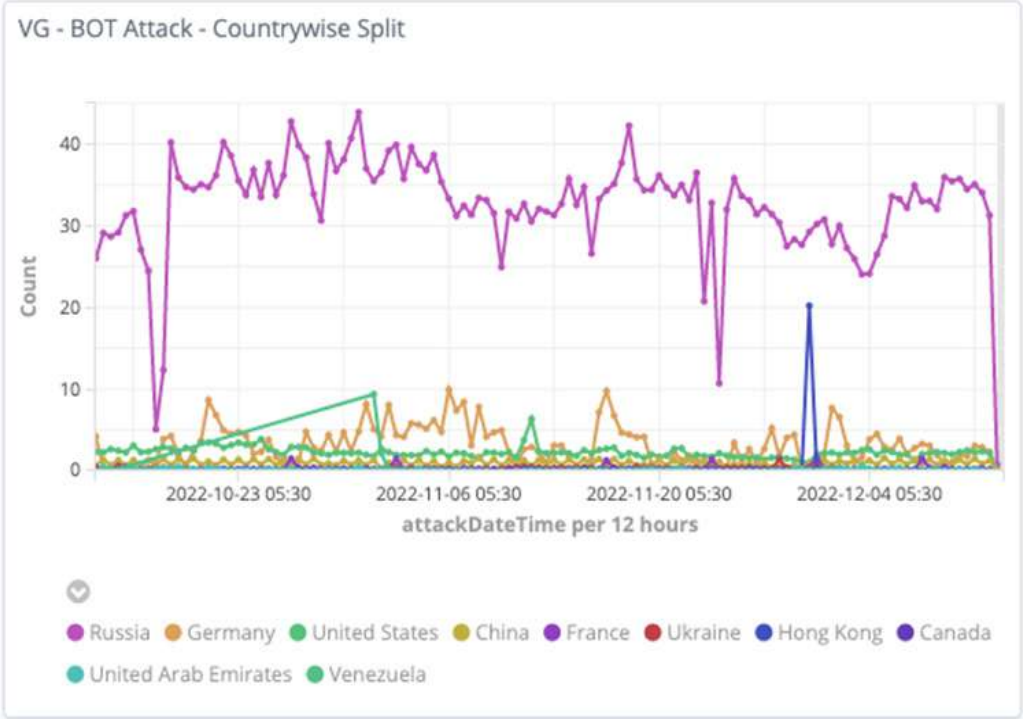
INDUSFACE™

10 Essential Considerations While Evaluating Bot Management Solutions

Saketh Rasakatla
Product Marketing Manager

In terms of a bot management solution, any company irrespective of its size and type would be unaware, confused, and distant to understand the features, technical details, and applicability to its application security needs.



VG- Top 10-BOT Attack Country

Country	Count
Russia	2,768,296
Germany	267,199
United States	192,743
India	132,759
China	82,117
France	24,991
Ukraine	16,195
Hong Kong	14,426
Canada	10,651
United Arab Emirates	10,461

Most are unaware of these latest bot trends. Hence, we have created this guide to help you evaluate Bot Management solutions.

Ask the following right questions to get the right answers for your security needs.

1

Range Of Detection Techniques

With the advancement of revolutionary and humanlike botnets, the bot management solution should have tertiary detection and response methods.

Check the following:

- The list of detection and response methods supported by the solution.
  For example: Bot vs Human Detection, Correlated Risk Scoring, Fingerprinting, Browser Validation, ML-based Behaviour Analysis, Reputation Analysis, Progressive Challenges, Rate-Limiting, Multi-factor Authentication, API security, IP Blacklisting, etc.
- How many methodologies are contained and the extent of their sophistication?
- Pick a solution comprising a full complement of bot detection & mitigation techniques, device and browser fingerprinting, intent and behavioural analysis, collective bot intelligence, and threat research along with the following as well:
  - Detection of OWASP Top 10 threats
  - Behavioral & real-time analysis of Bot traffic
  - Real-time visibility into Bot Mitigation

2

Managed Services

The bot management solution must provide managed services with 24*7 support.

Check the following:

- Is the solution available 24*7?
- Does the vendor provide/ include managed services in an SLA?
- Does it have the ability to add custom rules?
- Does the solution/ vendor take care of all your tech needs by themselves?
- How does the vendor take the responsibility for maintaining, anticipating, and improving the operations?
- Can the solution handle sophisticated bots? Ask for examples of sophisticated attacks the solution has successfully detected and blocked.

3

Flexibility Toward Various Threats

The bot management solution must be continuously upgraded or scaled according to the latest threats and bot attacks.

Check the following:

- Is deep learning and self-optimization available in the solution? Since these characteristics, identify that may adapt to escape detection.
- Can the solution handle sophisticated bots that mimic human behaviour, scrape websites, fill-out forms, etc? Ask for examples of sophisticated attacks the solution has successfully detected and blocked.

4

Multi-Generation Detection

A variety of approaches are designed for each of the current four bot generations.

