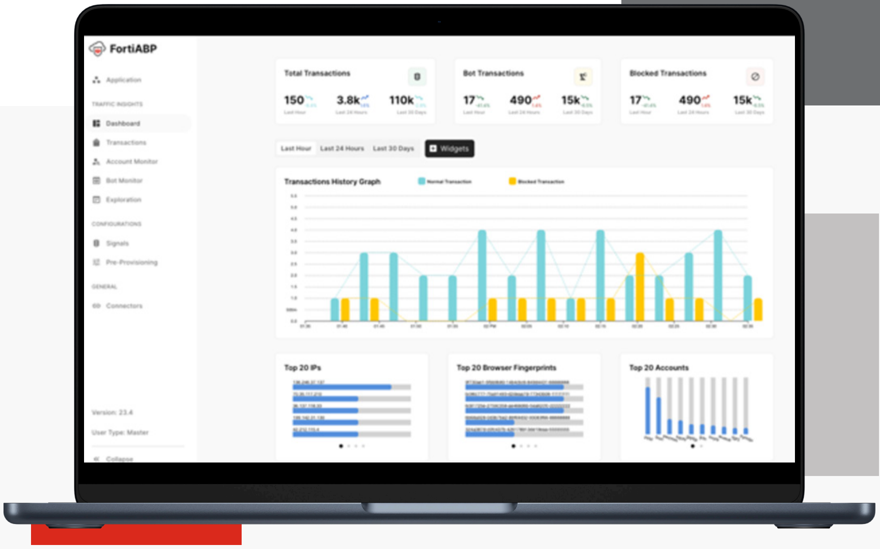
FORTINET

Data Sheet

FortiGuard Advanced Bot Protection™



Total Transactions: 150 (Last Hour), 3.8k (Last 24 Hours), 110k (Last 30 Days)

Bot Transactions: 17 (Last Hour), 490 (Last 24 Hours), 15k (Last 30 Days)

Blocked Transactions: 17 (Last Hour), 490 (Last 24 Hours), 15k (Last 30 Days)

Highlights

- **Advanced Bot Detection**: Accurately identifies and mitigates known and unknown bot threats using advanced techniques
- **Seamless Integration**: Easily integrates with FortiADC and FortiWeb or functions as a standalone service for flexibility
- **Customizable Rules**: Allows customization of bot detection rules to adapt to evolving threats
- **Action Flexibility**: Provides granular control over bot mitigation actions for optimal security and user experience

Safeguard Your Digital Ecosystem from Automated Threats

In today's digital landscape, the proliferation of bots presents a significant threat to organizations across various industries. Bots, automated software applications, can be programmed for malicious purposes, including fraud, data theft, content scraping, account takeover, and distributed denial-of-service (DDoS) attacks. In fact, recent studies show bad bots account for ~ a quarter of internet traffic. In addition, as bots become increasingly sophisticated, mimicking real user behaviors, organizations need to shore up their bot management capabilities to protect data, business continuity, and user experience.

Fortinet FortiGuard Advanced Bot Protection

For organizations looking to protect applications and APIs from sophisticated bot attacks and secure online revenue generation and user experience, FortiGuard Advanced Bot Protection integrates with FortiWeb and FortiADC for secured application delivery. It prevents account takeover, web scraping, data theft, and fraud by machine learning and behavioral-based indicators.

Capabilities

Biometric-based Detection

FortiGuard Advanced Bot Protection leverages state-of-the-art biometric-based detection algorithms to accurately differentiate between human users and automated bots. By analyzing unique biometric attributes, such as keystroke dynamics, mouse movements, and touch interactions, our solution effectively identifies and blocks malicious bot activity while allowing genuine users seamless access.

Monitor Client Events

Closely monitors client-side events, including mouse movements (scrolls, clicks) and keyboard clicks, to detect suspicious behavior patterns associated with bot activity. By analyzing these events in real-time, FortiGuard Advanced Bot Protection effectively mitigates various automated threats, such as click fraud and content scraping, ensuring the integrity of your web applications.

Device Fingerprinting

FortiGuard Advanced Bot Protection creates a comprehensive profile of each user's device using advanced device fingerprinting techniques, including multiple hardware and software attributes. This enables accurate identification of malicious bots attempting to impersonate legitimate users, allowing you to block them proactively and safeguard your web assets.

Detecting Crawler-Specific Attributes

FortiGuard Advanced Bot Protection utilizes advanced algorithms to detect crawler-specific attributes, such as user agent strings and HTTP header information. Our solution identifies and distinguishes between legitimate search engine crawlers and malicious bots by analyzing these characteristics, providing granular control over bot access.

Checking Browser and OS Inconsistencies

Examines browser and operating system (OS) inconsistencies exhibited by users, identifying potential bot activity. FortiGuard Advanced Bot Protection effectively blocks bots attempting to exploit vulnerabilities in outdated browsers or fraudulent OS versions by comparing user-agent strings, screen resolutions, and other attributes.

Bot Rules Analysis

FortiGuard Advanced Bot Protection offers a robust bot rules analysis engine, allowing you to define custom rules to identify and mitigate specific bot behaviors. With extensive rule customization options, our solution enables fine-tuning bot detection policies, ensuring optimal protection against known and emerging threats.

