

Prevent Automated Attacks on Websites, Mobile Apps and APIs

Over half of all internet traffic is generated by bots — some legitimate, some malicious. Competitors and adversaries alike often deploy “bad” bots that leverage different methods to achieve nefarious objectives. This includes account takeover, scraping data, denying available inventory and launching denial-of-service attacks with the intent of stealing data or causing service disruptions. Sophisticated, large-scale attacks often go undetected by conventional mitigation systems and strategies. Leveraging proprietary, semisupervised machine learning capabilities, Radware’s Bot Manager allows precise bot management across all channels, combining behavioral modeling for granular intent analysis, collective bot intelligence and device fingerprinting.



INTENT-BASED DEEP BEHAVIORAL ANALYSIS (IDBA)

Identify the intent of bots with the highest precision through proprietary semisupervised machine learning models

FULL COVERAGE OF OWASP AUTOMATED THREATS

Protect from all forms of account takeover, denial of inventory, DDoS card fraud and web scraping



SECURE ALL CHANNELS: WEB & MOBILE APPS, APIs

Defend against bots that target various digital assets — even sophisticated bots designed to hit multiple assets

NONINTRUSIVE APPROACH

Detect and block highly sophisticated humanlike bots in real time using APIs or an out-of-path mode — all with no impact to the technology stack



Protection From a Wide Array of Threats



Account Takeover

Credential stuffing and Brute Force attacks are used to gain unauthorized access to customer accounts.

Content Scraping

Scammers and third-party aggregators use bots to scrape content and illegally reproduce the stolen content on ghost websites.



Gift Card Fraud

Carders use bots to crack gift cards and identify valid coupon numbers and voucher codes.

Digital Ad Fraud

Malicious bots create false impressions and generate illegitimate clicks on publishing sites and their mobile apps.



Application DoS

Application DoS attacks degrade web applications by exhausting system resources, third-party APIs, inventory databases and other critical resources.

Skewed Analytics

Automated traffic on your web property skews metrics and misleads decision-making.



Price Scraping

Competitors deploy bots on your website to steal price information and influence your customers’ buying decisions.

Form Spam

Malicious bots deluge online marketplaces and community forums with spam leads, comments and fake registrations.



Key Features

▶ Ability to Handle Bot Traffic in Multiple Ways

Actions are customized based on bot signatures/types, e.g., feeding false pricing and product information to competitors' bots. Radware uses CAPTCHA for suspected bots, leveraging responses in a closed-loop feedback system to minimize false positives.

▶ Transparent Reporting and Comprehensive Analytics

Granular classification and reporting of different types of bots, such as search engine crawlers and malicious bots, enable efficient traffic management. Radware's Bot Manager can be seamlessly integrated with leading analytics platforms, including Google and Adobe Analytics.

▶ Easy Integration

Flexible deployment options include integration via our JavaScript tag, cloud connectors or web server plug-ins. Alternatively, a virtual appliance is available too, for the entire web app or selected sections. This allows for easy deployment of Bot Manager into your existing infrastructure.

▶ No DNS Redirection

Using an API-based approach to protect web assets, the solution doesn't require DNS redirection, thus allowing complete control over web applications, mobile apps and APIs.

▶ Accuracy and Scalability

IDBA filters highly sophisticated humanlike bots without causing false positives. Website functionality and user experience remain intact. Bot Manager leverages cutting-edge technologies to maintain high scalability during peaks in network traffic.

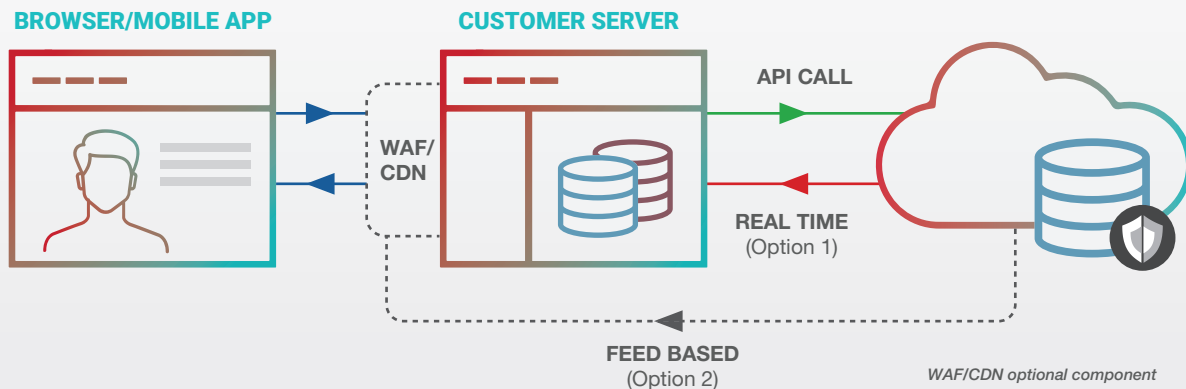


Figure 1: Diagram of Radware's Bot Manager

Radware's Attack Mitigation Solution

Radware's Bot Manager integrates with Radware's Attack Mitigation Solution (AMS) to offer the industry's most advanced protection from sophisticated, automated attacks. Radware's solution provides complete network and application security protection via a fully integrated system that synchronizes premise- and cloud-based solutions to protect organizations from a variety of threats, such as web application attacks, denial of service, malicious bots and advanced malware. Radware's AMS features proven, patent-protected machine learning capabilities, advanced automation and real-time intelligence sharing for maximum security at minimum false positives and latency.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.