appdome

MOBILE MALWARE PREVENTION

No-code mobile malware prevention in a Data-Driven DevSecOps™ build system.

FASTEST & EASIEST WAY TO STOP MALWARE ATTACKS

Deliver fully compatible, in-app, mobile app protections against on-device malware, including malware class tools like Magisk, Jailbreak Bypass Tools, Frida and more in Android & iOS apps. Enjoy full release orchestration & control, and no code, no SDK, no server, threat intelligence and protections, built right inside the DevOps CI/CD pipeline.

BLOCK MAGISK & MAGISK MANAGER

Defend Android & iOS apps from Magisk, Magisk Manager, malicious Magisk Modules, MagiskHide, Magisk Canary, Zygisk as well as malware, cheats and mobile app penetration testing tools that rely on Magisk. Magisk is a very powerful framework, supported by an open-source community of experts, that enables anyone to alter, add and modify files and the operation of a mobile app. Combined with MagiskHide and Zygisk, it is increasingly easy to hide the presence of root, Magisk, or malware on device and evade detection. As an attack vector, Magisk gives the attacker free rein to launch attacks, change app behavior and bypass protections.

STOP ROOT & JAILBREAK BYPASS

Root Hiding and Jailbreak Detection Bypass are methods and tools that are used to evade Root and Jailbreak detection in mobile apps, including SafetyNet Device Attestation and other protections. The purpose of these methods and tools is to allow an attacker more time and control to launch attacks, including installing malicious packages, modifying app logic, inject malicious code, edit memory, or harvest mobile app data and/or connections. Appdome prevents the use of Root Hiding and Jailbreak detection bypass tools like SuperSU, RootCloak, UnRootBeer, Fridantiroot, Objection, Magisk, Zygisk, Liberty Lite, Liberty Tweak, tsProtector, iHide, A-ByPass, HideJB, JailProtect, and many more.

BLOCK FRIDA DYNAMIC INSTRUMENTATION

Frida is an instrumentation toolkit intended for developers, pen-testers and security researchers. It can also be used by fraudsters, cybercriminals, black hats, mobile cheat creators, and other malicious actors to compromise mobile apps, inject malicious code, change a mobile app's logic and commit crimes. With Frida, bad actors can probe for encryption weaknesses, replace libraries with malicious libraries, trace function calls, use hooking to inject code and malware, disable SSL/TLS pinning and bypass rooting detection mechanisms. Appdome prevents the use of all Frida and custom Frida toolkits. This allows developers to pass pen tests and block the use of tools, cheats and methods that rely on Frida.

DETECT ON-DEVICE MALWARE

Appdome actively detects and defends mobile apps against mobile malware, including advanced techniques used to hide the malware or used to allow the malware to communicate privately with protected mobile applications installed on the mobile device. For example, Appdome can detect when (1) malware uses unspecified or random sockets as a backdoor to communicate between modules and (2) binaries are installed or launched from suspicious locations (such as the SD card or in shared locations). Appdome also identifies apps installed on the mobile device that have or update to have potentially malicious AccessibilityService permissions, to safeguard the protected mobile app.

PREVENT SHELL CODE & DYNAMIC HACKING

Prevent dynamic hacking tools including Dynamic Binary Instrumentation (DBIs), lightweight hooking tools, memory tracing and other malware methods from attaching to your mobile app. Appdome also stops malicious programs from injecting modules knows as shellcode into Android and iOS apps and prevents shellcode from executing inside mobile apps. These protections are especially important to transaction-based apps as these methods can also be used to launch fraud and similar attacks.

ANTI-REMOTE DESKTOP CONTROL

Appdome detects and defends mobile applications from remote desktop control software, like TeamViewer and others, that attempt to remotely control the Appdome-protected app.

