent Analytics® engine analyses web and API logs in near real-time to identify and mitigate 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.

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