appdome

ALL-IN-ONE MOBILE APP SECURITY

DYNAMIC, SELF-DEFENDING MOBILE APPLICATION PROTECTION - NO CODING REQUIRED

Appdome's All-in-One Mobile App Security is a no-code, layered, best practice mobile security solution that can be added to any Android or iOS app in minutes. Mobile developers can add sophisticated runtime application self-protection (RASP) features like anti-tampering, anti-debugging, code obfuscation, data encryption and more, to apps quickly and easily. This prevents malicious threats to mobile users, apps and data and protects the app against all OWASP Mobile Top 10 risks. Appdome-built apps are self-defending and provide protection from the ground up from hacking attempts designed to disable the security features in the app. Every feature in Appdome's Mobile Security Suite is applied directly to the app binary. Each implementation is unique to each app, framework and language used to build the app, dynamically providing different implementations across the life of the app.

TOTALDATA™ ENCRYPTION

Data at Rest Encryption

Protects mobile app data with dynamic AES 256-CTR (industry standard cryptographic protocols), without any dependencies on data structure, databases or file structures. Discrete blocks of data are encrypted and placed in a self-contained and segregated environment to isolate mobile app data from other resources. Encyrption keys are dynamically managed and changed with every build. This makes it impossible for a non-authorized user to decrypt and open this encrypted data.

Encrypt Strings and Resources

Encrypt all the apps' constants, strings and runtime information, removing critical loopholes hackers use to infiltrate apps.

Encrypt In-App User Preferences

Encrypt preferences such as username, email, contact info and other PII data that are otherwise stored in the clear inside an app, ensuring user and resource privacy inside of the app.

XMLEncrypt™ and APPCode Packer

Unique for Android apps, XMLEncrypt encrypts all sensitive strings.xml values and APPCode Packer hides and encrypts all the app's java classes (dex files). This eliminates the component hijacking vulnerability in apps without impacting performance.

Encryption Control

Customers who require a greater level of control over their mobile data encryption implementations can use encryption control. This allows them to seed the encryption keys, enable data in use (in memory) encryption and others.

FIPS 140-2 Cryptographic Modules

Use FIPS 140-2 certified cryptographic modules for data at rest encryption and network connections.

OPERATING SYSTEM INTEGRITY

Jailbreak and Root Protection

Detects if a device has been jailbroken (iOS) or rooted (Android). If the device has been jailbroken or rooted, Appdome-secured apps can be configured to shut down or "exit." Developer options also allow users to create in-app workflows for this event.

Detect Unknown Sources and Developer Options

Specifically for Android devices, an Appdome-secured app can detect if a mobile device has been set to allow app install from "unknown sources" or has enabled "developer options."

SECURE COMMUNICATION

MitM Prevention

Appdome's MitM prevention for Android and iOS apps validates the authenticity of the SSL certificate used by the destination server to ensure that the certificate has not been forged or compromised. This prevents mobile apps from connecting to untrusted, unknown or malicious destinations. In addition, Appdome offers advanced session control settings such as enforcing Cipher suites and TLS version to prevent the use of weak or outdated encryption and to prevent hackers from exploiting weaknesses in the app's encryption model.

Secure Certificate Pinning

Appdome's Secure Certificate Pinning prevents mobile apps from connecting to compromised servers or endpoints. It encrypts and securely stores the certificate(s) of known trusted servers in the app and validates the certificate before the connection is established. If there is a certificate mismatch, the session is denied or dropped.

Bot Defense

Appdome's Bot Defense prevents bot attacks against the mobile backend with Mobile Client Certificates and Shared Secrets.

ONESHIELD™ APP SHIELDING

Anti-Debugging

Appdome's comprehensive app shielding blocks debugging tools from reading an app's code. Appdome's anti-debugging counters and stunts malicious dynamic reverse-engineering attempts.

Detect Debugger Code Manipulations

Appdome actively detects and blocks code manipulations or injections performed by debuggers on the protected app during runtime. (Android only)

Detect App is Debuggable

Detect if an iOS app has been re-signed with a certificate with debug entitlements. Detect if an Android app is declared as debuggable in the AndroidManifest.xml file.

Anti-Tampering

Appdome's anti-tampering protection prevents any unwanted changes, mods and hacks. ONEShield seals an app and actively detects modifications during initialization and at multiple points during runtime.

