radware

Bot Manager Data Sheet

Gartner Cool Vendor 2018

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 (DoS) 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 web and mobile applications and application programming interfaces (APIs), 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, distributed denial of service (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

FLEXIBLE INTEGRATION OPTIONS

Nonintrusive deployment using SDK, web server or content delivery network (CDN) plug-ins, JavaScript (JS) tag or as a reverse proxy — no impact on 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.

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

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

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

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

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

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

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 JS tag, cloud connectors or web server plug-ins. Alternatively, a virtual appliance is also available for the entire web app or selected sections. Using Radware's API-based approach, Domain Name System (DNS) redirection is not mandatory, so deployment into the existing application stack is easy and seamless.
- **Accuracy and Scalability —** IDBA filters highly sophisticated humanlike bots without causing false positives. Website functionality and user experience remain intact. Radware's Bot Manager leverages cutting-edge technologies to maintain high scalability during peaks in network traffic.
- **Fully Managed Service —** Radware's Bot Manager is also available as a security service integrated with Radware's Cloud web application firewall (WAF) for complete 360° application protection.
- **Dedicated API Protection —** Ability to control navigation flow and fingerprint M2M communications to avoid invoking APIs that are accessed or targeted by misbehaving bots.
- **Complete Application Security Suite —** Includes a WAF, a bot manager, API security and DoS mitigation brought together to provide the most robust application protection.

API Protection From Malicious Bots

API Flow Control — Protect machine-to-machine & internet of things (IoT)

Invocation Context — Protect web and mobile APIs

API Client SDK — Unique source identification to secure M2M communication

Authentication Flow — ATO protection for APIs from sources failing to log in

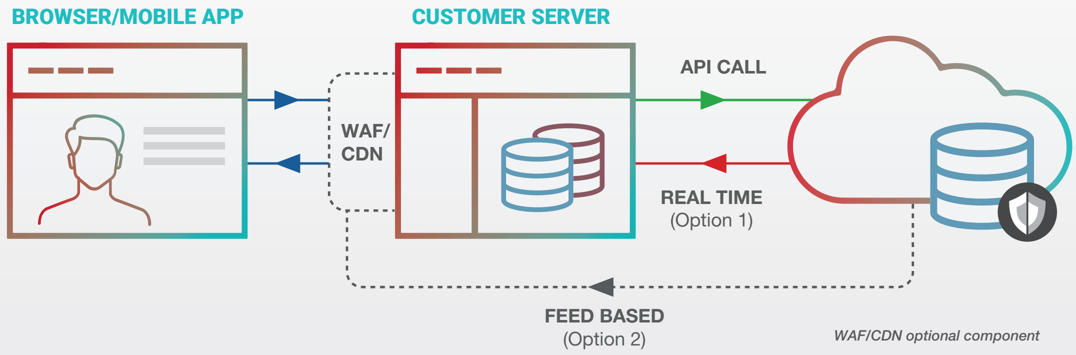

Figure 1: Diagram of Radware's Bot Manager Workflow

Radware's Complete Application Security Suite

Radware offers the industry's most advanced application protection with a WAF, bot manager, API protection and DDoS mitigation. Radware's solution set provides complete network and application protection on-premise and in the cloud. We protect organizations from a variety of threats, such as injections, cross-site scripting (XSS), unauthorized access, account takeover, web scraping and denial of service. Radware features proven, patent-protected machine learning capabilities, advanced automation and real-time intelligence sharing for maximum security with 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.