appdome

Unified Mobile App Defense

MOBILE GEO COMPLIANCE

See how easy it is to build, test, release, and monitor Mobile Geo Compliance in Android and iOS apps using Appdome's automated mobile app defense

FASTEST & EASIEST WAY TO DELIVER MOBILE GEO COMPLIANCE

Automate delivery of mobile geo compliance in Android & iOS apps to accelerate mobile DevOps CI/CD pipelines. Deliver Certified Secure™ protection against fake geolocation and GPS apps, unauthorized VPNs, SIM swapping, teleportation, and banned usage by location. Ensure the integrity, accuracy and authenticity of location data in iOS and Android apps to achieve geo compliance and fraud prevention with ease. Monitor attacks and defenses in real-time. No code, no SDK, & no added work for the dev team.

LOCATION INTEGRITY IS CRUCIAL IN MOBILE APPS

In today's mobile landscape, ensuring secure and lawful app operation is crucial. Brands grapple with challenges in geographical compliance, identity verification, and anti-fraud measures. Apps must comply with regulations, operating exclusively where legally allowed, especially in sectors like gaming and streaming. In social commerce, gig economy, dating apps and more, verifying user identities against claimed locations is crucial to prevent compliance breaches and fraud. Maintaining transaction integrity and reducing fraud are ongoing challenges, requiring robust Know Your Customer (KYC) processes and audit trails. Protecting targeted marketing efforts from unauthorized access is crucial to prevent program leakage, ensuring revenue alignment with marketing strategies. Whatever the circumstance, Appdome's Geo Compliance solution enables brands and mobile users to trust the integrity of the location data.

STOP FAKE LOCATION & GPS

Attackers and fraudsters spoof GPS signals or manipulate sensors such as the gyroscope or accelerometer, causing mobile apps to report fake location data, making it appear as if the user or device is in a different location than they are. Falsifying location facilitates malicious activities such as bypassing licensing controls, presenting fake location info in dating or social media apps, bypassing geographic restrictions for streaming services, and much more – all of which can interfere with a mobile brand's ability to comply with regulations or KYC requirements. Appdome enables brands to preserve the integrity of location services in Android & iOS apps by detecting the specific hooks and malicious methods used by attackers to instrument, modify or interfere with device-level geolocation of the mobile OS.

BLOCK FAKE GPS APPS

Using fake GPS apps, attackers can manipulate the location data of a mobile device, providing false GPS coordinates or overriding the location data reported by the mobile OS GPS sensors. Fake GPS apps enable all sorts of harmful activities such as location spoofing, license bypass, evasion of geo-fencing requirements, and more. Using Appdome Geo Compliance, mobile brands can easily stop the use of fake GPS apps to falsify location info, enabling mobile product managers to ensure the accuracy of location-based services and ensure the security and integrity of their apps.

DETECT SIM SWAPPING

SIM swapping is a type of mobile fraud where attackers take control of a victim's phone number by convincing a telecom provider to transfer the number to a new SIM card controlled by the attacker. This may enable attackers to bypass 2FA/MFA and or even conduct account takeovers (ATO). Appdome detects when an attacker or user changes the SIM or eSIMs associated with the mobile device to defend against all variants of SIM swapping attacks.

BLOCK UNAUTHORIZED VPNS

Unauthorized use of VPNs in mobile apps introduces risks by masking users' true IP addresses, enabling malicious activities. By routing traffic through a VPN, an attacker can intercept and manipulate the communication between the user's device and the backend server, leading to unauthorized data access. Appdome detects the use of an untrusted VPN to spoof the IP address or location of the device used with the app.

DETECT RANDOM LOCATIONS / TELEPORTATION

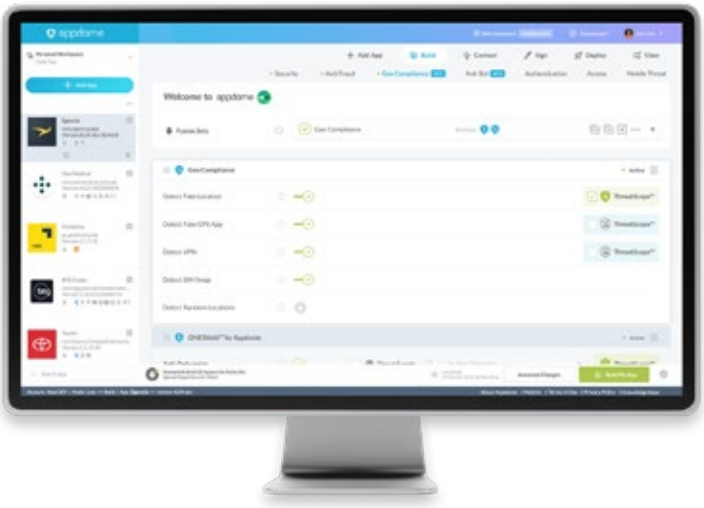
Attackers can spoof geo-location data or sensors in mobile apps using teleportation. Appdome detects abnormal patterns in GPS data such as the geo location of a mobile device reporting location data improbably (for example, moving from New York to Shanghai within 5 minutes).

