REAL-TIME BOT PROTECTION AGAINST ACCOUNT TAKEOVER

BLOCK CREDENTIAL STUFFING AND BRUTE FORCE ATTACKS

"Radware Bot Manager 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

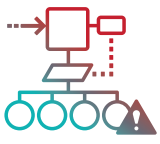
Account takeover is a necessary step for a variety of online frauds involving e-commerce, payments, reward programs and financial services. Credential stuffing and brute force methods are the two most common techniques used by fraudsters. Credential stuffing exploits users' propensity to use same username and password at multiple websites, and brute force method is a way to identify valid credentials by trying different values for usernames and passwords.

Symptoms of an Account Takeover Attack

High Number of Failed Login Attempts

Elevated Account Lock Rate

Increased Customer Complaints of Account Hijacking



Sequential Login Attempts with Different Credentials From Same HTTP Client

Impact of Account Takeover

Fraudulent Transactions & Abuse of Reward Programs

Financial fraud via compromised accounts doesn't only cause a loss of revenue but also sabotages customer loyalty efforts. Radware Bot Manager blocks illegal account access before it is used for fraudulent transactions. Our algorithms are battle-tested for higher accuracy during peak hours.

Damage to Brand Reputation

Reputational damage undermines customer's confidence and can cause loss of revenue. With collective bot intelligence, Radware Bot Manager continuously adapts to evolving bot patterns and can block sophisticated account takeover attacks.

KEY BENEFITS

Eliminate Account Takeover Attempts and Avert Financial Loss

Protect Reward Programs & Improve Customer Loyalty

Defend Brand Reputation

WHY RADWARE BOT MANAGER

Radware Bot Manager has a non-intrusive API based approach to detect bot activities on e-commerce websites. Our bot detection engine uses device fingerprinting, user behavior modeling, collective bot intelligence and machine learning techniques to spot any suspicious activity across login and signup pages. We have a proven track record in blocking advanced distributed attack and highly sophisticated 'slow & low' attacks.

OWASP THREATS STOPPED BY RADWARE BOT MANAGER

- **OAT-008** — Credential Stuffing

  Mass log in attempts used to verify the validity of stolen username/password pairs

- **OAT-007** — Credential Cracking

  Identify valid login credentials by trying different values for usernames and/or passwords.

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.