DATASHEET

appdome ONESHIELD™

Create self-defending mobile apps with advanced app shielding and hardening for Android and iOS, no code or coding required.

THE IMPORTANCE OF SHIELDING THE APP

Appdome's annual state of mobile app security research found that more than 90% of mobile apps lack application shielding. Gartner defines application shielding or app hardening as a set of technologies that make mobile apps more resistant to intrusion, tampering and reverse engineering.

Without app shielding, hackers can change the way an app works, insert malicious workflows, alter text or links inside the app, create fake or malicious versions of the app, and create malicious programs that leverage or abuse the app's logic. A lack of app shielding can result in data exploits, crafted attacks against the mobile end users and backend systems, mobile piracy, app defacing and more. All this can destroy a mobile app business, brand and user trust.

THE IMPORTANCE OF SHIELDING SECURITY

Just as thieves will first disable a burglar alarm before stealing items from a home, hackers will often disable existing protections in mobile apps before carrying out their malicious intent against the app, users and networks. Most security protections, such as SDKs and other methods, lack anti-tampering protection that prevents disabling the security feature itself.

Failing to prevent tampering or disabling any security measures in the app can render any security methods added to the app vulnerable to attack. Imagine spending weeks or months to add a security SDK to your app, only to realize that hackers can identify, discover the inner workings and disable that SDK in your app.

DEPLOY ONESHIELD STANDALONE OR BUNDLED

Appdome's allows users to deploy ONEShield stand alone or in combination with other services added via Appdome's no-code security platform. In addition, SDK partners of Appdome can elect to bundle ONEShield features to protect SDKs added to mobile apps via Appdome, hardening SDKs for the benefit of developers and users.

ALL-IN-ONE APP SHIELDING WITHOUT CODING

Appdome is the best, fastest, and easiest way to shield and harden Android and iOS apps, including native and non-native components in the app. Using Appdome's self-service, no-code SaaS Security platform, developers and non-developers alike can protect mobile apps, and prevent attempts to modify, disable or reverse engineer, everything inside the app bundle, including all native and non-native code, external components, security SDKs and more built into the app. Sophisticated runtime application self-protection (RASP) features like anti- tampering, anti-debugging, anti-reversing, multi-layered checksum validation and more, block attempts to tamper, reverse engineer, or inspect the app using static and dynamic code analysis.

DYNAMIC APP SHIELDING, RELEASE-BY-RELEASE

Appdome automatically builds the app shielding and hardening features of ONEShield, adjusting the protection scheme to the specific app uploaded to the Appdome product. Each implementation of ONEShield is unique to each app, framework and language used to build the app, providing diverse app shielding and hardening implementations across apps and over the life of each app. This presents a unique problem for hackers, who now have to contend with different protection schemes across apps.

Appdome offers two methods to build application shielding and hardening into mobile apps. First, users can simply upload any app binary (.ipa, .apk or .aab) to Appdome, select ONEShield, and click Build my App. Or, users can utilize Appdome's DEV offering and build ONEShield into apps using DEV-APIs, integrated directly into CI/CD pipelines.

1 ONEShield™ by appdome

ONESHIELD™ APP SHIELDING FEATURES

Anti-Debugging

Appdome provides multi-layered debugging prevention that can cause the debugger to crash, terminate specific sessions, prevent connecting a debugger or code injector, or exit the app, all depending on the debug method used by the attacker.

Detect Debugger Code Manipulators

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

Anti-Tampering

Prevents app re-signing and repackaging, as well as attempts to modify the app executable, including any Appdome implementations in the app.

Prevent Simulators

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

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

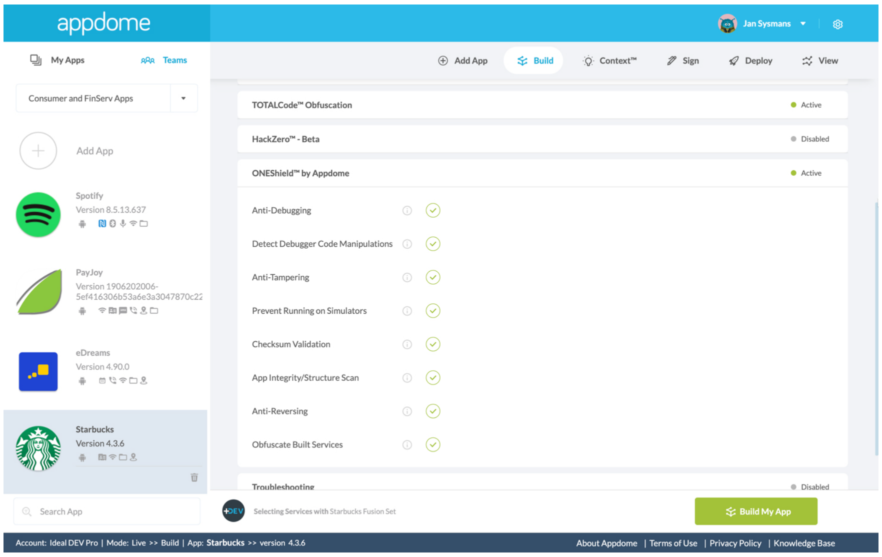
Check an app's composition, data structure, data elements, and communication paths to validate the integrity and authenticity of the app. It also detects elements within the app which could be used as attack vectors such as unknown or malicious URLs.

Anti-Reversing

In iOS apps, this feature obfuscates selector references in the main executable (which prevents the cross-reference searches). In Android apps, this feature obfuscates all plaintext strings in DEX files

Shield Appdome 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).



TOTALCode™ Obfuscation ● Active

HackZero™ - Beta ● Disabled

ONEShield™ by Appdome ● Active

- Anti-Debugging ✓
- Detect Debugger Code Manipulations ✓
- Anti-Tampering ✓
- Prevent Running on Simulators ✓
- Checksum Validation ✓
- App Integrity/Structure Scan ✓
- Anti-Reversing ✓
- Obfuscate Built Services ✓

Troubleshooting ● Disabled

Selecting Services with Starbucks Fusion Set

Account: Ideal DEV Pro | Mode: Live >> Build | App: **Starbucks** >> version 4.3.6

Image: Appdome ONEShield protects and hardens all Android and iOS apps.

Learn more about Appdome ONEShield 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 development and security 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.