DATASHEET

INDUSFACE™

AppTrana - BOT Protection

AI-powered, fully managed bot management for websites and APIs

According to research, nearly 40% of internet traffic is bot traffic, with a significant ratio of them being bad bots. Generally, bots are a common tool employed by threat actors to carry out complex attacks in a sophisticated manner. Bot attacks may easily go undetected via conventional mitigation solutions. With AppTrana WAAP's AI-driven bot mitigation, protect your business against bot attacks like account takeover, credential stuffing, and scrapping from day zero.

KEY FEATURES

Behavioral & Real-time Analysis of Bot Traffic

Detect and block malicious bot activity in real time with AI/ML based behavioral patterns. Get multi-layered bot protection through behavioral analysis of a variety of parameters including IPs, user agents, URI, bounce rates and so on, making it easier to spot malicious bot requests.

Correlated Risk Scoring and Anomaly Detection

Scrutinise and observe the behavior of each request against various bot modules and get a correlated risk score to ensure any risky/anomalous behavior is accounted for in real-time.

Better Bot Protection Through Custom Controls

Get custom and granular controls to adjust how the bot modules protect your site. Adjust the risk tolerance to determine the protection level/ aggressiveness of each bot module.

Real-time Visibility Into Bot Mitigation

Get deeper insights and real-time visibility into the traffic patterns to your site, the classification of bot vs human traffic, and the types of bots interacting with your site to customize protection based on your needs.

Customized Protection

All applications are not same, there could be workflows that will trip the good bots that your applications leverage. Work with our managed service team to build workflow based custom policies to uniquely identify bots.

HIGHLIGHTS

Protection against account take over, brute force, scalping, card cracking and more

AI/ML based behavioral analysis

24X7, fully managed bot protection

Workflow based policies with zero false positive guarantee

Indusface is the only Cloud WAAP (WAF) Vendor With 100% Customer Recommendation For 4 Consecutive Years

Bot Threats Covered:

Threats	Characteristics
Carding	Perform multiple payment authorization attempts to verify the validity of bulk stolen payment card data
Token Cracking	Get mass enumeration of coupon numbers, voucher codes, discount tokens, etc.
Fingerprinting	Extract ilicit information from the web, application and database servers about the supporting software and framework types and versions
Scalping	Obtain limited-availability and/or preferred goods/services by unfair methods
Expediting	Perform actions to hasten the progress of usually slow, tedious or time-consuming actions on behalf of a person
Credential Cracking	Identify valid login credentials by trying different values for usernames and/or passwords
Credential Stuffing	Multiple log in attempts used to verify the validity of stolen username/ password pairs
Captcha Bypass	Solve anti-automation tests
Card Cracking	Identify missing expiry dates and security codes for stolen payment card data by trying different variations of these details until the correct combination is found, allowing unauthorized access to the card's funds
Scraping	Collect application content and/or other data for use elsewhere
Crashing Out	Buy goods or obtain cash utilizing validated stolen payment card or other user's account data
Sniping	Get last minute bid or offer, for goods or services
Vulnerability scanning	Crawl and fuzz application to identify weaknesses and possible vulnerabilities
Denial of Service	Target resources of the application and database servers, or individual user accounts, to achieve denial of service (DoS)
Skewing	Repeated link clicks, page requests or form submissions intended to alter metrics
Spamming	Malicious and/or more benign information addition, that appears in public or private content, databases or user messages
Foot printing	Probe and explore application to identify its constituents and properties
Account Creation	Create multiple accounts for subsequent misuse
Account Aggregation	Aggregate data from multiple accounts and interact with them on behalf of the account holders using an intermediary application