Radware Bot Manager Mobile Application Protection

Real-Time Protection Against Malicious Bot Threats on Native Mobile Applications

Mobile applications have become prime targets for increasingly sophisticated bot attacks in today's increasingly mobile-first digital environment. Sophisticated bots now possess the capability to rapidly rotate identities and emulate mobile devices to exploit vulnerabilities in native mobile applications. Consequently, bot protection solutions that are primarily designed for web applications often fail to address the unique challenges of the mobile ecosystem. Tackling sophisticated bots in such an environment requires a purpose-built approach to mobile application security that delivers comprehensive protection against these evolving threats.

Radware Bot Manager's dedicated mobile application protection capabilities deliver real-time bot detection with advanced attestation technology to validate and block malicious traffic on native mobile applications, while ensuring a seamless experience for legitimate users.

The Need for Dedicated Bot Protection for Mobile Applications

Mobile applications are a critical business channel for organizations across sectors, but mobile platforms have unique security challenges due to fundamental differences in architecture, user interaction patterns, traffic characteristics, and development frameworks between mobile and web applications:

API-Based Communication

Native mobile applications primarily communicate through APIs, unlike web applications that rely on browser interactions. Web-focused bot protection that relies on browser-specific signals for bot detection—such as JavaScript execution, cookies, and user-agent strings—is ineffective in API-first mobile architectures that bypass the browser layer with direct HTTP requests to back-end APIs.

A dedicated mobile application protection module can access device-level signals and perform real-time checks to detect tampering or the use of mobile emulator environments. The module can ensure the integrity of communication between an application and back-end APIs and validate that API requests originate from legitimate applications through device and application integrity checks via attestation mechanisms.

Differences Between Platform Architectures

Web applications operate on standardized protocols and technologies within web browsers such as HTML, CSS, and JavaScript, but mobile applications function on fundamentally different architectures based on iOS, Android, and cross-platform frameworks such as React Native. Native mobile applications are also built using platform-specific tools and languages such as Swift/Objective-C or Java/Kotlin and require security solutions that are optimized for the specific platform.

Mobile-Specific Attack Vectors

The nature of threats is significantly different on mobile applications, with unique attack vectors that are not present in web environments. The mobile application itself is an attack surface due to its execution directly on the user's device, unlike web applications that run on a server and render through a browser. Attackers can reverse-engineer the application to inspect its logic, API endpoints, or tamper with the application itself. The vast array of mobile devices, operating systems, and versions creates complexity in accurate bot detection, with emulators and application impersonators increasingly being leveraged for sophisticated bot attacks.

Identity Data Collection Limitations

Unique device identifiers like IMEI, device ID, etc., that could be useful for bot detection cannot be collected from mobile devices due to privacy concerns and regulatory restrictions, requiring a different approach such as platform-specific attestation to identify malicious activity.

Radware's Multi-Layered Bot Protection for Mobile Applications

Radware Bot Manager's dedicated mobile application protection for Android and iOS platforms leverages a multi-layered protection strategy to identify bad bots and block them before they gain access to application resources. The solution identifies malicious bot activity by evaluating multiple non-PII (personally identifiable information) attributes on the end user's device for anomalies, analyzing behavioral intent-based interaction parameters, and leveraging the solution's integrated attestation for Android and iOS devices to verify the integrity of the mobile application and host device. This real-time protection that is specifically tailored for API-first mobile applications provides a higher level of visibility and accurate, comprehensive defense against malicious mobile-focused bot attacks.

Mobile Application Protection Capabilities

Integrated Device Authentication: Radware Bot Manager's dedicated mobile application protection capabilities include an integrated, one-of-a-kind, tamper-proof attestation mechanism for Android and iOS devices and native mobile applications that ensures robust bot protection:

- Radware's 'Mobile Attestation Challenge' leverages Google's and Apple's platform-native attestation mechanisms to mandate authentication for every request through a device-specific, time-bound token, reducing the risk of spoofing or tampering and allowing only genuine devices and applications to access protected resources. Malicious bot requests that lack authentication or rotate identities are served with an interstitial challenge screen and denied access to the application, thereby mitigating the threat.
- This unique capability ensures that only requests originating from unaltered, authentic applications running on genuine devices are getting access to resources, and not emulators, modified applications, or modified OS.

Secure Identity: This engine creates a unique identity for each user and cryptographically signs each request made from the application, which is then validated at the back end to make sure that the request is not tampered with during transit. This unique capability protects against request tampering, spoofing, and replay attacks.

Together, Radware Bot Manager's Secure Identity and Integrated Device Authentication provide multi-layered bot protection to mobile applications, stopping malicious traffic from accessing application resources and continuously validating each user request to ensure authentication and prevent user impersonation.

Behavioral Analysis: The module identifies malicious behavior unique to mobile interactions by analyzing touch patterns, device data, and interaction flows to detect even the most sophisticated mobile bot activity.

Analytics and Reporting: Radware offers granular analytics as well as detailed reports on bot activities across protected mobile applications. The report includes global bot distribution, malicious IPs list, and traffic patterns, along with detailed insights on the severity of attacks.

Flexible Integration: Bot Manager's mobile application protection module is lightweight and easy to integrate with native iOS, Android, and React Native-based apps

CAPTCHA Customization: Both the CAPTCHA and Block pages for mobile application protection can be customized to suit client requirements. The customization options are provided across multiple elements in the CAPTCHA/Block page including text, text alignment, font, color, language, image, etc.

Comprehensive Application Protection and Correlation Engine: Radware clients can leverage a single unified interface for all Radware Cloud Application Protection solutions including Bot Manager, WAF, DDoS Protection, Client-Side Protection, and API Protection solutions with ease of configuration, granular control options, and detailed analytics into all application security events and protection metrics. Radware's API Protection solution provides auto-discovery of APIs and real-time protection against business logic vulnerability attacks to significantly enhance protection accuracy in API-first environments. The AI-based correlation engine automatically and preemptively cross-correlates between Radware solutions including Bot Manager, WAF, and API Protection solutions and blocks malicious sources. Radware's unified portal helps manage these security solutions through a 'single pane of glass' view in a frictionless manner with reduced overheads.

Case Study

A leading US-based financial services organization implemented Radware Bot Manager for web and mobile application protection after experiencing a surge in brute-force ATO (account takeover) attacks. As a result of the implementation:

- Over 5 billion bad bot hits were mitigated in real-time within three months.
- Approximately $155 million in potential breach losses were prevented.

Click here to download the full case study.

For more information, visit our website or contact our sales team at:

Contact Radware

Alternatively, schedule a demo or request a consultation to learn how Radware can secure your mobile applications. Take advantage of free Radware tools such as the Application Security Analyzer and Application Vulnerability Scanner to understand your current security risks.

RWI 534 I 05.27.2025