Multi-layered Checksum Validation

Appdome uses 1000s of overlapping checksum validations to calculate a cryptographic hash and validates the hash at runtime, detecting any modifications to the app, app resources, configuration elements and more.

App Integrity and Structure Scan

Check an app's composition, data structure, data elements, and communication paths to validate the integrity and authenticity of the app. It also detects elements within the app which could be used as attack vectors such as unknown or malicious URLs.

Anti-Reversing

With Appdome, even the most sophisticated hacker cannot understand how apps work. Apps are shielded from changes and modifications by others. Additionally, key logical elements and resources such as methods, protocols and assets will be encrypted to make reverse engineering impossible.

Obfuscate Built Services

Shields Appdome's code and the new customer-selected services added to the app during the Appdome build process. In addition, the data embedded in Appdome's code will be encrypted, to prevent common "recon" attacks (like searching for strings in the code).

Prevent Running on Emulators and Simulators

Appdome prevents dynamic code analysis, including running the app on an emulator or simulator to observe the app's behaviors and study how the app functions in a running environment.

TOTALCODE™ OBFUSCATION

Binary Based Obfuscation

Appdome's proprietary binary-based obfuscation method obfuscates the entire app binary, including the framework and non-native filesystems, without source code or developer implementation.

Non Native Code Obfuscation

Appdome protects the entire app, including apps built in Cordova, React Native, Xamarin and other modern frameworks.

Advanced Obfuscation Instrumentation

Advanced features include Flow Relocation to obfuscate control flows and business logic across the binary, without the need to code or expose source code.

Strip debug symbols removes source code file names, line numbers, and variable names.

MOBILE PRIVACY

Copy/Paste Prevention

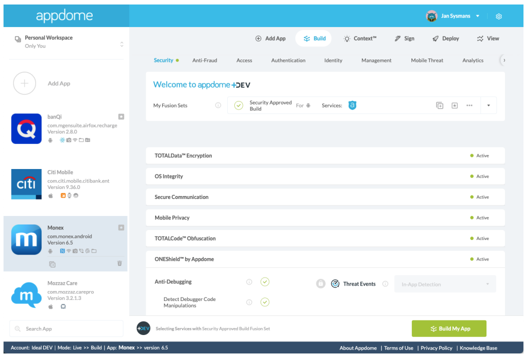
Prevents app data from being copied and pasted outside of the app. Copy/Paste is available between Appdome-secured apps.

Prevent App Screen Sharing

Prevents taking screenshots, mirroring and sharing the app's screen and hides the preview thumbnail when minimized.

THREAT EVENTS™

With Threat Events, mobile app developers can code their mobile apps with the ability to take specific actions based on events that happen in the app or on the device. Effectively, they are giving their mobile apps the operational intelligence to act independently (i.e., without the need for an external policy service) when security events happen. Threat Events is available for several security categories in the Appdome Mobile Security Suite.



Welcome to appdome +DEV

My Fusion Sets: Security Approved Build For Services:

TOTALData™ Encryption	Active
OS Integrity	Active
Secure Communication	Active
Mobile Privacy	Active
TOTALCode™ Obfuscation	Active
ONEShield™ by Appdome	Active

Anti-Debugging ✓ Threat Events In-App Detection

Detect Debugger Code Manipulations ✓

Selecting Services with Security Approved Build Fusion Set

Account: Ideal DEV | Mode: Live >> Build | App: Monex >> version 6.5 About Appdome | Terms of Use | Privacy Policy | Knowledge Base

Image: Appdome's Mobile Security Suite provides a layered defense against security threats.

Learn more about Appdome's All-in-One Mobile App Security at **www.appdome.com**.
Open a free Appdome account at **fusion.appdome.com** and start securing your apps!

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 Fraud Prevention platform uses a patented, artificial-intelligence based, no code technology to power a self-serve DevSecOps service used to secure, defend and protect mobile apps from reverse engineering, data exploits, OS and device level threats, dynamic and static analysis, MiTM attacks, mobile fraud, mobile malware and mobile piracy. Over 25,000 unique combinations of mobile security and fraud prevention features, SDKs and APIs are available on Appdome. Over 200+ leading financial, healthcare, government, and m-commerce providers use Appdome to protect apps, users and data, preempt fraud, and consistently deliver richer and safer mobile experiences to hundreds of millions of mobile end users globally.

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