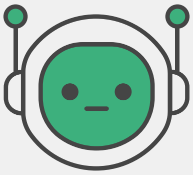
SERVICE BRIEF

Protect Digital Assets with the FortiGuard Advanced Bot Protection Service

Executive Summary

A substantial portion of automated traffic or bots are designed to carry out nefarious attacks like credential theft, web scraping, fraud, and denial of service. These advanced bots often evade older defenses when targeting digital assets by mimicking real user behavior. Organizations that fail to detect and thwart these attacks can suffer financial losses, data breaches, website crashes, and brand reputation damage.

As malicious bots grow in sophistication, defenses need to as well. Protecting applications from bot-related threats requires continuous learning about bot behaviors and the ability to correlate between patterns of bot activities. Reactive methods like basic CAPTCHA tests, IP blacklisting, and even device fingerprinting are no longer sufficient. Defending against bots requires advanced techniques, such as behavioral analysis, machine learning (ML), biometric indicators, and threat intelligence. The FortiGuard Advanced Bot Protection Service enhances the Fortinet web application and API protection solution set with these capabilities to defend against bot attacks.



A recent report found that 47.4% of all internet traffic came from bots, a 5.1% increase from 2021. During the same period, human traffic fell to 52.6%, reaching an eight-year low. And traffic from bad bots increased for the fourth consecutive year, reaching 30.2%.[1]

The Challenges Posed by Malicious Bots

The proliferation of bots on the internet is a threat to organizations because they can be programmed for malicious purposes, such as fraud, data theft, content scraping, account takeover, and distributed denial-of-service (DDoS) attacks. As bots become more sophisticated and can mimic real user behaviors, it is critical to accurately distinguish between bots and real users.

Whether hosted locally or in the cloud, traffic from the Internet to an application comprises humans and bots. Bots can be either legitimate programs or have malicious intent, so it's essential to accurately classify bot traffic based on intent analysis. Legitimate bots such as search engine crawlers, chatbots, data aggregators, and other robotic process automation programs should be allowed through the organization's defenses, while malicious ones must be detected and blocked.

To meet data privacy standards, many organizations also must be able to protect internet-facing applications and network infrastructure from data theft and unnecessary load. The ultimate goal is to protect digital assets from a spectrum of automated threats while securing the user experience, online revenue streams, and intellectual property.

Detect and Mitigate Bot Attacks with FortiGuard Advanced Bot Protection

FortiGuard Advanced Bot Protection Service features sophisticated techniques to detect and mitigate malicious bot attacks while allowing legitimate traffic through. Delivered as Software-as-a-Service (SaaS) with continuously updated datasets, it is easily deployed as a standalone solution or an integrated add-on to FortiADC or FortiWeb. The Advanced Bot Protection Service collects telemetric data by injecting JavaScript code into the client. It then analyzes multiple behavioral indicators to identify the intent of the bot. Based on this analysis, the service determines a risk score fed back into the application. The Advanced Bot Protection Service helps defend against bot threats using:

- **IP reputation database:** Maintains a real-time database of known or suspicious IP addresses associated with bots and blocks traffic from them
- **Browser fingerprinting:** Creates unique fingerprints for each visitor by looking at various browser and device attributes to recognize repeat offenders
- **Biometric detection**: Analyzes visitor device interactions, such as mouse movements, scrolling behavior, and other human-like patterns to determine if a user is a real human or a bot

- **ML models:** Uses artificial intelligence (AI) to train models on vast datasets and continuously improve and refine bot detection capabilities
- **Real-time threat intelligence (AI score):** Leverages global threat intelligence to stay abreast of new and emerging bot threats and update protections
- **Comprehensive analytics:** Provides detailed bot traffic analytics and attack forensics to enhance understanding of bot patterns and strategies
- **Integration with FortiADC and FortiWeb:** Allows FortiADC and FortiWeb to send telemetry data to the bot protection system, providing deeper insights into sophisticated bots for more accurate detection and blocking

Secure Online Revenue and Keep Data Safe

Organizations must protect their applications from sophisticated bot attacks to continue to earn online revenue and preserve the user experience. The FortiGuard Advanced Bot Protection Service distinguishes between good, bad, and real users. The solution is designed to provide precise detection across web, mobile, and APIs while minimizing false positives and negatives. FortiGuard Advanced Bot Protection allows users to monitor and block malicious bot behaviors, such as account takeover, web scraping, data theft, and fraud.

The ML algorithms used by the FortiGuard Advanced Bot Protection Service continuously monitor and study sophisticated bot behaviors to deliver maximum protection and detection accuracy.

