# Radware Bot Manager Mobile Application Protection

## Real-time Native Mobile App Protection Against Bad Bots, App Impersonators, and Emulators

Today, 10% of bad bots target native mobile applications. With the ubiquitous adoption of the native mobile applications, cyber attackers have found another attack surface to exploit. Attackers prey on business-critical data, customers' personal information (PII), credentials, and payment card details using bots. These bots change their identity, behavior, and IP address to operate under permissible limits of conventional security measures. Additionally, native mobile traffic characteristics are less predictable than web browsers traffic. Tackling such sophisticated bots requires an advanced approach that improves its logic faster than continuously evolving bot patterns. Radware Bot Manager leverages the latest developments in deep learning to filter and mitigate invalid traffic from mobile devices in real-time.

## Protect User Data and Content from Sophisticated Attacks

Radware Bot Manager's SDKs are designed to deliver unparalleled accuracy and performance. To protect against bot attacks on native mobile apps, Radware Bot Manager SDK collects multiple parameters (non-PII data) from the end user's device to build a database of unique fingerprints and filter anomalous behavior patterns. We apply device fingerprinting and device level unique cookies to separate genuine users from bots, and accurately manage automated traffic while ensuring zero false positives. Our SDKs are tested across a wide range of devices and OS environments to ensure compatibility, speed, and scalability.

## 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 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 Device 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.

**Analytics and Reporting –** Radware offers granular analytics as well as detailed reports on bot activities across your mobile app and web. The report includes highly targeted screens, global bot distribution, malicious IPs list, traffic pattern along with detailed insight on the severity of an attack.

**Flexible Integration –** The SDKs are lightweight and easy to integrate with iOS and Android apps. SDKs can be embedded into native apps as well as hybrid apps, and are optimized to consume less space, memory, CPU, and battery power. Radware Bot Manager SDK can be deployed in any existing infrastructure provided by the customer through our multiple server-side integration options.

**CAPTCHA Customization** – Users can customize the Captcha and Block Pages on the Mobile SDK as per their requirement. The customization options are provided across multiple elements in the CAPTCHA/Block page like text, text alignment font, color, language, image etc.

**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.



HK-111 | 20.4.2023