Real-time Bot Protection Against Account Takeover

Block Credential Stuffing and Brute Force Attacks

Account takeover is a necessary step for a variety of fraudulent online activities targeting 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 brute force methods are used to identify valid credentials by trying different values for usernames and passwords.

We onboarded Bot Manager in the midst of our peak season and saw immediate results/benefits. Our customers' experiences are our top priority. By working with Radware, we are able to better secure and improve the shopping experience."

— Boris Nađ, Technical Operations Manager, Njuskalo, Croatia's No. 1 Marketplace.

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

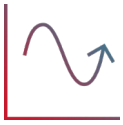
Integration Options

- CDN
- Other Third-party Integrations
- On-premise Sensor
- App Server SDKs
- Web Server Plugins
- DNS Diversion
- ADC

Impact of Account Takeover

Fraudulent Transactions and Abuse of Reward Programs:

Financial fraud via compromised accounts not only causes a loss of revenue but also sabotages customer loyalty efforts. Radware Bot Manager blocks illegal account access before it can be abused to carry out fraudulent transactions. Our algorithms are battle-tested for highest detection accuracy even during peak traffic periods.



Damage to Brand Reputation:

Reputational damage undermines the 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.

Stolen PII and Confidential Information:

Another reason that companies should be alert about protecting confidential information, especially in industries such as healthcare, airlines, and e-commerce, which have Personally Identifiable Information stored about their customers. Fraudsters can extract the confidential information and abuse it to commit financial crimes or sell the data to other interested nefarious parties.

Strain on Resources:

A lot of times, companies realize that they have been under attack only after the damage has been done, and when that happens, resolution and investigation can be time-consuming and expensive processes that impose unnecessary strain on customer service, legal and compliance departments.

Radware Bot Manager Benefits

- Eliminate Account Takeover Attempts and Avert Financial Loss
- Protect Reward Programs & Improve Customer Loyalty
- Defend Brand Reputation

Why Radware Bot Manager

Non-intrusive Bot Detection:

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 log-in and signup pages.

We have a proven track record in blocking advanced distributed attacks and highly sophisticated 'low and slow' attacks.

Widest Mitigation Options:

Radware Bot Manager has the widest mitigation option available to its users, and now with Crypto Challenge, Radware Bot Manager adds another mitigation option to stop sophisticated bot attacks, while providing a CAPTCHA-less mitigation option with Blockchain-based Cryptographic Proof of Work.

CAPTCHA-less Mitigation:

Blockchain based Crypto Challenge is a behavior-enforcing mechanism that detects anomalies against a baseline of normative behavior. When an anomaly is detected, the mitigation method challenges the user device by creating CPU-intensive browser-based challenges with gradually increasing difficulty, forcing the attacker's CPU to work harder every time it is challenged, eventually choking the device, thereby transferring the cost of the attack to the attacker.

Mobile Application Protection Capabilities:

- **Integrated Device Authentication** – Radware Bot Manager SDK includes a one-of-a-kind attestation for Google (Android) and Apple (iOS) devices, for tighter and faster protection of native mobile applications. This unique capability keeps device authenticity in check, making sure only real devices and not emulators, modified applications or modified OS are getting access to your resources.
- **Secure Identity** – This unique solution ensures the security of your client identity (requests to your web application) against identity spoofing, identity tampering, and replay attacks by creating a unique identity for each user against which it validates every request.

Secure Identity along with Google/Apple attestation (Integrated Authentication) provides enhanced protection to your mobile devices and apps and stops bot attacks on mobile apps before they materialize and take a toll on your infrastructure.

Unified Portal:

Radware's Cloud Application Protection portal provides a single interface for all Radware Cloud Application Protection solutions with ease of configuration, granular control options and detailed analytics into all application security events and protection metrics. This 'single pane of glass' view helps you manage your security solutions in a frictionless manner with reduced overheads.

Widest Mitigation Options

- Allow
- Challenge CAPTCHA
- Block
- Feed Fake Data
- Throttle
- Drop
- Session Termination
- Redirect Loop
- Log Only
- Custom Response
- Crypto Challenge

Success Story

One of the largest global online marketplaces with nearly 200 million users was targeted by cybercriminals using bots to attack its websites, mobile applications, and APIs. Radware Bot Manager not only ensured robust security for user accounts through prevention of account takeover attacks, but also greatly reduced human intervention needed for bot management compared to the enterprise's previous solution.

Radware Bot Manager Protects a Leading Online Marketplace

HK-103 | 20.4.2023