REAL-TIME BOT MITIGATION AND MANAGEMENT

PREVENT AUTOMATED ATTACKS ON WEBSITE, MOBILE APPS, AND APIS

> "We onboarded Bot Manager in the midst of our peak season, and saw immediate results/benefits. Our customers' experiences are our top priority. By working with Radware, we are able to better secure and improve the shopping experience."
>
> *– DANIEL PADEVET, HEAD OF WEB & IT OPERATIONS TEAM, ALZA.CZ*

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 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 human-like 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.

We Protect You From

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 slow down web applications by exhausting system resources, 3rd 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

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

Digital Ad Fraud

Bad 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

Intent-based Deep Behavioral Analysis

A large number of sophisticated attacks are either massively distributed or adequately 'low and slow' to operate under the permissible limits of rule-based security measures. We use proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent of highly sophisticated non-human traffic. IDBA performs behavioral analysis at a higher level of abstraction of 'intent' unlike the commonly used shallow 'interaction'-based behavior analysis. Capturing intent enables IDBA to provide significantly higher levels of accuracy while detecting bots with advanced human-like interaction capabilities. IDBA builds upon Radware Bot Manager's research findings in semi-supervised machine learning and leverages the latest developments in deep learning.

Ability to Handle Bot Traffic in Multiple Ways

The aggregators and competitors continuously target your web properties to scrape price, content and other business-critical information. We allow you to take custom actions based on bot signatures/ types. You can outsmart competitors using our 'feed fake data' method that enables you to feed fake pricing and product information to the bots deployed by competitors. Our system shows challenges such as CAPTCHAs to suspected non-human traffic. The responses to these challenges help us build a closed-loop feedback system to minimize false positives down to negligible values. Our bot mitigation solution allows publishers to show ads only to humans, and block non-human invalid traffic before pages load.

Transparent Reporting, and Comprehensive Analytics

Transparency in traffic reports helps you build trust with internal stakeholders and partners. A granular classification of different types of bots such as search engine crawlers and malicious bots allows you to efficiently manage non-human traffic. Clean analytics and transparent reports offer a clear understanding of web traffic and give you a detailed picture of bots' intent on your internet properties. We provide you with comprehensive analytics of non-human traffic, their source, and URL analytics. One of the key benefits of our bot detection engine is its modularity and transparency in reports — this is particularly useful for automated threats such as digital ad fraud. Our analytics dashboard demonstrates the distinctive user behavior on your site. Our bot mitigation solution can be seamlessly integrated with leading analytics platforms including Google Analytics and Adobe Analytics.

Easy Integration

Radware Bot Manager provides easy and flexible deployment options that suit your business requirements. You can integrate our JS tag, cloud connectors, or web server plugin into your existing infrastructure in minutes. Alternately, you can also opt for our virtual appliance. We also allow you to integrate our solution into specific sections of your website based on requirements, instead of the entire web application.

No DNS Redirection

DNS rerouting techniques add a risk factor for business-critical enterprise applications — if the DNS is down, so does your business. Radware Bot Manager uses an API-based approach to protect your web properties. Our solution doesn't require DNS redirection. Radware Bot Manager eliminates this external dependency by giving you complete control over your web applications, mobile apps, and APIs.

Accuracy and Scalability

Detecting advanced bots based on shallow interaction characteristics results in a high number of false positives. Our Intent-based Deep Behavior Analysis helps you filter highly sophisticated human-like bots without causing false positives. We also ensure that website functionality and user experience remain intact. We use cutting-edge technologies such as Kubernetes container orchestration and Kafka to maintain high scalability during peak hours.