Historical Analytics

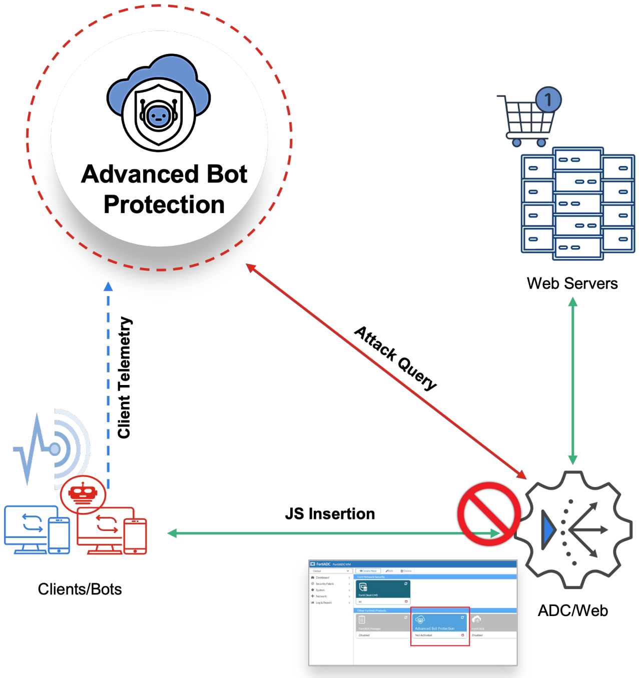
FortiGuard Advanced Bot Protection provided comprehensive historical analytics on HTTP attempts, including success and failed counts over time. By visualizing bot activity trends, you gain valuable insights into attack patterns, allowing you to enhance your security posture and proactively adapt your mitigation strategies.

Action

FortiGuard Advanced Bot Protection empowers you with various flexible measures to respond to bot threats effectively. Whether allowing legitimate users seamless access, blocking malicious bots, or employing CAPTCHA challenges for suspicious activity, our solution offers granular control over bot mitigation actions to suit your specific security requirements.

Security Fabric

FortiGuard Advanced Bot Protection delivers broad protection and visibility to FortiADC/FortiWeb, whether virtual, in the cloud, or on-premises. It can automatically synchronize security actions to enforce policies and coordinate automated responses to threats detected anywhere in your web application.



Known Bots / Signatures

- Search Engine Bypass
- Crawler Detection/Limit
- Fingerprint Detect

Browser Fingerprinting Detection

- Detecting Crawler-Specific Attributes
- Checking Browser Inconsistencies
- Checking OS Inconsistencies

Biometric-based Detection

- Monitor client events (over 250 characteristics)
- Mouse movements (scroll, clicks)
- Keyboard clicks

AI Score Analysis

- Deep Learning and Data Correlation
- Multiple Dimensions Comparing
- Multivariate data over time

Deployment

Seamless Integration with FortiADC and FortiWeb

FortiGuard Advanced Bot Protection seamlessly integrates with FortiADC and FortiWeb, strengthening your overall security infrastructure and providing enhanced bot mitigation capabilities. Here's how the integration works:

Traffic Flow and JS insertion
Traffic flows from the client to the web application through the FortiADC/FortiWeb, which acts as a reverse proxy. This allows FortiADC/FortiWeb to intercept and inspect incoming requests, providing an additional layer of security before they reach your web applications.

Telemetric Information
The client and the FortiADC/FortiWeb (using the fabric connector) sends telemetric information to the FortiGuard Advanced Bot Protection, which helps gather relevant data about client interactions, device fingerprinting, and other comprehensive analyses to detect bot activity.

Data Analysis
FortiGuard Advanced Bot Protection analyzes incoming requests to determine whether the client is a human or a bot. By leveraging sophisticated algorithms and data telemetry information, FortiGuard Advanced Bot Protection accurately evaluates the nature of the request and identifies potential bot activity.

Action
Based on the analysis results, FortiGuard Advanced Bot Protection sends instructions back to FortiADC/FortiWeb. These instructions guide handling the request, including whether to block, display a Captcha challenge, or allow the request to proceed.

This integration enables real-time analysis and decision-making, ensuring adequate protection against bot threats while allowing legitimate traffic to access your web applications seamlessly.

Key Advantages

Comprehensive Bot Protection

FortiGuard Advanced Bot Manager combines a multitude of advanced detection techniques, including biometric-based detection, device fingerprinting, and crawler-specific attribute analysis. This holistic approach ensures robust protection against known and unknown bots, minimizing the risk of fraud, data breaches, and service disruptions.

Enhanced User Experience

By accurately distinguishing between bots and legitimate users, our solution optimizes user experience by minimizing false positives and false negatives. This ensures frictionless access for genuine users, improving customer satisfaction and engagement while maintaining strong security.

Easy Integration

FortiGuard Advanced Bot Manager seamlessly integrates with FortiADC/FortiWeb, enhancing the security capabilities of your existing infrastructure. Alternatively, it can be deployed as a standalone service on your web server, providing flexibility and scalability to meet your organization’s unique requirements.

Customizable and Adaptive

Our solution offers extensive customization options, allowing you to tailor bot detection rules, actions, and thresholds to align with your specific security policies. Moreover, FortiGuard Advanced Bot Manager continuously evolves to adapt to emerging threats, providing ongoing protection and peace of mind.

Ordering Information

Product	SKU	Description
FortiGuard Advanced Bot Protection	FC1-10-BMCLD-726-01-DD	FortiGuard Advanced Bot Protection - 10M requests/month. Annual Subscription (standalone purchase).
	FC2-10-BMCLD-726-01-DD	FortiGuard Advanced Bot Protection. Add-on 1M requests/month Annual Subscription. Must first purchase standalone FC1-10-BMCLD-726 SKU.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

November 30, 2023