Check the following:

- How can the solution beat the earlier generations? Common approaches like blacklists, fingerprinting, and Javascript are observed.
- How does it defeat modern bots such as social media bots, download bots, scraper bots, spam bots, spider bots, etc?
- Complex user behavioral analysis is needed for humanlike and advanced distributed bots.
- How can the solution comprehend and neutralize a bot's intent?

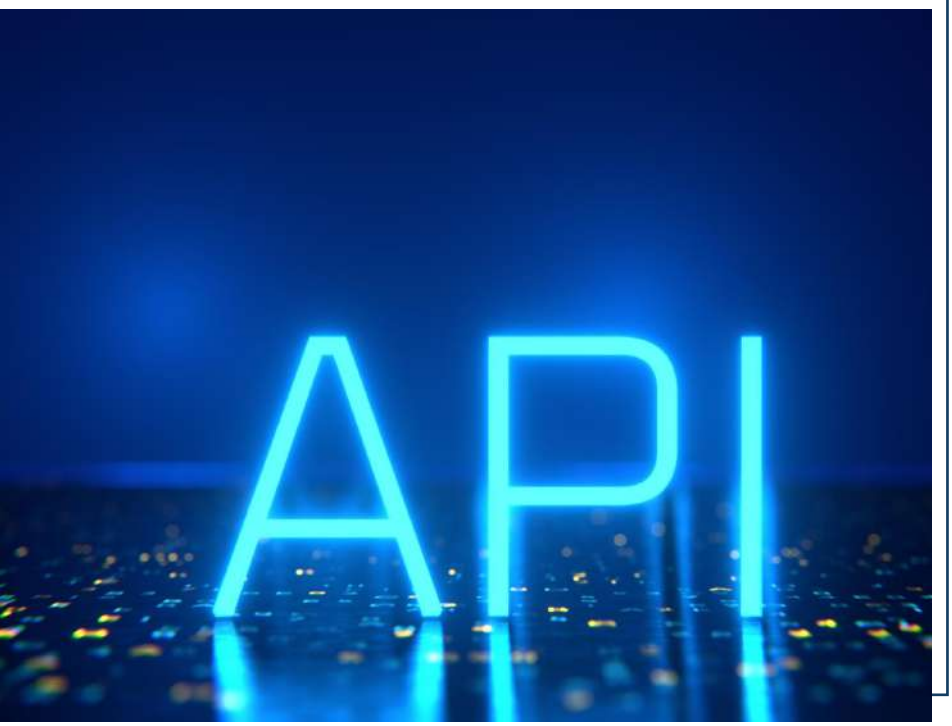
5

Robust Automated Response

Carefully, pick a solution that gives multiple response mechanisms to bot traffic.

Check the following:

- Execute a solution that can block and limit the custom actions based on threat identification.



6

Specialized Focus On API Protection

With the rise in API consumption in business and use-cases (IoT, microservices, backend integration, machine-to-machine), bot mitigation on APIs must be executed to protect sensitive data from going to fraudulent botmasters. Spotting malicious behaviour on APIs can vary from the web and mobile applications, demanding smart distinction between 'good' and 'bad' API calls.

Check the following:

- Does the solution ensure the safety of data transactions through APIs or a generic approach used for websites?
- Does the solution detect authentic access patterns to detect malicious access attempts?
- Can the bot mitigation engine analyze attempts to take over user accounts, scrape data or lead to denial-of-service?

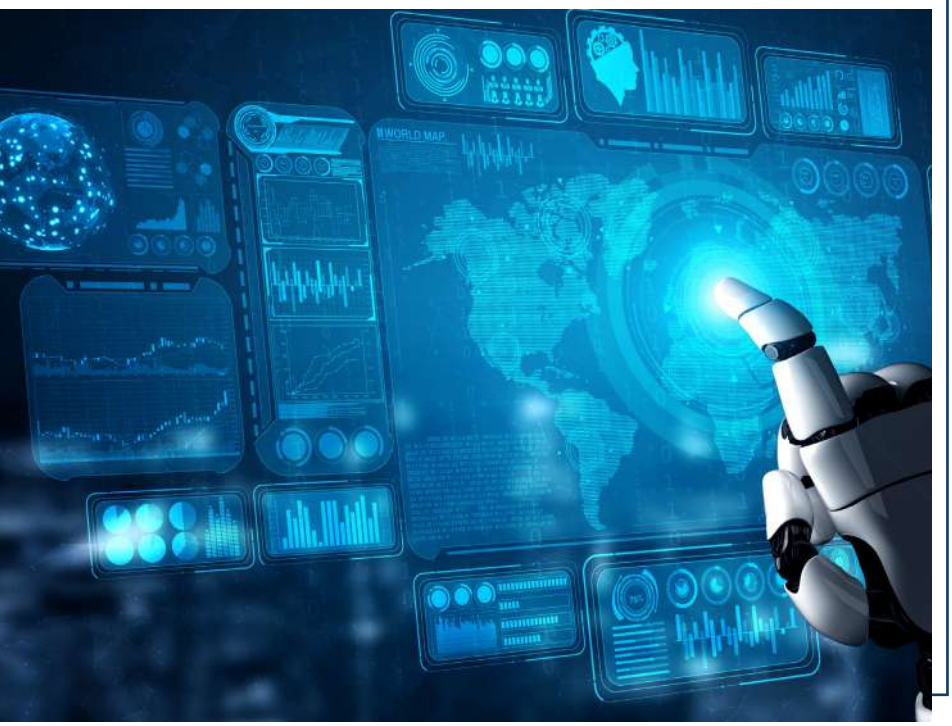
7

Deployment Flexibility

Each network is unique.

