BOT PREVENTION FOR EDTECH

PROTECT YOUR WEB APPLICATIONS, MOBILE APPS, AND APIS AGAINST AUTOMATED ATTACKS IN REAL-TIME

"We're extremely happy with Radware Bot Manager's solution that not only takes care of blocking all the bad bots but also provides comprehensive bot analysis. Radware Bot Manager has really kept their promise of zero false positives, as a result we are able to satisfy our website visitors better than ever!"

— John Potter, Former CTO, Purch (Acquired by Future PLC)

The online education industry is one of the fastest-growing sectors. Even before COVID-19, the overall market for online education was projected to reach $325 billion by 2025. Now it is one of the few industries where investment has not dried up, post lockdown across the globe. But with rapid growth, the sector has also garnered unwanted attention of cybercriminals.

INTEGRATION OPTIONS

- Web server plugins
- Cloud connectors
- JavaScript tags
- Virtual appliances

Among our customer base, nearly one-third of the traffic on EdTech platforms was generated by bad bots. Cybercriminals are deploying advanced, human-like bots to target EdTech platforms with automated attacks such as account takeover and web scraping.

TOP 5 AUTOMATED THREATS FACED BY EDTECH PLATFORMS

Account Takeover

Login pages are the prime target of cybercriminals across verticals, and EdTech is no different. Bad bots take over user accounts to steal PII and other sensitive information. On various EdTech platforms, cybercriminals also take over user accounts or even create fake accounts to access and scrape gated content. Radware Bot Manager blocks attempt to take over user accounts on the login page. It also analyses API requests to detect and block malicious attempts to evade device profiling and directly access the login API.

Application DDoS

The application layer in an enterprise infrastructure stack directly impacts the user experience. Layer 7, Distributed Denial of Service (DDoS) attacks severely affect resource-intensive functions, including inventory database checks, notifications, payment processing, and third-party services. These attacks are distributed over thousands of IP addresses and make a few hits every hour, but exhaust system resources that can affect business continuity. Radware Bot Manager identifies the intent behind attacks and blocks automated scripts (bots) that exploit the security vulnerabilities in business logic.

Skewed Analytics

The presence of web crawlers, aggregators, and malicious bots on your website causes noise in business KPIs. Non-human visitors impact conversion rates and other revenue metrics, such as the look-to-book ratio. Automated traffic skews user engagement and retention metrics. Radware Bot Manager helps in filtering non-human traffic present in paid and organic acquisition reports. You can seamlessly integrate Bot Manager with leading analytics platforms such as Adobe and Google Analytics.

SYMPTOMS OF SKEWED ANALYTICS

- High number of failed login attempts
- Consecutive login attempts with different credentials from the same HTTP client
- Unusual request activity for selected application content and data
- Unusual activity on selected resources (e.g., unexpected surge in traffic on a particular category page)
- Duplicate content in search engine results
- Unexpected changes in website performance and metrics
- Sudden increase in account creation rate

BENEFITS

- Ensure exclusivity of your unique content
- Improve conversion rate with Enhanced User Experience
- Strengthen product and marketing decision-making with accurate business KPIs
- Reduce Infrastructure Cost

SUCCESS STORY

Future PLC helps millions of people worldwide make smarter purchases through its popular portfolio of sites like Toms Guide, Toms Hardware, AnandTech, etc. However, Future PLC's proprietary content like product reviews, buying guides, etc., were subject to constant threat, given the value they possess.

Know why Future PLC entrusts Radware Bot Manager

WHY RADWARE BOT MANAGER

Radware Bot Manager defends EdTech platforms against automated attacks and ensures that only legitimate users and devices can access their applications and APIs. Radware Bot Manager leverages patented Intent-based Deep Behavioral analysis (IDBA) to understand a visitor's intent and block malicious ones. It relies on the collective intelligence of bot profiles and fingerprinted devices to optimize detection accuracy and is integrated into the existing infrastructure without any change in the technology stack.

FIVE ADVANTAGES OF RADWARE BOT MANAGER

Broad Attack Detection and Coverage:

Radware Bot Manager protects all channels (web, mobile, and APIs) against sophisticated attacks in real-time and helps organizations accurately distinguish between good bots, bad bots, and genuine users.

Collective Bot Intelligence:

Our Collective Bot Intelligence is a global threat intelligence repository that gathers bot signatures from across our client base to build a database of bot fingerprints and to help take pre-emptive action against infiltration attempts by bad bots. Collective Bot Intelligence also provides pre-attack notification gathered from continuously mining data across the web and darknet.

Comprehensive Reporting and Analytics:

Radware offers out-of-the-box granular reporting for all bot families including token-based offline analytics. Organizations can track automated activity based on user agents, geographies, referrers, and pages targeted. We also provide visualization APIs for data collection, management, and reporting.

Flexible Deployment Options:

Radware offers flexible integration options that include on-demand, on-premise, and cloud-based deployment into diverse infrastructure. Organizations can deploy Radware Bot Manager through CDN plug-ins, JavaScript tags, web server plugins, and API cloud connectors. Other options are the mobile SDK and a virtual appliance. Integration with popular analytics tools including Google Analytics and Adobe Analytics is also available.

Fully Managed Service:

Radware Bot Manager is also available as a cloud application security service that can be fully integrated with Radware's Cloud WAF. Radware Cloud Applications Security Suite includes Cloud WAF, Cloud Bot Manager and ERT Active Attackers Feed – as a unified Cloud Service with seamless experience for onboarding, reporting, and configuration.

Complete Application and API Security Suite:

Easy integration with AppWall®, Radware CWAF and DDoS mitigation solutions, both on-premise and in the cloud.

ABOUT RADWARE

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019. ShieldSquare is now Radware Bot Manager.

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.