How Radware Bot Manager Works

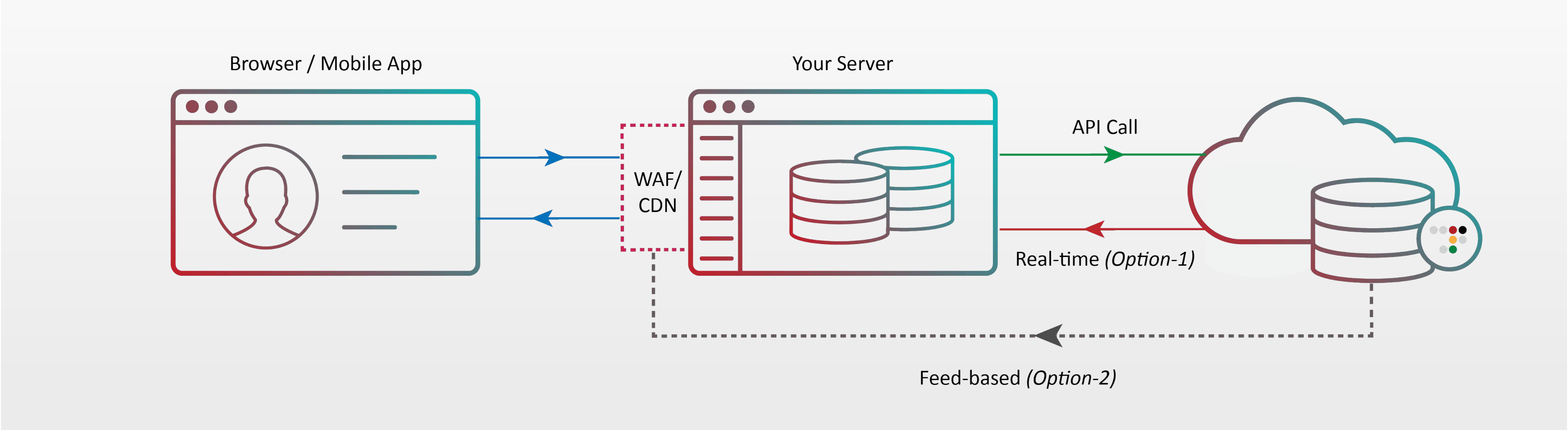
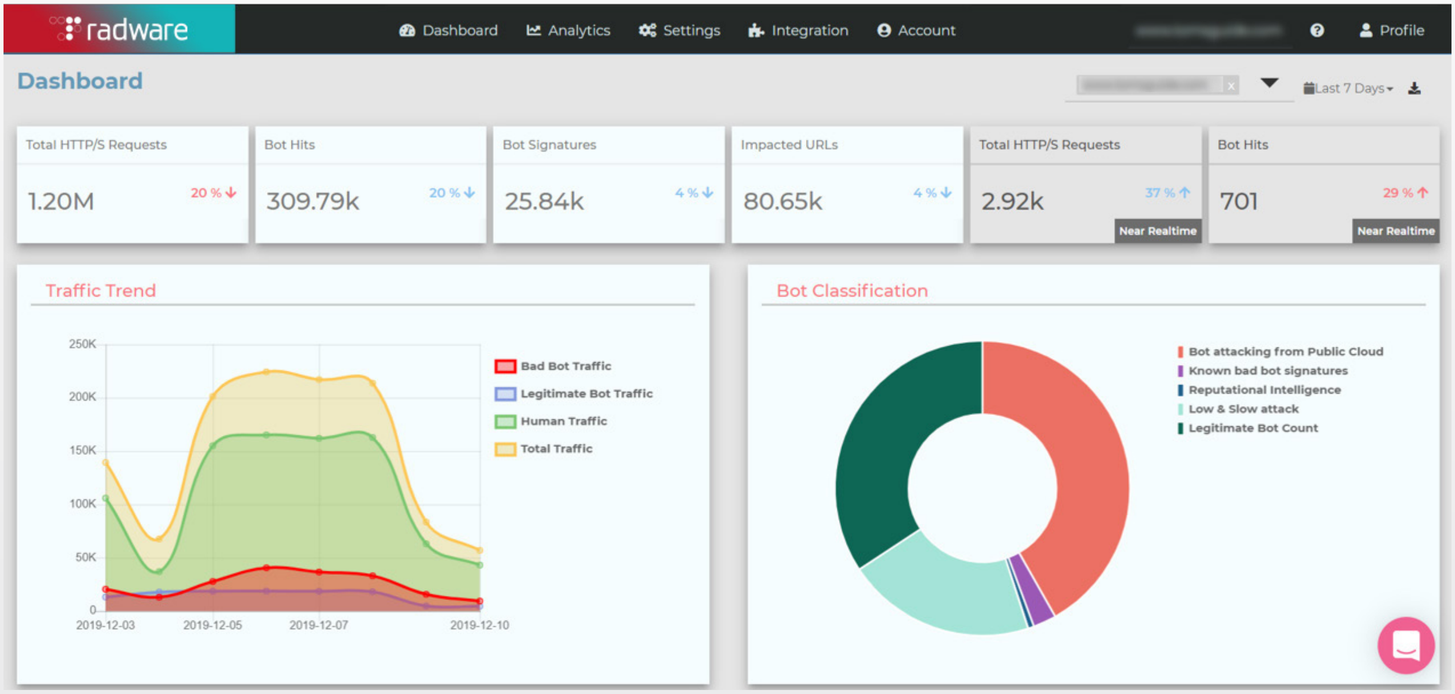


Figure 1: Diagram of Radware's Bot Manager

Traffic Analysis



Total HTTP/S Requests 1.20M 20 % ↓

Bot Hits 309.79k 20 % ↓

Bot Signatures 25.84k 4 % ↓

Impacted URLs 80.65k 4 % ↓

Total HTTP/S Requests 2.92k 37 % ↑ Near Realtime

Bot Hits 701 29 % ↑ Near Realtime

Figure 2: Diagram of Radware's Bot Manager Traffic Analysis

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, Radware Mobile for iOS and Android, and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

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 thi document. The technologies, functionalities, services or processes described herein are subject ro change without notice.