PRICING PACKAGES

appdome
App PROTECT™

No-Code Protection for
Android and iOS Apps and Data

WHY PROTECT THE MOBILE APP & DATA?

Mobile apps are the primary way people shop, save, game, invest, communicate, entertain, order and receive healthcare. To make apps useful and personalized, they need lots of data from and about your business and the users of mobile apps.

Mobile apps must contain the business logic and access points to download and use tons of business and user information. Each app contains all the data created by the app and the user, service domains and URLs, APIs and API keys, external services and SDKs, app permissions, communication methods, as well as the certificates used to establish "trust" between the app and its backend. When users interact with the mobile app, the app creates and stores data, including personally identifiable information (PII), user credentials, passwords, account information, payment methods, preferences, account histories and more.

Hackers, good and bad, focus their efforts on exploiting the gaps in the protection used in your apps. To stop these attacks, protecting the app and the data in the app is critical.

INTRODUCING APPDOME APP PROTECT™

Appdome App PROTECT is designed to protect your mobile app, its data and the end users' data from attempts to access, modify, copy or steal it, including detection and prevention of all the methods and tools hackers use to reverse engineer your app or weaken your defenses. App PROTECT also protects your app against malware and cheat engines that rely on Jailbreak and Root to launch attacks. Whether your goal is to pass a pen test, security audit or simply stop hackers from exploiting your app and its data, Appdome App PROTECT is the right choice for you.

WHY APPDOME APP PROTECT?

App PROTECT provides the industry's only no-code mobile app security solution capable of protecting any Android and iOS mobile app and its data from exploit and compromise. It is perfect for blocking static and dynamic analysis tools, passing pen tests, stopping hackers who attempt to access or harvest local data-at-rest, and blocking tools and methods that rely on OS compromise.

App PROTECT includes the following top features from Appdome:

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

TOTALCode™ Obfuscation – Complete code obfuscating solution that 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.

Additional features are available with the App DEFEND™ package.

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

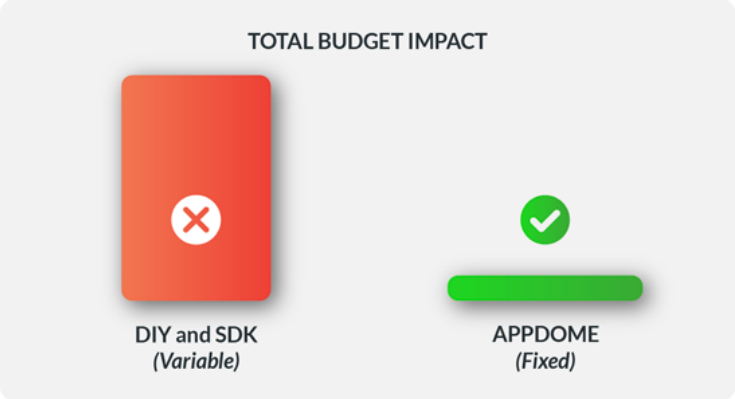
Most organizations underestimate the challenges of building and maintaining security themselves, including using SDK-based security products. Are you really ready for Do-It-Yourself (DIY) security? To find out, answer the following questions:

- 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.

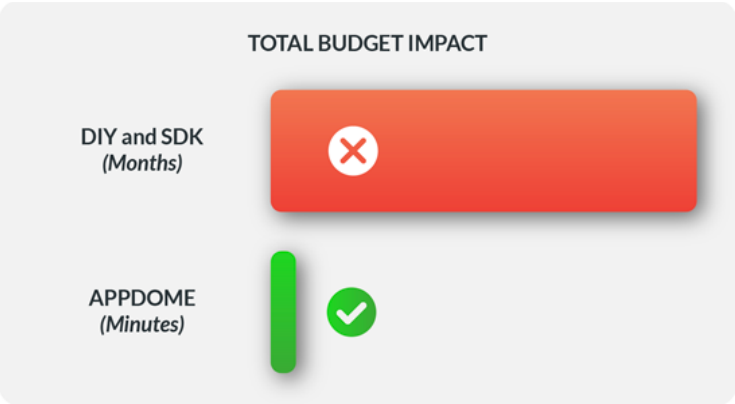
Lowest Total Budget Impact

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.