

appdome

App DEFEND™

360° No-Code Protection for Mobile Apps, Data, Users and Businesses.



WHY PROTECT YOUR MOBILE BUSINESS?

Today, everyone - from consumers, gamers, frontline and essential workers, to first responders and soldiers – all rely on mobile apps to live, buy, save and work. Hundreds of millions of terabytes of data, as well as hundreds of millions of dollars, flow through mobile apps because mobile apps are where people and businesses meet, share and transact.

Hackers know mobile apps have all the information and data needed to carry out exploits. They also know that mobile apps are vulnerable entry points into broad based attacks against the backend or users. Protecting the mobile business requires protecting the mobile app, the data, the connections and the people that use the mobile app. This protection is critical to business continuity, as well as economic and enterprise stability and growth.

INTRODUCING APPDOME APP DEFEND™

Appdome App DEFEND is the industry's only 'all-in-one', no-code security solution capable of protecting mobile apps and businesses end-to-end. With App DEFEND, developers and app makers can quickly and easily protect mobile businesses, by protecting the app, connections, data and users against all mobile threats, hacking attempts, mobile fraud, account takeovers, ransomware, identity and credential theft, credential stuffing and other backend network attacks.

WHY APPDOME APP DEFEND?

Appdome App DEFEND brings Appdome's industry leading, no-code security offerings together in one comprehensive mobile app security solution.

Here are the top features of App DEFEND:

ONEShield™ App Hardening – Comprehensive mobile app shielding and hardening solution that prevents dynamic analysis, tampering, modifying, debugging or interfering with the app's workflows as well as blocks emulators and simulators.

TOTALCode™ Obfuscation – Complete code obfuscating solution that prevents static analysis, obfuscates the entire binary, native code and non-native code/libraries, SDKs and frameworks in the app, protects control flows and strips debug information in the app.

TOTALData™ Encryption – AES-256 or FIPS 140-2 Data-at-Rest Encryption for all data stored by the mobile app, in the app sandbox, SD Card and file system, as well as encryption for app preferences, app secrets, XML and other strings, resources and DEX files (Java classes).

OS Security Integrity – Prevents the app from running on rooted and jailbroken environments, root hiding, root and jailbreak tools, and hacking and cheat engines that rely on root and jailbreak.

MiTM Protection – Protects all mobile data in transit from network-based attacks with active man-in-the-middle detection and prevention, including forged certificates, malicious redirection or proxies as well as adds secure certificate pinning and client certificates (for bot prevention). Dozens of enforcement options are available.

Mobile Privacy and Data Loss Prevention – Protects mobile end users' data and prevents data loss by preventing malicious keyloggers, restricting screensharing, screenshots and recording.

THE BUSINESS CASE FOR APPDOME

Advantages of No-Code Mobile App Security

Appdome is the industry's only 100% no-code mobile app security platform. Using Appdome, developers and security teams eliminate the technical complexities and resource constraints that come with DIY and SDK security. Security teams meet their goals with ease and developers have complete freedom to use any development environment, framework and methods inside Android and iOS apps.



With each build, Appdome does what no other vendor can. It certifies the security implementation added to each app.

DIY and SDK security products cannot certify the security features added to apps because all the implementation burden is on others (not the vendor).

Certified Secure gives developers the trust and confidence that their apps are protected with the features needed for their business, and reduces time and expense spent on penetration testing and vulnerability scans.

Challenges of DIY Mobile App Security

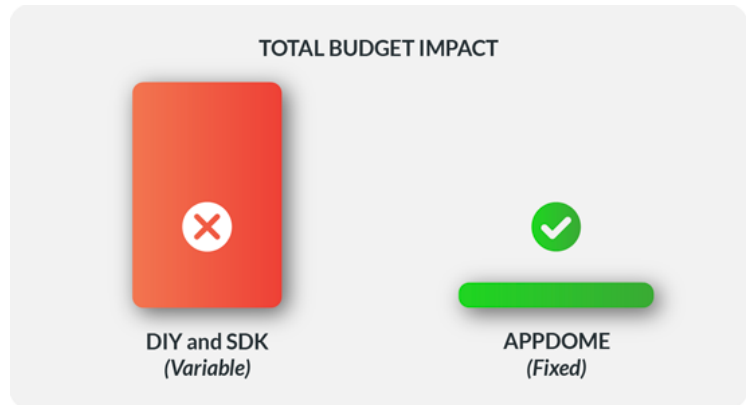
Most organizations underestimate the challenges of building and maintaining security themselves, including using SDK-based security products. Are you really ready for Do-It-Yourself (DIY) security? To find out, answer the following questions:

- Do you have the engineering skills and expertise to code security in your app?
- Will your engineers be continually available to secure the app, release by release?
- Will you wait or hold up releasing your app if you can't finish coding security on time?
- Are frameworks and methods in the app compatible with the chosen security SDK?
- Has your company ever faced urgencies such as failed audits, attacks, exploits or customer commitments that require security?

If you answered **NO** to any of the above, you should not attempt to use DIY and SDK based security.

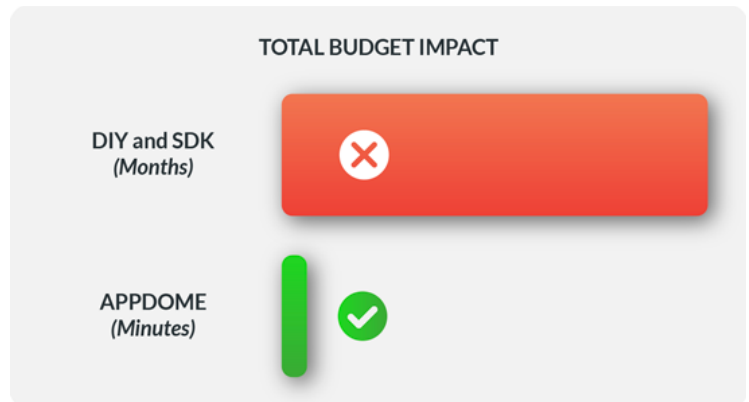
Lowest Total Budget Impact

Appdome's patented technology and security automation platform delivers fast, consistent and repeatable mobile app security at a fixed price. This zero-dev and fixed cost model provides a 10x advantage to security and development budgets by eliminating the variable dev and headcount costs, and the uncertain outcomes, that are associated with DIY coding of mobile app security.



Fastest Time to Market

Appdome accelerates time to market by reducing the time to secure Android and iOS apps, data and users to mere minutes. Organizations no longer need to choose between longer or blocked release cycles or compromising on security. Appdome fits within existing app pipelines and CI/CD processes, provides direct build-to-publish APIs, removes any coding dependencies, and allows users to apply approved security templates, build-by-build, across 1, 10, 100 or 1,000s of apps, simultaneously.



ABOUT APPDOME

Appdome's mission is to protect the mobile economy and the people who use mobile apps in their lives and at work. Appdome's industry defining no-code mobile security and solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new mobile security, mobile threat, mobile fraud and enterprise authentication, access, UEM/MDM/MAM and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 200+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.