DATASHEET

appdome

MOBILE SECURITY SUITE

COMPLETE SELF-DEFENDING MOBILE APPLICATION PROTECTION - NO CODING REQUIRED

Appdome's Mobile Security Suite is a comprehensive, layered, best practice mobile security feature set that can be added to any Android or iOS app in minutes. Mobile developers and non-developers alike 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-build apps are self-defending and provide protection from the ground up from tampering, altering, reversing and other 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 - no source code or coding required. Key features of Appdome Mobile Security Suite are:

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. 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 information and other PII data that are otherwise stored in the clear inside an app, ensuring user and resource privacy inside of the app.

APPCode Packer

The industry's first no-code Android App Packer hides and encrypts all Java code of an Android app. This eliminates the component hijacking vulnerability in Android apps. APPCode Packer does not impact app 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.

MOBILE PRIVACY

Keylogging Prevention

Prevents the use of a non-trusted keyboard in the app. Default setting is to only use the OS built-in keyboard.

Copy/Paste Prevention

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

Prevent App Screen Sharing

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

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-Built 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, Developer Options, and Emulators

Specifically for Android devices, an Appdome-Built app can detect if a mobile device has been set to allow app install from "unknown sources" or has enabled "developer options." Additionally, Appdome-Built apps can be prevented from running on an "Emulator". If enabled, Built apps can be configured to shut down.

SECURE COMMUNICATION

Trusted Session

Protects against malicious proxies and Man-in-the-Middle (MiTM) attacks. Detects if a session is intercepted by an unauthorized or unknown party and redirected to a server or proxy. By keeping track of SSL sessions and validating the Certificate Authority's (CA) authenticity as it is being sent, it delivers malicious proxy detection whether the proxy is internal or external to the mobile device. It can also prohibit state sessions to prevent authorized session reuse and SessionID reclaiming.

SecureAPI™

Secures all the APIs in the mobile app, regardless of vendor or workflow. SecureAPI will encrypt and obfuscate the API keys, the API secrets and the strings that denote the use of the API. SecureAPI also protects and secures the payload of the API, without relying on the security of the API vendor.

SSL Certificate Validation

Verifies certificates and CAs to ensure that apps are only communicating with trusted sites with valid and authentic certificates.

Manual Whitelisting

To limit app access to just a handful of known sites, those site addresses can be specified for the app. When that is done, all other sites will be blocked.

Hostname Verification

Some apps don't verify hostnames in their certificate pinning schemes. This exposes the app to possible MiTM attacks. Appdome verifies hostnames for all CAs to protect our customers' apps against MiTM attacks.

Session Control*

Customers who require a greater level of control over their secure communication implementations can use session control. This allows them to pin a trusted CA to the app and the webserver. Session control can also enforce cipher suites, TLS version, strong RSA and ECC signatures, SHA256 digest and certificate roles. It can also make real IP address visible to the app and pin a static client certificate to the Appdome-Built app to authenticate client connections on the MicroVPN gateway.

ONESHIELD™ APP SHIELDING

Anti-Debugging, Anti-Tampering and Anti-Reversing

Appdome's comprehensive app shielding prevents app debugging, tampering with or reverse engineering. 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.

Checksum Validation

Appdome performs checksum validation to calculate a unique hash or fingerprint of binary data and assets and validates them at runtime. This prevents changes to an app, its resources, code, configuration and more.

Prevent Running on Simulators

Protects the app by restricting app install and execution to physical mobile devices only.

Obfuscate Built Services

Appdome's proprietary binary-based obfuscation method obfuscates Appdome-Built services added to an app. This protects service implementations against hacking and reverse engineering.

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.

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

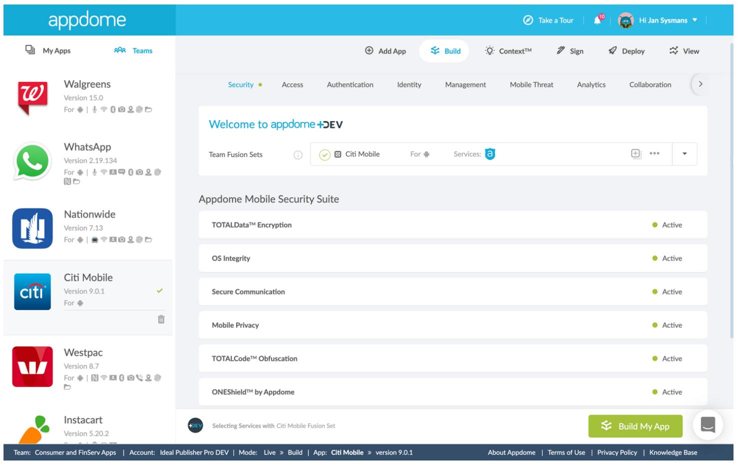
Advanced features include Flow Relocation to obfuscate control flows and business logic across the binary, without the need to code or expose source code.

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

DEV-EVENTS™

With DEV-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.

DEV-Events is available for all the security categories in the Appdome Mobile Security Suite.



Walgreens
Version 15.0

WhatsApp
Version 2.19.134

Nationwide
Version 7.13

Citi Mobile
Version 9.0.1

Westpac
Version 8.7

Instacart
Version 5.20.2

Welcome to appdome +DEV

Team Fusion Sets: Citi Mobile For Services:

Appdome Mobile Security Suite

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

Selecting Services with Citi Mobile Fusion Set

Team: Consumer and FinServ Apps | Account: Ideal Publisher Pro DEV | Mode: Live » Build | App: Citi Mobile » version 9.0.1

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

* Requires Appdome-DEV license

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

ABOUT APPDOME

Appdome changes the way people build mobile apps. Appdome's industry defining no-code mobile solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new security, authentication, access, enterprise mobility, mobile threat, analytics 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 150+ 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.

For more information, visit www.appdome.com

*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.