

# PerimeterX Bot Defender Mobile™

As mobile adoption continues to grow, industries are increasingly leveraging mobile applications to easily interact with users. The increased mobile presence is a prime target for bot attacks.

PerimeterX Bot Defender Mobile prevents automated attacks by hackers who attempt to exploit vulnerabilities in mobile applications to perform account takeovers, account abuse or fraudulent transactions.

PerimeterX Bot Defender Mobile is highly scalable, and is deployed easily, without disrupting the customer experience or touching application logic and flows.

## PERIMETERX BOT DEFENDER MOBILE: HOW IT WORKS

**Deploy** — Once PX Mobile Sensor is natively integrated with iOS or Android applications, PerimeterX tracks application activity on the device.

**Collect** — PX Mobile Sensor collects and sends activities about user-behavior, application and device usage to PX Detector.

**Analyze** — PX Detector uses advanced machine learning and behavioral analytics to analyze authenticity, profile the user's behavior and create a risk score.

**Enforce** — Based on the risk score, PX Enforcer can issue a challenge or block the request.

**Monitor** — The PerimeterX Console displays all activity about mobile applications and API requests in real-time.

## PROTECTION FROM HACKING TECHNIQUES



### Stop App Impersonation

Only allows genuine mobile apps to access APIs— all others are blocked



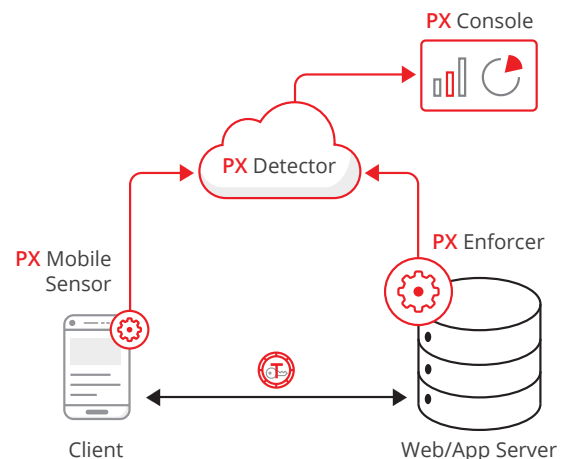
### Block Emulator Use

Only allows mobile APIs to be accessed by actual user devices—not malicious apps running in an emulator



### Detect Automated Control

Verifies that only humans are driving native app—not automated processes or bots



# PERIMETERX BOT DEFENDER MOBILE: HOW IT'S DIFFERENT

## BOT DETECTION ACCURACY

PerimeterX Bot Defender Mobile offers a new approach to bot detection using dynamic behavior profiles of real users within mobile applications and environments. Unlike legacy solutions based on historical signature or fingerprint technologies, PerimeterX Bot Defender Mobile can accurately detect even the newest, most advanced bot attacks in real time. It separates actual human behavior versus suspicious non-human behavior, achieving superior attack detection accuracy.

## NATIVE SDK IMPLEMENTATION

PerimeterX Bot Defender Mobile is designed for high-scalability and web-scale performance. PX Mobile Sensor is natively implemented via SDK in mobile iOS or Android apps without rewriting logic or changing the application flow. It provides real time sensor data and enforcement via out-of-band communication with PerimeterX's cloud-based detection and enforcement platform.

## DEPLOYABILITY

PerimeterX Bot Defender Mobile can be deployed in a few hours with pre-built integrations. The solution integrates with leading cloud infrastructure, SDK/Middleware, Load Balancers, Web Servers and analytic tools. Whether you're using Google App Engine, Adobe Analytics or Salesforce Commerce Cloud, using Fastly as a CDN, AWS or deployed on your own servers, PerimeterX Bot Defender Mobile integrates to your infrastructure easily and deploys quickly and reliably.

## SUPERIOR USER EXPERIENCE

PerimeterX Bot Defender Mobile is invisible to users and provides the best user experience and application performance, while ensuring app integrity and security. The solution blocks bots in real time with detection policies created by behavioral analytics that are continuously refined by machine learning to ensure a superior user-experience by minimizing false-positives.

## KEY FEATURES

<b>DETECTION</b>	<ul style="list-style-type: none"><li>• Machine learning based behavioral analytics engine</li><li>• Accurate identification of Generation 1, 2, 3, and 4 bot technologies</li><li>• Block/allow policies may be implemented per application class</li><li>• Blacklist and whitelist apps and domains</li></ul>
<b>SERVER SIDE INTEGRATIONS</b>	<ul style="list-style-type: none"><li>• Cloud Infrastructure: Salesforce Commerce Cloud, Amazon Cloudfront, Google App Engine, Fastly</li><li>• SDK/Middleware: Java, Python, PHP, Ruby, ASP.NET, Node</li><li>• Load Balancer/Web Server: Apache, NGINX, Kong, Varnish, F5</li><li>• Analytics: Adobe, adKernal, ironSource</li></ul>
<b>CLIENT SIDE INTEGRATIONS</b>	<ul style="list-style-type: none"><li>• IOS 8 and higher</li><li>• Android 4.1 and higher</li></ul>
<b>REPORTS</b>	<ul style="list-style-type: none"><li>• Top malicious IPs, traffic patterns</li><li>• Score breakdown, incident types</li><li>• Top domains, top known bots</li><li>• Breakout mobile versus web attack data</li><li>• Export reports as CSV files</li><li>• Detailed forensics analysis of malicious activities</li></ul>

perimeterx

www.perimeterx.com

info@perimeterx.com