One of the key benefits of FortiGuard Advanced Bot Protection is that beyond enhancing application delivery and web application security capabilities, it can also be integrated into the Fortinet Security Fabric, which provides centralized management, visibility, and consistent security wherever applications are located. FortiGuard Advanced Bot Protection offers:

- A minimal footprint and low latency thanks to the Fortinet global infrastructure
- Easy deployment as a SaaS component collecting telemetric data using JavaScript
- Visibility for network and security operations teams
- Integration with additional services from Fortinet that can be bundled to deliver comprehensive application security

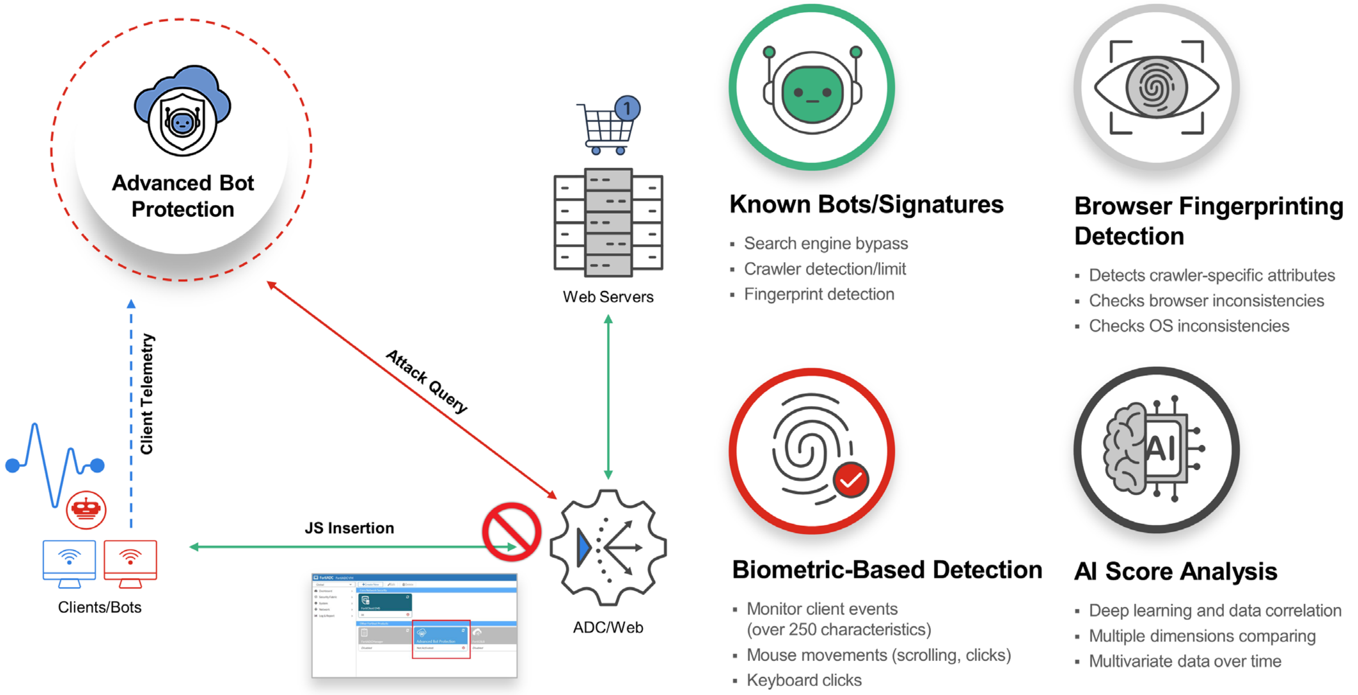

Advanced Bot Protection
Client Telemetry
Attack Query
Web Servers
1
JS Insertion
Clients/Bots
ADC/Web
Known Bots/Signatures
Search engine bypass
Crawler detection/limit
Fingerprint detection
Browser Fingerprinting Detection
Detects crawler-specific attributes
Checks browser inconsistencies
Checks OS inconsistencies
Biometric-Based Detection
Monitor client events (over 250 characteristics)
Mouse movements (scrolling, clicks)
Keyboard clicks
AI Score Analysis
Deep learning and data correlation
Multiple dimensions comparing
Multivariate data over time
AI

Figure 1: The FortiGuard Advanced Bot Protection Service

Effective Protection against Bot Attacks

Malicious bots are more pervasive and sophisticated than ever, so it is more difficult for older security solutions to detect and block them. Organizations need solutions that distinguish between good and bad bots and between bots and human users. Today, effective bot protection technology must combine advanced detection and mitigation techniques with continuous updates to protect against attacks. As a SaaS bot solution, FortiGuard Advanced Bot Protection secures digital assets and activities while optimizing resource investments. Learn more about securing the application journey from end to end using Fortinet solutions.

[1] CPO Magazine, Bad Bots Account For 30% Of Internet Traffic and Are More Frequent in Account Takeover and API Attacks, May 30, 2023.

December 30, 2023 3:02 PM
2489260-0-0-EN