REAL-TIME BOT PROTECTION AGAINST ACCOUNT TAKEOVER

BLOCK CREDENTIAL STUFFING AND BRUTE FORCE ATTACKS

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

– BRENT STACKHOUSE, DIRECTOR OF SECURITY AND COMPLIANCE, ZULILY

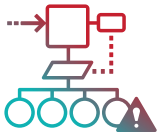
Account takeover is a necessary step for a variety of online frauds involving e-commerce, payments, reward programs and financial services. Credential stuffing and brute force methods are the two most common techniques used by fraudsters. Credential stuffing exploits users' propensity to use the same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

***Formerly a ShieldSquare solution**

Impact of Account Takeover

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

Damage to Brand Reputation
Reputational damage undermines customers' confidence and can cause loss of revenue. With collective bot intelligence, Radware's 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 and Improve Customer Loyalty

Defend Brand Reputation

WHY RADWARE

Radware's Bot Manager has a nonintrusive 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 of blocking advanced distributed attacks and highly sophisticated "low and slow" attacks.

OWASP THREATS STOPPED BY RADWARE

- OAT-008 — Credential Stuffing
  Mass login attempts used to verify the validity of stolen username/password pairs
- OAT-007 — Credential Cracking
  Valid login credentials identified by trying different values for usernames and/or passwords

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.