appdome

Unified Mobile App Defense

BETTER ANDROID ANTI-MALWARE IN CI/CD

Continuously build, test, monitor and respond with Android Anti-Malware and 300+ other defenses in Android & iOS mobile apps in one platform in CI/CD.

DELIVER ANDROID ANTI-MALWARE AT DEVOPS SPEED

Mobile DevOps pipelines use systems to drive rapid, automated and continuous integration, delivery and release cycles of Android & iOS apps. Appdome's Unified Mobile App Defense platform lets you do the same, using a factory model to build, test, monitor and respond with Android Anti-Malware in mobile apps, fast. Here's what you get by combining Appdome with CI/CD:

RAPID RELEASE & DELIVERY, ANDROID ANTI-MALWARE

Getting Android anti-malware in mobile applications right requires releasing dozens of unique defenses in Android apps fast. With Appdome, you do just that. Instead of needing engineering resources and work, you build Android anti-malware features in Android apps on-demand. From the CI/CD, trigger the build command in Appdome and release Android anti-malware in mobile apps either all at once or in an iterative release process to respond to new threats as they emerge and match the needs of the business instantly.

CONTINUOUS SECURITY FOR MOBILE APPS

Mobile apps and operating systems change constantly. Coding languages for mobile apps change regularly. New APIs, frameworks, and capabilities are added and updated in mobile apps continuously. Appdome automatically adjusts and adapts each Android anti-malware feature to the changes in the updated mobile app. Release-by-release, no manual work, retooling, or coding change are needed to make Android anti-malware features work in the new app. Instead, Appdome does that for you and provides continuous security across all mobile app versions and releases with ease.

CONTINUOUS DETECTION & RESPONSE

DevOps requires real-time data and feedback on each iterative release of a mobile app. Appdome provides real-time data and feedback on each Android anti-malware and other defenses in the mobile app. With Appdome, mobile brands and organizations monitor all attack vectors impacting the mobile app, revealing the impact of each defense and the total active attack surface in real-time. Armed with this data, brands click-to-add new defenses or update enforcement models in existing defenses to keep the mobile app, business and users safe.

COMPLIANCE TRANSPARENCY & CONTROL

Continuous compliance transparency and control over each step of the build, test, and release lifecycle for mobile apps and defenses alike is critical. Without Appdome, compliance is a leaky bucket and gaps arise. Appdome provides enterprise-grade (1) access, version, and change control, (2) role-based and team entitlements, and (3) tracking for each mobile defense choice, change, detection, and enforcement event. Build by build, each mobile app is Certified Secure™ compliant in the CI/CD pipeline

"BEST OF SUITE" COST SAVINGS & CONSOLIDATION

Appdome offers unparalleled cost consolidation and TCO savings for Android anti-malware and other defenses in mobile applications. With Appdome, Android anti-malware features are delivered without resource dependencies or compatibility limitations. In addition, features are instantly interoperable with 300+ other defenses offered via the Appdome platform. Eliminate point products, multi-vendor integration risk and complexity, and streamline release cycles for mobile applications and mobile app defenses alike.

FULL ANDROID ANTI-MALWARE FEATURE COVERAGE

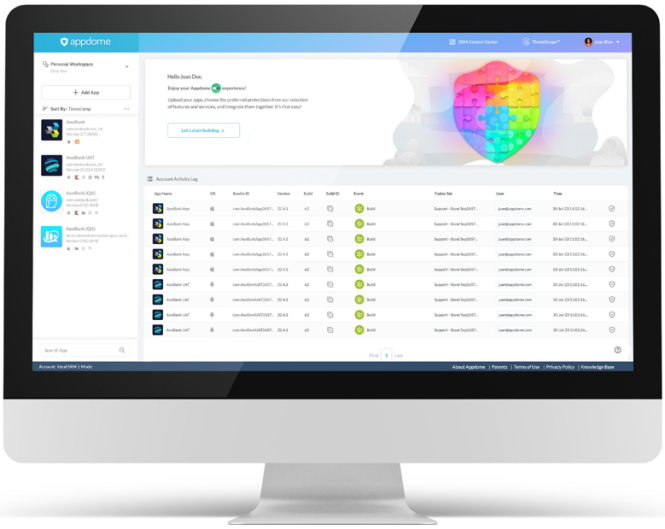
Android malware includes any malicious programs and tools unintended by the app's developers and designed to harm users, steal data, gain unauthorized access to accounts, etc. Appdome provides comprehensive protection against Android malware including:

- **Anti-Magisk:** Protect Android apps from all forms of Magisk & custom Magisk modules.
- **Detect Hooking Frameworks:** Protect Android apps from tools that intercept and modify the behavior of the app at runtime.
- **Remote Desktop Control (RDC) Apps:** Prevent misuse of RDC apps like TeamViewer, which attackers abuse to deliver malware and conduct ATOs.
- **Deep Fake Detection:** Protect Android apps from biometric authentication bypass attacks using fake images + social engineering.
- **Android Accessibility & ATM Malware:** Protects from malware, RATs, & Trojans that abuse Accessibility Services, permissions & other mobile functions to trick users into revealing sensitive data or performing harmful actions.

Android malware defenses are often part of a larger mobile app defense strategy. Combine the above Android anti-malware features with any or all of Appdome's 300+ other mobile app defenses including mobile app security, anti-fraud, anti-cheat, anti-bot, geo compliance features and more.

ONE SOLUTION FOR ALL YOUR MOBILE APP DEFENSE NEEDS.

Appdome's Unified Mobile App Defense platform provides a one-stop shop to protect your mobile apps, save money on mobile app defense, and deliver beautiful user experiences when attacks happen.



THREATSCOPE™ MOBILE XDR

ThreatScope™ Mobile XDR provides mobile brands, developers and cyber professionals extended detection and response (XDR) for Android & iOS mobile apps. ThreatScope Mobile XDR uses dedicated sensors inside mobile apps, not a separate agent or app on the end user's mobile device. These sensors provide real-time, continuous monitoring of 1000s of unique attack vectors, giving mobile brands real-time visibility into the entire range of threats and attacks impacting their mobile app and users. As an XDR, ThreatScope also provides the power to respond to attacks instantly build-by-build, and release-by-release. Inside ThreatScope, organizations can (1) see and analyze the top mobile app threats and attacks impacting the mobile channel, (2) prove the value of the Appdome defenses deployed in mobile apps (3) make data-driven decisions of what protections to deploy in each release, and (4) create customized views and comparisons to report on threats and attacks impacting different parts of the mobile business.

UNIFIED MOBILE APP DEFENSE

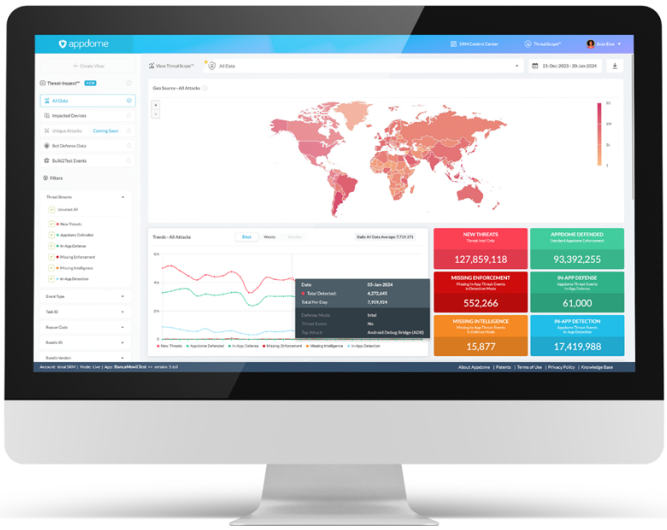
Appdome's patented Unified Mobile App Defense platform provides mobile developers, cyber security and fraud teams a centralized automation, monitoring and control center for protecting mobile apps. With Appdome, choose, build, test, release and monitor any or all of Appdome 300+ mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and other defense features in Android or iOS apps with ease. Maintain full compliance control over the defense lifecycle and enjoy complete compatibility with the entire tech stack used in mobile development, DevOps, and DevSecOps.

THREAT-EVENTS™ CONTROL FRAMEWORK

All of Appdome's runtime and dynamic protections come enabled with Threat-Events™, Appdome's in-app attack intelligence and 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 deliver beautiful user experienceswhen each attack occurs.

CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Build-by-build, mobile apps are Certified Secure™ to guarantee the mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and threat intelligence features are embedded, active and protecting the mobile app. Cybersecurity and mobile dev teams use Certified Secure™ as a continuous record of compliance and as the DevSecOps artifact to clear mobile 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 Mobile App 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.

AAM-SG-05202024