appdome

MobileTRUST™ Delivers Guaranteed Mobile Commerce

Don't let credential theft, MiTM, bots and other mobile attacks or unsecure data destroy consumer confidence in your mobile apps and your brand.

GUARANTEED M-COMMERCE WITH APPDOME MOBILETRUST

Appdome's MobileTRUST provides a simple and comprehensive solution to protect mobile apps. By providing anti-tampering and code obfuscation, runtime application self-protection (RASP) and more. MobileTRUST allows developers and others to complete mobile app security projects in minutes, with no code or development required.

MobileTRUST utilizes 5, non-cascading layers to give apps the defense-in-depth they need whether the goal is to eliminate mobile vulnerabilties such as the OWASP Top 10, ensure safe mobile transactions, create brand trust among your cliens, or comply with regulations like PCI, PDS2 and GDPR.

- Shielding and hardening apps against hacking;
- Encrypting mobile app data in all three states (at rest, in transit and in memory);
- Obfuscating all code, including app logic, flow, strip debug symbols, non-native files and 3rd party SDKs;
- Protecting data-in-transit and mobile APIs;
- Preventing apps from running on non-secure devices.

BEST LINE OF DEFENSE - MOBILE APP

All mobile attacks, such as credential theft, credential stuffing, man-in-the-middle (MiTM) attacks, data theft, identity theft, malicious bots and more begin with the app itself. Hackers use unsecured mobile apps to create micro-breaches in user's accounts, steal information and exploit the app vendor's systems.

The OWASP Mobile Top 10 recommends the basic security needed in every mobile app. Some mobile commerce rules go beyond the Top 10, adding security requirements in specific jurisdictions or transactions. All of these rules make it clear, protecting the mobile app and the mobile app backend is a necessity.

Micro-breaches are commonplace and every mobile consumer is at risk. Unfortunately, manually implementing 10+ security methods in a mobile app isn't easy. Often, developers have to try and stitch together different methods, from different vendors, each of which may not be compatible with the other. The result is often project failure, leaving the app vulnerable.

Over half of all consumers now use mobile apps daily to purchase, save, invest, redeem and send money to others. Because of this, mobile commerce or M-Commerce is predicted to grow to $250B by 2021. At the same time, only a fraction of mobile apps put into the hands of end users have the protections needed to safeguard user credentials, mobile transactions, personally identifiable data and more.

INSTANT PROTECTION, NO CODING

Appdome MobileTRUST gives app makers the power to ensure brand safety, protect mobile app data, mobile transactions, new transaction types and new currencies without having to go through the manual efforts required to code these critical security capabilities into mobile apps.

Appdome's integration platform allows customers to achieve their outcomes predictably and quickly. The process is simple. Upload an app binary (.apk or .ipa). Select the desired security options and click "Build My App." Appdome leverages a proprietary AI-Mobile Integration coding engine to handle the rest.

Appdome is 100% compatible with all Android and iOS native, cross-platform, hybrid and non-native apps, developed in any framework, without dependencies. You can integrate Appdome with any CI/CD system, for complete automation of the customization process.

APPDOME MOBILETRUST™ - A LAYERED DEFENSE FOR M-COMMERCE APPS

Advanced App Shielding

ONEShield™, Appdome's comprehensive app shielding technology, prevents hackers from debugging, tampering with or reverse engineering an app. With Appdome, even the most sophisticated hacker cannot understand how an app functions. Additionally, key logical elements and resources such as methods, protocols and assets are encrypted, making reverse engineering infeasible.

ONEShield also performs checksum validation by calculating a unique hash of binary data and assets and validating them at runtime. This prevents unknown or unintended changes to an app.

360° Data Encryption

TOTALData™ Encryption protects mobile app data in all the three states in which it exists; at rest, in transit and in use. TOTALData Encryption eliminates the need for developers to design, build and maintain encryption inside mobile apps. TOTALData Encryption automatically encrypts all or selected mobile app data, regardless of how that data is generated or where it's stored in the app. With Appdome, extensive options are available for managing and controlling the encryption methods and keys in apps.

360° Code Obfuscation

TOTALCode™ Obfuscation provides a complete binary-based obfuscation, agnostic to build system, tools and source code languages. With no development effort, and a click of a button, an entire app binary can be obfuscated – protecting the implementation, code, framework, structure, logic, strings and secrets contained in the app. No other obfuscation method on the market comes remotely close to achieving a similar outcome, all without accessing the source code.

Man-in-The-Middle Protection

Appdome appSECURE™ protects data in transit from malicious proxies and MiTM attacks, blocking unauthorized or unknown parties from being redirected to a server or proxy. By keeping track of SSL sessions and validating the CA authenticity at runtime, Appdome delivers protection whether the proxy is internal or external to the mobile device. Developers can also prohibit stale sessions and Session IDs from being reclaimed and reused by unauthorized users.

Appdome apiSECURE™ protects the mobile APIs in the app by pinning CA files to a mobile app and webserver, ensuring that only valid apps can connect to the backend. Other options include enforcement of Cipher Suites, TLS versions and Certificate Roles, manage IP address visibility and pin static client certificates to apps to authenticate client connections using a flexible MicroVPN gateway.

OS Integrity

Jailbreak/Rooted Protection detects if a device has been jailbroken (iOS) or rooted (Android), upon which apps can be configured to Exit or another orchestrated command using Appdome DEV-Events, thus preventing protected apps from running on non-secure devices. Appdome's protection enforces the configuration when the user launched the app, as well as in situations where a device is jailbroken/rooted after the app is already installed and running.

Detect Unknown Sources detects if a mobile device has been set to allow app installs from "unknown sources." If the setting has been enabled, apps can be configured to Exit.

100% No-Code

ZERO Code Mobile App Security allows developers to upload an app (.apk or .ipa), select the desired security options and click "Build My App." Appdome uses AI to build the target features in the app in 30 seconds or less. Appdome is 100% compatible with all Android and iOS native, cross-platform, hybrid and non-native apps, developed in any framework, without dependencies..

Learn more about Appdome MobileTRUST at **www.appdome.com**.
Open a free Appdome account at **fusion.appdome.com** and start securing your apps!

ABOUT APPDOME

Appdome is the industry's first no-code mobile integration platform. Appdome's patented*, Fusion technology and its AI-Digital Developer™, known as AMI, powers a self-service platform that allows anyone to complete the integration of thousands of mobile services, standards, vendors, SDKs and APIs in security, authentication, access, mobility, mobile threat, analytics and more, adding these services to any mobile app instantly. Leading financial, healthcare, government and e-commerce providers use Appdome to deliver rich mobile experiences, eliminating development complexity and accelerating mobile app lifecycles. For more information, visit www.appdome.com.

*Yehuda et al. Method and system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.