BAN APP USAGE BY REGION

Many mobile brands want additional controls for where their Android & iOS apps can and cannot be used. Appdome Geo Compliance provides controls to set up boundaries where usage is not permitted, giving brands peace of mind regarding appropriate location app usage.

ONE SOLUTION IS ALL MOBILE DEVSECOPS NEEDS.

Appdome delivers mobile app protection, certification, XDR, and cyber release management in one unified, fully integrated platform.



THREATSCOPE™ MOBILE XDR

ThreatScope™ Mobile XDR provides mobile brands, developers and cyber professionals extended detection and response (XDR) for in-production Android & iOS mobile apps. ThreatScope Moible XDR gives mobile brands a consolidated view and real-time visibility into the entire range of threats and attacks impacting the mobile brand, apps and users, including full visibility into 1000s of threat streams covering mobile app security, mobile fraud, malware, cheats, bot attacks, and geo compliance. As an XDR, ThreatScope also provides the configuration as code power to remediate attacks instantly build-by-build, and release-by-release.

With ThreatScope, organizations can (1) see and analyze the top mobile app threats and attacks impacting the mobile channel, (2) prove the value of protections deployed in mobile apps (3) make data-driven decisions of what protections to deploy in each release, and (4) create customized views and comparisons that track the most relevant threats & attacks impacting the mobile business. Stay one step ahead of attackers, fraudsters and hackers with ThreatScope.

MOBILE CYBER DEFENSE AUTOMATION

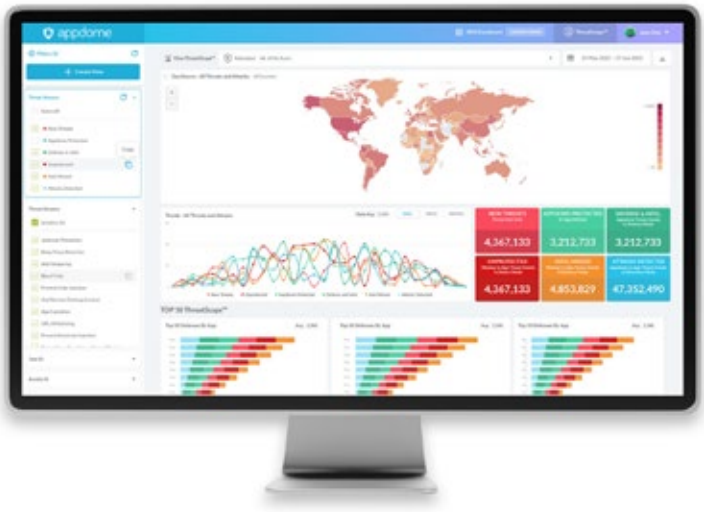
Appdome pioneered the no-code mobile app security market with an automated Mobile App Defense platform. This flagship product provides mobile developers, cyber security and fraud teams a centralized system and configuration as code ease to build, test, release and monitor mobile app security, anti-fraud, anti-malware, anti-cheat and anti-bot features in Android or iOS apps. Patented cyber release management, event logging, build tracking, version control, code freeze, security templating, role-based access and CI/CD DEV APIs allow instant DevOps readiness for any mobile app.

THREAT-EVENTS™ THREAT AWARE UI/UX CONTROL

All runtime and dynamic protections come enabled with Threat-Events™, Appdome's in-app attack intelligence and UI/UX control framework. Threat-Events empower developers to read/write from the Appdome Security Framework™, gather data on each attack inside the app and use the detection and defense data to create and control beautiful user experiences when attacks occur.

CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Each protected build generated on Appdome comes with a Certified Secure™ certificate that guarantees the mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and threat intelligence features protecting the mobile app. Mobile Dev Teams use Certified Secure™ as the DevSecOps artifact to clear apps for release and save money and time vs. using code scans and penetration tests in the release process.



ABOUT APPDOME

Appdome is the mobile app economy's one-stop shop for mobile app defense. Appdome is on a mission to protect every mobile app in the world and the people who use mobile apps in their lives and at work. Appdome provides the mobile industry's only fully-automated, Unified Defense Platform, powered by a patented coding engine, used by mobile brands to eliminate complexity, save money and deliver 300+ Certified Secure™ mobile app security, anti-malware, anti-fraud, MOBILEBot™ Defense, Geo Compliance, anti-cheat, MiTM attack prevention, code obfuscation and other protections in Android and iOS apps with ease, all inside the mobile DevOps and CI/CD pipeline. Appdome's Unified Defense Platform also comes with Threat-Events™ for UX/UI Control and ThreatScope™ Mobile XDR. Leading financial, healthcare, mobile games, government and m-commerce brands use Appdome to protect Android and iOS apps, mobile customers and mobile businesses globally.

GC-DS-20240206