Check the following:

- To which extent can the solution cater your network's unique needs?
- Can the solution be deployed exactly the way you need it? Search for a bot management solution that is easier to handle, and completes deployment without infrastructure changes or the risk of rerouting traffic
- Does your architecture need an in-line solution or something out-of-the-box?
- Do you prefer to detect & mitigate or just detect & notify?
- Make sure to check out the options which can be stand-alone or integrated with WAF for complete coverage.



8

Clean, Feature-Rich Reporting For Optimal Visibility

Reporting is a crucial aspect of any bot management tool. Contemplate how every solution provides reporting information. Having access to granular reports could be crucial, yet too much information could be hidden about what you are searching for.

Check the following:

- Can it offer clean, easy-to-understand reporting? It must show granular details such as total bot requests, total bot bandwidth usage, total requests, total bandwidth usage, and bot classification based on Data Center IP, Anamoly Behaviour Detection, IP Reputation, User Agent Based Detection, TOR IP, etc.
- Does it provide custom controls?

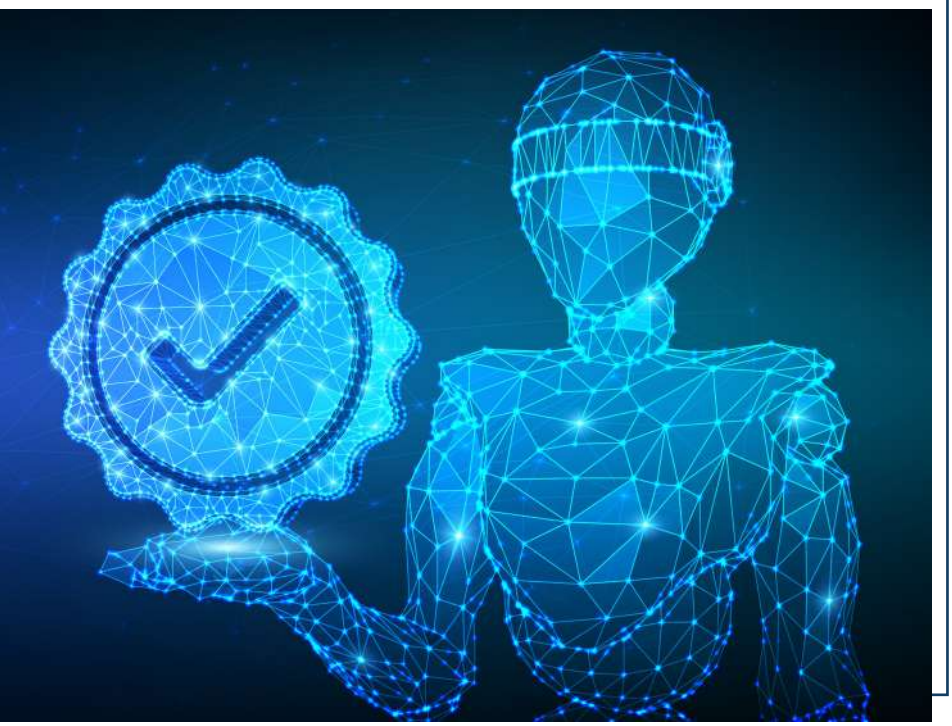
9

Governance And Compliance Factors

For several organizations, applications and supporting data must be present in their most valued assets.

Check the following:

- Does the bot weakening solution guarantee that traffic does not withdraw from a network?
- If it does, transform this data into an encrypted and hashed format to intensify privacy and compliance.
- Make sure the bot reduction solution is adaptable to the General Data Protection Regulation (GDPR) regarding data at rest and data in transit to prevent personal data breaches and the risk of financial and legal penalties.
- Similarly, is it PCI, SOC, ISO27001 compliant?



10

Analyst Reviews

For any robust bot management solution, a good indicator of its capabilities and value in the market would be recognition from 3rd-party, respected, and established business research and consulting firms.

Check the following:

- Is the vendor/bot management solution rated by Gartner in its latest Voice of Customer Report or Magic Quadrant for web application and API Protection?

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 2000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 and several other such prestigious recognitions.

CONTACT US - +91 265 6133021 | +1 866 537 8234

EMAIL - sales@indusface.com

Gartner Peer Insights Customers' Choice 2022™

Indusface is the Only Vendor To Be Named Gartner® Peer Insights™ Customers' Choice in All the 7 Segments of the Voice of Customer WAAP 2022 Report.