Real-time Bot Mitigation and Management

Prevent Automated Attacks on Websites, Mobile Apps, and APIs

The Challenge in Potecting against Bot Attacks

In recent years, automated attacks have threatened almost every industry. Competitors and fraudsters deploy bots that can mimic human browsing behavior to visit your website, mobile apps, and APIs and commit automated attacks such as account takeover, credit/gift card fraud, content and price scraping, digital ad fraud, form spam, and more. Attackers deploy thousands of bots on your web properties to perform large-scale distributed attacks that are often 'low and slow' to evade conventional defenses. Such automated attacks affect customer experience, tarnish a brand's reputation, skew analytics and cause loss of revenue.

Radware Bot Management Solution

Radware Bot Manager's non-intrusive API-based approach detects and blocks highly sophisticated human-like bots in real time. Its bot detection engine uses proprietary Intent-based Deep Behavior Analysis (IDBA) to understand the intent of visitors and filter sophisticated invalid traffic.

Radware Bot Manager collects over 250 parameters including browsing patterns, mouse movements, keystrokes, and URL traversal data points from the end user's browser and uses 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:

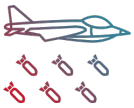
OWASP Top 21 Automated Threats

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 (Denial of Service) attacks slow down web applications by exhausting system resources, 3rd party APIs, inventory databases, and other critical resources

Digital Ad Fraud:

Bad bots create false impressions and generate illegitimate clicks on publishing sites and their mobile apps, depriving advertisers and publishers of their revenue.

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.

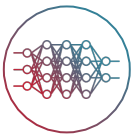
Price and Content Scraping:

Competitors deploy bots on your website to steal price information and influence your customers' buying decisions. Fraudsters, copycat sites and third-party aggregators use bots to scrape your valuable original content and illegally reproduce it on ghost websites, which can lower your search engine rankings.

Integration Options

- CDN
- App Server SDKs
- DNS Diversion
- Other Third-party Integrations
- Web Server Plugins
- ADC
- On-premise Sensor

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:

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.

Transparent Reporting and Comprehensive Analytics:

Radware Bot Manager provides granular classification of different types of bots such as search engine crawlers and malicious bots to allow 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 JavaScript tag, cloud connectors, or web server plugin into your existing infrastructure in minutes. Alternately, you can

opt for our virtual appliance and mobile SDKs. We also allow you to integrate our solution into specific sections of your website based on requirements, instead of the entire web application.

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.

Widest Mitigation Options:

Radware Bot Manager has the widest mitigation option available to its users, and now with Crypto Challenge, Radware Bot Manager adds another mitigation option to stop sophisticated bot attacks, while providing a CAPTCHA-less mitigation option with Blockchain-based Cryptographic Proof of Work.

CAPTCHA-less Mitigation:

Blockchain based Crypto Challenge is a behavior-enforcing mechanism that detects anomalies against a baseline of normative behavior. When an anomaly is detected, the mitigation method challenges the user device by creating CPU-intensive browser-based challenges with gradually increasing difficulty, forcing the attacker's CPU to work harder every time it is challenged, eventually choking the device, thereby transferring the cost of the attack to the attacker.

Mobile Application Protection Capabilities:

- **Integrated Device Authentication** – Radware Bot Manager SDK includes a one-of-a-kind attestation for Google (Android) and Apple (iOS) devices, for tighter and faster protection of native mobile applications. This unique capability keeps device authenticity in check, making sure only real devices and not emulators, modified applications or modified OS are getting access to your resources.
- **Secure Identity** – This unique solution ensures the security of your client identity (requests to your web application) against identity spoofing, identity tampering, and replay attacks by creating a unique identity for each user against which it validates every request.

Secure Identity along with Google/Apple attestation (Integrated Authentication) provides enhanced protection to your mobile devices and apps and stops bot attacks on mobile apps before they materialize and take a toll on your infrastructure.

Unified Portal:

Radware's Cloud Application Protection portal provides a single interface for all Radware Cloud Application Protection solutions with ease of configuration, granular control options and detailed analytics into all application security events and protection metrics. This 'single pane of glass' view helps you manage your security solutions in a frictionless manner with reduced overheads.

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.

Widest Mitigation Options

- Allow
- Challenge CAPTCHA
- Block
- Feed Fake Data
- Throttle
- Drop
- Session Termination
- Redirect Loop
- Log Only
- Custom Response
- Crypto Challenge

HK-120 | 04.5.2023