appdome

Unified Mobile App Defense

BETTER MOBILE SDK PROTECTION IN CI/CD

Continuously build, test, monitor and respond with Mobile SDK Protection in Android & iOS mobile SDKs in one platform in CI/CD.

DELIVER MOBILE SDK PROTECTION AT DEVOPS SPEED

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

RAPID RELEASE & DELIVERY, MOBILE SDK PROTECTION

Mobile SDKs are integral to the mobile app economy, enabling faster development and enhanced app capabilities. Protecting SDKs has been a significant challenge, with manual coding options providing only minimal protection and lacking badly needed visibility and data on threats to the SDK. To effectively secure mobile SDKs, it's crucial to extend protection to the SDKs within apps and to do so in a way that fits within the dynamic and fast-paced environments in which Android and iOS apps are built and delivered.

With Appdome, achieving comprehensive and continuous protection for mobile SDKs is streamlined. Instead of relying on extensive engineering resources and timelines, you can seamlessly build mobile SDK protection into your Android and iOS SDKs on demand. From the CI/CD, trigger the build command in Appdome and release mobile SDK protection in mobile apps either all at once or in an iterative release process to respond to new threats as they emerge and instantly match the needs of the business.

CONTINUOUS DETECTION & RESPONSE

SDK developers require real-time data and feedback on each iterative release of a mobile SDK. Appdome provides real-time Threat-Monitoring and Threat-Streaming so you can monitor all threats and attacks against SDKs as they occur, and create custom responses based on attack metadata being fed back to the SDK's backend. This provides SDK makers unprecedented visibility on all attack vectors impacting the mobile SDKs, revealing the impact of each defense and the total active attack surface against your SDKs in real-time. Armed with this data, SDK makers can click-to-add new protections or update back-end enforcement models to keep the mobile SDK and users safe.

COMPLIANCE TRANSPARENCY & CONTROL

Continuous compliance transparency and control over each step of the build, test, and release lifecycle for mobile SDKs 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 SDK protection, change, detection, and telemetry event. Build by build, each mobile SDK is Certified Secure™ compliant with the necessary protections added to the SDK in the CI/CD pipeline.

"BEST OF SUITE" COST SAVINGS & CONSOLIDATION

Appdome offers unparalleled cost consolidation and TCO savings for mobile SDK protection. With Appdome, mobile SDK protections are delivered without resource dependencies or compatibility limitations. Eliminate point products, multi-vendor integration risk and complexity, and streamline release cycles for mobile SDK defenses.

FULL MOBILE SDK PROTECTION FEATURE COVERAGE

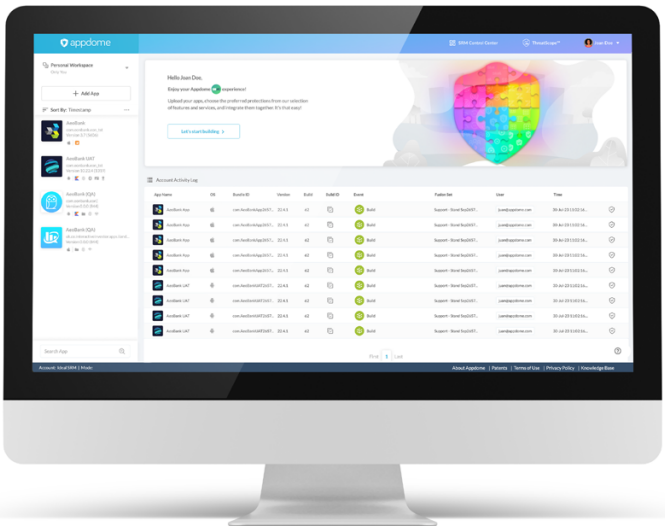
Make mobile SDKs compliant and threat-aware with Appdome SDKProtect™ to meet internal or external security requirements, such as EMVco and PCI DSS. Deliver comprehensive mobile SDK protection without engineering work:

- **SDK Threat-Shielding:** Protect SDKs from reverse engineering and tampering attempts to compromise the SDK. Obfuscate SDK logic, and encrypt SDK data, strings, resources, and preferences. Prevent MitM attacks and enforce the use of secure TLS versions.
- **Mobile Risk Evaluation:** Comprehensive coverage across all SDK attack vectors, including facial recognition bypass prevention, root and jailbreak detection, emulator detection, preventing hooking frameworks, debuggers, ADB abuse and 300+ other protections available on Appdome.
- **Threat-Monitoring:** Real-time attack monitoring of Mobile Risk Evaluation features via ThreatScope™, the industry's only agentless mobile XDR solution.
- **Threat-Streaming:** Stream real-time threat data to the SDK's back-end services, allowing developers to create customized in-app threat responses or modified workflows when attacks against the SDK are detected.

Mobile SDK protections are critical to meet internal security requirements, industry regulations, and protecting the mobile app economy. Combine the above mobile SDK Protection features with any or all of Appdome's 300+ other mobile app defenses including mobile app security, anti-fraud, anti-malware, anti-MiTM, anti-cheat, anti-bot, social engineering prevention, geo compliance features and more.

ONE SOLUTION FOR ALL YOUR MOBILE APP DEFENSE NEEDS.

Appdome's Unified Mobile 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 and SDKs. ThreatScope Mobile XDR uses dedicated sensors inside mobile apps and SDKs, 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 SDKs, apps 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 SDK DEFENSE

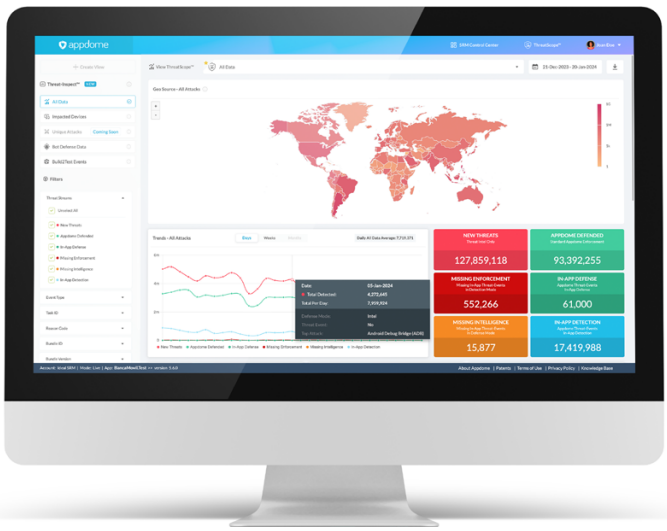
Appdome's patented Unified Mobile Defense platform provides mobile developers, cyber security and fraud teams a centralized automation, monitoring and control center for protecting mobile apps and SDKs. With Appdome, choose, build, test, release and monitor any or all of Appdome 300+ mobile app security, 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 and SDK 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 or SDK and use the detection and defense data to deliver beautiful user experiences when each attack occurs.

CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Build-by-build, mobile apps are Certified Secure™ to guarantee the mobile SDK protection, mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and threat intelligence features are embedded, active and protecting the mobile SDKs. 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.

SDKP-SG-0604024