
radware

RADWARE BOT MANAGER - USER GUIDE

Overview of Radware Bot Manager

In recent years, automated attacks have threatened almost every industry. Competitors and fraudsters deploy human-like bots that attack your website, mobile apps, and APIs to commit automated attacks such as account takeover, gift card fraud, web scraping, digital ad fraud and form spam. Fraudsters deploy thousands of bots on your web properties to perform large-scale distributed attacks that are often 'low and slow' to go unnoticed by conventional defenses such as Web Application Firewalls (WAFs). Such automated attacks affect customer experience, tarnish a brand's reputation, skew analytics and cause loss of revenue.

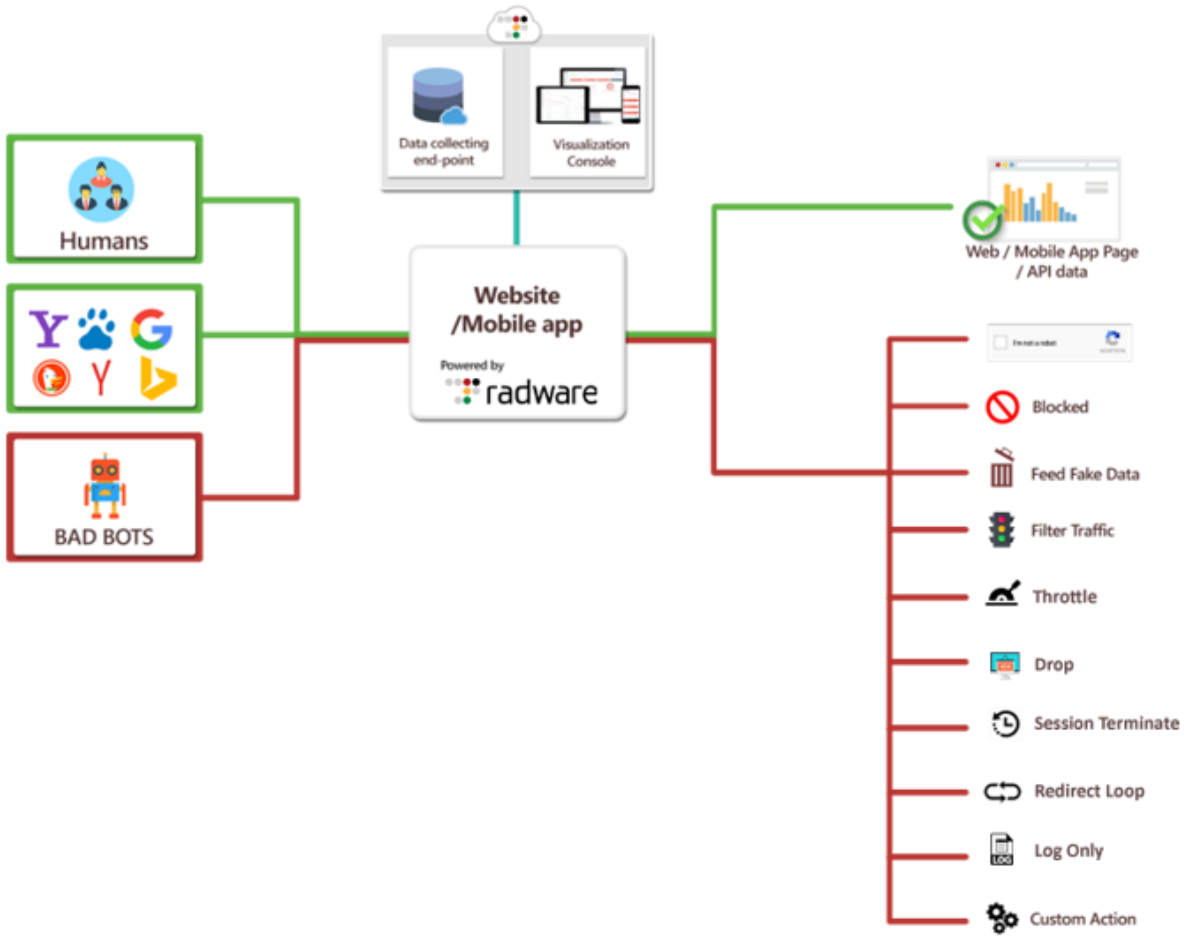
Radware Bot Manager's non-intrusive API-based approach detects and blocks highly sophisticated humanlike bots in real time. Our bot detection engine uses proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent of visitors and filter sophisticated invalid traffic. We collect over 250 parameters including browsing patterns, mouse movements, keystrokes, and URL traversal data points from the end user's browser and use proprietary algorithms to build a unique digital fingerprint of each visitor. Our collective bot intelligence gathers bot signatures from across our client base (i.e., over 80,000 internet properties) to build a database of bot fingerprints and proactively stop bots from infiltrating into your internet properties.

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019.

We protect you from:

- Account Takeover
- Application DDoS
- API Abuse
- Price Scraping
- Content Scraping
- Carding
- Digital Ad Fraud
- Gift Card Fraud
- Skewed Analytics
- Form Spam

How Does Radware Bot Manager defend you?



Integrate Radware Bot Manager via our cloud connectors, web server & CDN plugins, or virtual-appliance. Radware Bot Manager proactively acts behind the scenes when a visitor visits a page on your website or mobile app.

- As and when a page visit happens, Radware Bot Manager's API call and JavaScript embedded on the page collects and shares various parameters about the visitor with the Radware Bot Manager Engine. Using proprietary technologies, Artificial Intelligence, and Machine Learning, the Radware Bot Manager engine builds a unique fingerprint for each visitor and bot.

- Based on the exhaustive bot detection tests done on the visitor's activity, our cloud engine classifies the visitor as a human, search engine crawler, or a bad bot. Based on the classification, if the visitor is a friendly entity (human or search engine crawler), then Radware Bot Manager transparently allows the user to pass through by sending the API response code as Allow. All of this is achieved in a few milliseconds without impacting user experience.

- In the event of a bad bot, Radware Bot Manager sends the corresponding response code back to the application. Based on the response codes, you can implement actions like blocking the bot, serving a CAPTCHA, feeding fake data, etc. Radware Bot Manager, thus covers all routes and provides you the flexibility to choose a desired response to act against bots as per your business needs.
- CAPTCHA feedback mechanism helps ML modules fine-tune thresholds.

Key Features:

- Proprietary Intent-based Deep Behavioral Analysis leverages collection of ML modules
- Battle-tested for zero false positives
- No DNS traffic rerouting
- High Performance
- Easy Integration
- Secured user privacy
- Exhaustive out-of-the-box reporting

Visit the Radware Bot Manager website to know more about the product