REAL-TIME BOT PROTECTION FOR BANKING & FINANCIAL SERVICES INDUSTRY

RADWARE BOT MANAGER PROTECTS YOUR WEBSITES, MOBILE APPS & APIS FROM ACCOUNT TAKEOVER, APPLICATION VULNERABILITIES AND DATA THEFT

- Highest accuracy
- Fast and flexible deployment
- Filter bots from analytics dashboards
- Feed fake data or take custom actions against bot signatures

Banking and Financial Services Industry is largely impacted by bots. Competitors and fraudsters deploy human-like bots that attack your website, mobile apps, and APIs to commit automated attacks such as account takeover, payment card fraud, application DoS, content scraping, form spam, and more. Botmasters deploy thousands of bots on your digital properties to perform large-scale distributed attacks that are often 'low and slow' to go unnoticed by conventional defenses. Such automated attacks affect your customer experience, harm your brand and its reputation, skew your traffic analytics, and ultimately lead to loss of revenue.

INTEGRATION OPTIONS

- Web Server Plugins
- Cloud Connectors
- JavaScript Tag
- Virtual Appliance

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 to build a database of bot fingerprints and proactively stop bots from infiltrating into your internet properties.

WE PROTECT BANKING & FINANCIAL SERVICES FROM:

- **Account Takeover:**
  Credential stuffing and credential cracking attacks are used to gain unauthorized access to customer accounts. Account takeover is the first step for cybercriminals to carry out a range of online frauds involving impersonation, payments, reward programs and other financial services. Credential stuffing and brute force methods are the two most common techniques used by fraudsters. Credential stuffing exploits users' propensity to use same username and password at multiple websites, while credential cracking (also known as a 'brute force' attack) is a method of identifying valid credentials by trying different values for usernames and passwords.

- **API Abuse:**
  APIs are crucial in interconnecting a wide range of services that support websites and apps. Bad actors can use bots to exploit API vulnerabilities to steal sensitive data such as personally identifiable information (PII) and business-critical data. They can also tap into APIs in overwhelming numbers to carry out Application Distributed Denial of Service, attempt credential stuffing attacks, and systematically scrape website and application content.

- **Application DoS:**
  Application DoS attacks can slow down or even take down Web applications by exhausting system resources, third-party APIs, inventory databases, and other critical resources.

OWASP THREATS STOPPED BY RADWARE

- **OAT-001 — Carding**
  Multiple payment authorization attempts used to verify the validity of bulk stolen payment card data

- **OAT-005 — Scalping**
  Obtain limited-availability and/or preffered goods/ services by unfair methods

- **OAT-007 — Credential Cracking**
  Valid login credentials identified by trying different values for usernames

- **OAT-008 — Credential Stuffing**
  Mass login attempts used to verify the validity of stolen username/password pairs and/or passwords

- **OAT-011 — Scraping**
  Collect application content and/or other data for use elsewhere

- **OAT-015 — Denial of Service**
  Target resources of the application and database servers, or individual user accounts, to achieve denial of service (DoS)

- **OAT-016 — Skewing**
  Related link clicks, page requests or form submissions intended to alter some metric

- **OAT-021 — Denial of Inventory**
  Deplete goods or services stock without ever completing the purchase or committing to the transaction

- **Content Scraping:**
  Fraudsters and third-party aggregators use bots to scrape content and illegally reproduce your valuable original content on ghost websites and other unsavory portals, which not only harm your search engine ranking but also result in your content being downgraded in rank.

Skewed Look-to-Book ratio & KPIs:

Automated traffic on your Web properties distorts visitor metrics and hinders your strategic, marketing, and operation teams from making the right decisions based on accurate visitor data.

Form Spam:

Malicious bots constantly fill out lead generation forms with fake information and post unwanted comments on user discussion forums.

KEY FEATURES

Comprehensive API Protection:

Radware Bot Manager provides dedicated enterprise-grade protection from bot threats that are increasingly proliferating. Bot Manager secures internal and external APIs that drive back-end systems, mobile applications, and other essential services to travel enterprises and their customers by:

- Addressing gaps in unique source identification in M2M communications through our API-Client SDK
- Charting the statistical probability in how APIs are invoked in a sequence, and marking low probability flows for scrutiny.
- Collecting data from authentication APIs to validate legitimacy in access to resources.
- Detecting anomalous navigation flows or access patterns

Intent-based Deep Behavioral Analysis:

Many sophisticated bot 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.

Content aggregators and competitors continuously target your Web properties to scrape your proprietary content and other business-critical information. Our dedicated solution allows you to take custom actions based on bot signatures and types, and even choose to show 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 a comprehensive, real-time overview of traffic across your digital properties, and take action against malicious traffic that threatens your BFSI portals. Our system can also be integrated with leading SIEM tools to provide an unparalleled view and insights into your traffic, as well as page-level data on your website or mobile app, and a range of customizable options based on your specific organizational needs.

- **Easy Integration:**
  Radware Bot Manager provides easy and flexible deployment options that suit your business requirements. We offer integration options to work with virtually any existing infrastructure in minutes, using our JavaScript (JS) tag, Cloud connectors, Web server/ CDN/ CMS plugins, as well as SDKs for PHP, Java, .Net, Ruby, Django, Node.js, ColdFusion, Android and iOS. 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 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.

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: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.