Proactive Real-time Bot Mitigation and Management

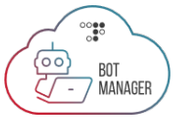
Prevent automated attacks on websites, mobile apps, and APIs.

The Challenge in Protecting Against Bot Attacks

In today's digital landscape, bad bots are everywhere, and automated attacks threaten almost every industry. Competitors and fraudsters deploy bots that can mimic human browsing behavior to visit your website, mobile apps and APIs. They search for vulnerabilities and commit automated attacks such as account takeover, credit/gift card fraud, content and price scraping, digital ad fraud, form spam, denial of inventory attacks and more. Such automated attacks affect customer experience, tarnish a brand's reputation, skew analytics and cause loss of revenue. Moreover, the sheer volume of bot traffic places a strain on application infrastructure, leading to increased costs related to bandwidth consumption, computing power, delivery and CDN services. This not only impacts the financial aspect but also affects the overall performance and efficiency of the organization's digital operations.

Bot Attacks Driven By AI

To make matters worse, hackers are constantly evolving their tactics. They now employ generative AI tools to create sophisticated, zero-day scripts that mimic legitimate human traffic. This poses a significant challenge for traditional bot management solutions that rely on predefined signatures, CAPTCHAs and rate limiting to detect and mitigate bot attacks. As a result, organizations are left vulnerable to these new and increasingly sophisticated threats.



Radware Bot Management Solution

Part of Radware's comprehensive Cloud Application Protection Services, Bot Manager's non-intrusive API-based approach detects and blocks highly sophisticated human-like bots in real time. Its AI-driven behavioral-based detection engine uses hundreds of advanced algorithms to understand the intent of visitors and filter sophisticated invalid traffic.

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.

Proactive Multi-layered Protection

Radware's industry-leading bot management and mitigation solution can accurately detect and distinguish between human traffic, good bots and bad bots. It ensures comprehensive protection of web applications, mobile apps and APIs from sophisticated AI-driven automated threats and bots.

It also provides robust and precise bot management across web, mobile and API traffic by applying an AI-based proactive protection approach that comprises three layers: preemptive protection, behavioral-based detection and advanced mitigation.

1. PREEMPTIVE PROTECTION	2. AI BEHAVIORAL-BASED DETECTION	3. ADVANCED MITIGATION
↗ AI-based Correlation Engine	↗ Rotators	↗ Real-time Signature Generation
↗ ERT Active Attackers Feed	↗ Header Anomalies	↗ Blockchain-based Cryptographic Challenges
↗ JavaScript Challenge	↗ CAPTCHA Farms	↗ Comprehensive Mitigation Options
↗ Android and iOS Attestation	↗ Distributed Traffic Anomalies	
	↗ User Behavior Anomalies	

Fight AI with AI

Radware Bot Manager preemptively blocks unwanted identities, utilizing unique capabilities such as AI-based cross-correlation, JavaScript challenges and mobile attestation for Android and iOS devices. These, along with its proprietary Secure Identity Engine, stop bot attacks on web and mobile apps before they materialize and take a toll on your infrastructure.

The solution employs advanced AI-based technologies such as behavioral modeling for granular intent analysis, behavioral-based detection of sophisticated bot evasion behavior such as rotating IPs and identities, distributed attack detection, machine-learning-based anomaly detection, and browser and device fingerprinting. It is also capable of detecting third-party CAPTCHA-farm services.

↗ AI-Based Correlation Engine

Radware's AI-driven threat analysis algorithms preemptively and automatically block malicious sources across all applications within an account. It prevents incoming bad traffic from overloading your application server and reduces overheads to your applications' infrastructure and security operation management costs. It does so by cross-correlating events between Bot Manager and the web application firewall (WAF) and API protection modules. When it detects malicious activity, it automatically blocks the nefarious source IPs across all applications within the account for a predefined period. Additionally, it provides complete visibility into each blocked source attack story.

Advanced Behavioral Detection Modules

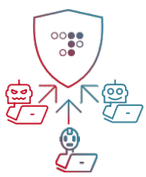
Radware Bot Manager employs proprietary AI-based detection algorithms to combat highly sophisticated non-human traffic that often operates within permissible limits of rule-based security measures. Our Rotator module accurately identifies sophisticated bots that manipulate identities and IPs. By swiftly detecting anomalies across multiple sub-domains within a root domain and deploying automated signatures, it provides robust protection against distributed attacks. This minimizes false positives and bolsters security for various customer account applications. Another example is the advanced behavioral detection module that automatically identifies distributed bot attacks based on traffic anomalies across specific URL endpoints and creates a real-time signature to mitigate that attack.

HTTP Header Anomaly Detection

Sophisticated bad bots typically manipulate the HTTP headers when carrying out their malicious activities. So being able to detect bad bots automatically based on the anomaly in the HTTP headers is a powerful technique to thwart suspicious activity. Radware Bot Manager has now added a new and advanced bot detection module known as an HTTP Header Anomaly. This ML-based module automatically identifies anomalies based on the presence or absence of standard headers and the presence of rare headers.

CAPTCHA Farm Detection Module

To thwart CAPTCHA Farms, Radware Bot Manager decodes signals post-CAPTCHA solving to identify third-party CAPTCHA farm services. It leverages URL analysis, IP reputa¬tion, and user behavior analysis like mouse click patterns and solving times apart from the other signals to detect these third-party CAPTCHA farm services. Once CAPTCHA farm service is detected, Radware Bot Manager can keep the source in a continuous CAPTCHA loop to completely thwart the suspicious activity.



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 offer the widest array of mitigation options and allow you to take custom actions based on bot signatures/types. For example, you can outsmart competitors using our “feed fake data” method, which enables you to feed fake pricing and product information to the bots deployed by competitors. You can also show interactive challenges such as CAPTCHAs to suspected non-human traffic or even use a fully non-interactive challenge like Crypt Challenge. The responses to these challenges help us build a closed-loop feedback system to minimize false positives down to negligible values.

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.

Widest Mitigation Options

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

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. As well, our bot management solution can be seamlessly integrated with leading analytics platforms.

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, ensuring 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.

Accuracy and Scalability

Detecting advanced bots based on shallow interaction characteristics results in a high number of false positives. Our behavior analysis helps you filter highly sophisticated hu¬man-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.

Unified Portal

The Bot Manager solution is managed through Radware's Cloud Application Protection Services portal and can connect to any environment via inline or through an API-based out-of-path deployment. The 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 and the synchronicity with Radware's WAF, API, client-side and DDos protection modules help you see the complete picture and manage your security solutions in a frictionless manner with reduced overheads.

Other Integration Options

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

Our experience with Bot Manager has been very good. It served the reason we bought it, and it's doing its job from a scalability, performance and reliability perspective. Overall, I'd rate it a 10 out of 10."

— Cloud Security Engineer, Financial Service Firm

(see verified reviews on PeerSpot: Radware Bot Manager reviews, pricing and features 2024 | PeerSpot)

RWI 120 | 04.02.2024