PREVENT LOGGING ATTACKS

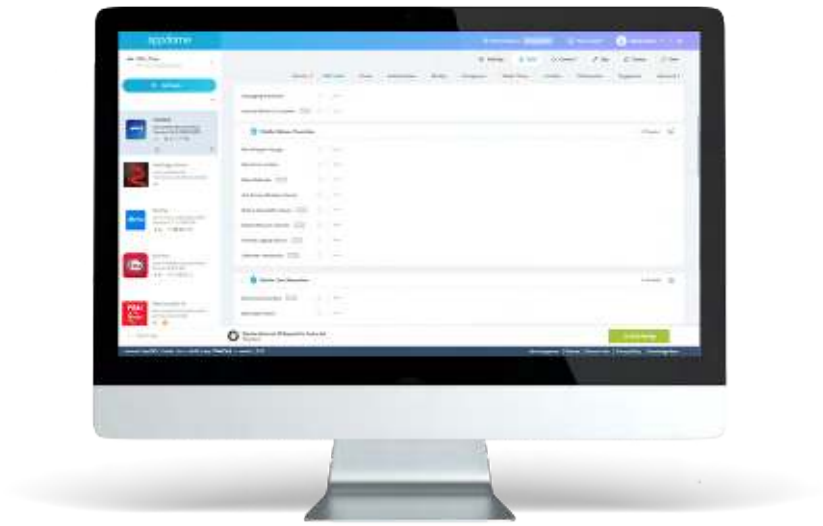
Appdome actively monitors the log function in mobile applications for malicious activity and defend the mobile app against attacks on the log function. For example, Appdome can dynamically disable Android log function calls. This prevents any data leakage and attacks via logging infrastructure (i.e. log4j).

ONESHIELD™ RASP PROTECTION TO BOOT!

Appdome's out-of-the-box Mobile Runtime Application Self Protection (RASP) is included in all protections to safeguard the mobile app and the protections defending the mobile app.

ONE SOLUTION IS ALL MOBILE DEVSECOPS NEEDS.

Appdome delivers mobile app protection, certification, threat intelligence, and release orchestration in one unified, fully integrated platform.



THREATSCOPE™ MOBILE THREAT INTELLIGENCE

ThreatScope™ is a groundbreaking new analytics-grade mobile threat and attack intelligence service that gives mobile brands data, intelligence and telemetry as well as a mobile security operations center (SOC) to manage and control mobile malware threats out-of-the-box. With ThreatScope, developers and cyber security teams gain full visibility into 1000s of threat streams covering the entire range of mobile app security, mobile fraud, malware, and cheat events offered on Appdome and the power to inspect events by release, build, device, OS, threat, attack and more. ThreatScope, makes it easy to (1) analyze the top mobile threats and attacks, (2) prove the value of existing protections, (3) make data-based decisions of what protections to deploy in each, release, and (4) review and implement defense recommendations to stop each threat and attacks. All data is fully integrated in the same DevSecOps build system. There's no added implementation, integration, SDK or server needed.

MOBILE DEVSECOPS BUILD SYSTEM

Appdome pioneered the no-code mobile app security market with its one-of-a-kind Mobile DevSecOps Build System. This flagship product allows developers and cyber security teams to design, manage and deploy security, anti-fraud, anti-malware and anti-cheat features into any Android or iOS app with ease. Patented release management, event logging, build tracking, version control, code freeze, security templating, role-based access and CI/CD DEV APIs allow instant DevOps readiness for any mobile app.

THREAT-EVENT™ ATTACK HANDLING

All runtime and dynamic protections come enabled with Appdome's Threat-Event™ in-app attack intelligence and experience handling framework. Threat-Events empower developers to read/write from the Appdome Security Framework™, gather data on the top attacks from inside an app and use the detection and defense data to create and control the user experience when threat or attack occurs.

CERTIFIED SECURE™ SECURITY CERTIFICATION

Appdome provides a Certified Secure ™ certificate that guarantees the security, anti-fraud, anti-malware, anti-cheat, and threat intelligence features are protecting the Appdome protected app. Developers and cyber security teams use Certified Secure™ as the DevSecOps artifact to clear apps for release and save money on code scans and pen tests in the release process.

ABOUT APPDOME

Appdome's mission is to protect every mobile app in the world and the people who use mobile apps in their lives and at work. Appdome provides the mobile industry a patented, no-code, Data-Driven DevSecOps™ Build System, powered by patented artificial-intelligence based, coding technology, Threat-Events™ mobile threat intelligence and ThreatScope™ mobile security operations center, to deliver 100s of Certified Secure™ mobile app security, anti-malware, anti-fraud, anti-cheat, MiTM attack prevention, code obfuscation and other protections in Android & iOS apps, right inside mobile DevOps and CI/CD pipeline. Over 500+ leading financial, healthcare, government, and m-commerce brand use Appdome to protect Android & iOS apps, mobile customers, and mobile businesses globally. Learn more at www.appdome.com. Open a free account at fusion.appdome.com and start securing your apps! Appdome holds several patents including U.S. Patents 9,934,017 B2, 10,310,870 B2, 10,606,582 B2, 11,243,748 B2, and 11,294,663 B2. Additional patents pending.