E-COMMERCE BOT PROTECTION

PREVENT ACCOUNT TAKEOVER, CARDING, WEB SCRAPING AND OTHER AUTOMATED THREATS

- Highest Accuracy
- Fast and Flexible Deployment
- Filter Bots from Analytics Dashboards
- Feed Fake Data or Take Custom Actions against Bot Signature

---

"Radware Bot Manager solution meets our stringent latency and false-positive requirements and has virtually eliminated the threat we were facing from bots. Radware Bot Manager is a rare example of a company whose product exceeds the marketing promises."

— BRENT STACKHOUSE, DIRECTOR OF SECURITY AND COMPLIANCE, ZULILY

At Radware, we process tens of billions of page views every month. Our research shows that account takeover, carding, and scraping are the most common bot-originated threats to e-commerce businesses. Our bot detection engine applies advanced machine learning models to block automated attacks at the application layer, rather than following traditional web application firewalls' rule-based approach.

INTEGRATION OPTIONS

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

Fraudsters and competitors devise ingenious ways to scrape prices, plot carding, and gift card frauds. Criminals use credential stuffing and brute force approach to hack into customers' accounts and execute fraudulent transactions. A large number of attacks are either massively distributed or are adequately 'slow & low' to evade the in-house security measures. Such automated attacks can be prevented by a dedicated bot mitigation solution, specifically built to detect sophisticated bots. Radware Bot Manager uses device and browser fingerprinting, collective bot intelligence, and dynamic Turing test to identify and block automated usage before bots commit any fraud.

E-COMMERCE THREATS THAT WE PREVENT

Account Takeover

(Credential stuffing and brute force attacks are used to gain unauthorized access to customer accounts)

Carding

(Carders deploy bots on checkout pages to validate stolen-card-details, and to crack gift cards)

Scraping of Price, Content & Inventory Information

(Competitors illegally scrape content, price and inventory information to gain competitive advantage)

Cart Abandonment & Inventory Exhaustion

(Bots add hundreds of items in the cart and later, abandon them to prevent real shoppers from buying the products)

Application DoS

(Application DoS attacks slow down the e-commerce portals by exhausting web servers, 3rd party APIs, inventory database and other critical resources)

Scalping Products & Tickets

(Hackers deploy bots to buy goods and tickets during a flash sale, and they sell them later at a much higher price)

Fake Account Creation

(Bots are used to generate fake accounts on a massive scale for content spamming, virtual money laundering, SEO and skewing the surveys)

Skewed Analytics

(Automated traffic on your e-commerce portal skews metrics and misleads decision making)

SYMPTOMS OF A BOT ATTACK ON AN E-COMMERCE WEBSITE

- High number of failed login attempts
- Increased chargebacks and transaction disputes
- Consecutive login attempts with different credentials from the same HTTP client
- Unusual request activity for selected application content and data
- Unexpected changes in website performance and metrics
- Sudden increase in account creation rate
- Elevated traffic for certain limited-availability goods or services

BENEFITS

- Outsmart competition by concealing the pricing and inventory details
- Eliminate fraudulent purchases, protect reward programs and improve customer loyalty
- Reduce financial risks, chargebacks, penalties and improve merchant reputation.
- Make inventory available for real online shoppers
- Trust analytics again. Improve outcome of paid and unpaid growth strategies.

WHY RADWARE BOT MANAGER

Radware Bot Manager has a non-intrusive API based approach to detect bot activities on e-commerce websites. Our deep learning systems analyze multiple streams of data including mouse movements, keystrokes and URL traversal patterns to perform 'user intent analysis,' find anomalies and avert large-scale distributed attacks. Radware Bot Manager can be seamlessly integrated to an e-commerce portal's existing infrastructure in minutes. We offer easy integration using web server plugins, cloud connectors, JS tag, and virtual appliance. Top global online brands trust us for lowest latency and highest accuracy.

OWASP THREATS STOPPED BY RADWARE BOT MANAGER

- **OAT-007** — Credential Cracking
- **OAT-008** — Credential Stuffing
- **OAT-001** — Carding
- **OAT-002** — Token Cracking
- **OAT-010** — Card Cracking
- **OAT-011** — Scraping
- **OAT-005** — Scalping
- **OAT-015** — Denial of Service
- **OAT-016** — Skewing
- **OAT-019** — Account Creation

Success Story

The e-tailer was continuously targeted by account takeover attacks and carding fraud. Radware Bot Manager stopped account takeover activity in its tracks and eliminated carding attempts that resulted in reduced chargebacks.

Read How A Top 5 E-tailer of US Eliminated Account Takeovers

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.