appdome

Unified Mobile App Defense

BETTER ANTI-INJECTION ATTACK IN CI/CD

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

DELIVER ANTI-INJECTION ATTACK 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 Anti-Injection Attacks in apps, fast. Here's what you get by combining Appdome with CI/CD:

RAPID RELEASE & DELIVERY, ANTI-INJECTION ATTACKS

Getting anti-injection attack protection in mobile apps right requires releasing dozens of unique defenses in Android & iOS apps fast. With Appdome, you do just that. Instead of needing engineering resources and work, you build anti-injection attack features in Android & iOS apps on-demand. From the CI/CD, trigger the build command in Appdome and release anti-injection features 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 APPLICATIONS

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 anti-injection attack feature to the changes in the updated mobile app. Release by release, no manual work, retooling, or coding change are needed to make anti-injection attack 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 anti-injection attack 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 anti-injection attack and other defenses in mobile applications. With Appdome, anti-injection attack features are delivered without resource dependencies or compatibility limitations. In addition, anti-injection attack 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 ANTI-INJECTION ATTACK FEATURE COVERAGE

Appdome's anti-injection attack solution prevents injection of malicious code into mobile app running processes, memory, libraries, and more. Appdome also blocks the methods and tools used for injection, including hooking, memory editing, script injection, etc.

- **Prevent Code Injection:** Defend against code, process, and library injection, including shell code injection and shared object, dylib, and reflective DLL injection.

- **Block Memory Editing:** Block all methods and tools used to inject code into mobile app memory, alter values, or cheat in mobile games.

- **Prevent Hooking & Swizzling:** Prevent interception of method calls and runtime modification of app behavior.

- **Prevent Auto-Clicking & Keystroke Injection:** Stop tools and methods used to inject fake clicks, keystrokes or events into apps, where attackers attempt to imitate user actions.

- **Anti-Frida:** Detect all forms of Frida, including Frida gadget, objection, inject, custom Frida, and more.

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

appdome

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.
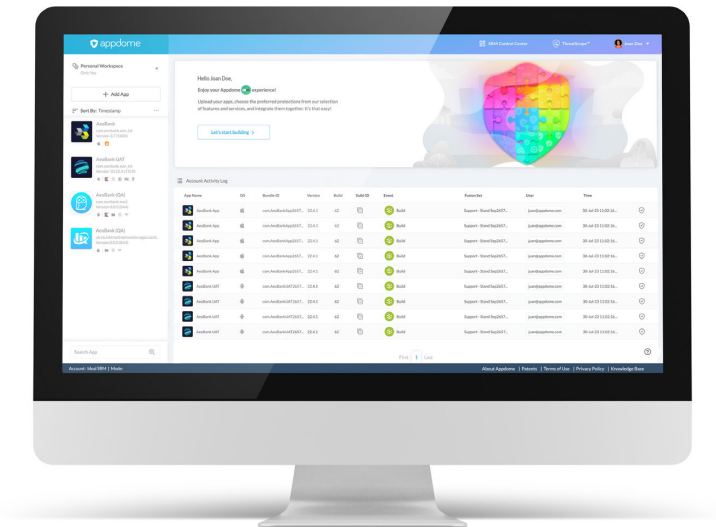
THREATSCOPE™ MOBILE XDR

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 beautiful user experiences when 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.