appdome

Choose Cyber Defense Automation

ONESHIELD™ - MOBILE RASP SECURITY

See how easy it can be to build, test, release and monitor Mobile RASP Security in Android and iOS apps in a Mobile Cyber Defense Automation platform.

FASTEST & EASIEST WAY TO DELIVER MOBILE RASP SECURITY

Automate delivery of mobile RASP security in Android & iOS apps to accelerate mobile DevOps CI/CD pipelines. Deliver Certified Secure™ anti-debugging, anti-tampering, checksum validation, anti-reversing, prevent running on emulators and simulators, and other RASP features in Android & iOS apps with ease. Clear mobile apps for release fast. Monitor attacks and defenses in real-time. No code, no SDK, and no added work for the dev team.

WHY YOU NEED APPLICATION SHIELDING

Application Shielding, aka RASP (Runtime Application Self-Protection) is a set of technologies that make mobile apps more resistant to intrusion, tampering and dynamic 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 back end systems, mobile piracy, app defacing and more. Hackers ofter disable existing security protections in mobile apps before carrying out their attacks. Traditional approaches to RASP, such as SDKs and other methods lack anti-tampering protections that prevent disabling the security features. All this can destroy a mobile app business, brand and user trust.

DELIVERING RASP PROTECTION IN CI/CD

Appdome delivers RASP protections and Mobile XDR (threat intelligence & response) inside Android and iOS apps via a Mobile Cyber Defense Automation platform all from within the CI/CD pipeline – no code, no SDK and no attestation service required. Appdome actively protects against debugging and tampering attempts and prevents apps from running on emulators and simulators. Appdome is fully compatible with all native and non-native Android and iOS apps, dev frameworks and languages, including Java, C++, C#, Swift, Obj-C, Flutter, JS, Kotlin, Cordova, Unity, React Native, Xamarin and more.

ALL-IN-ONE APP SHIELDING WITHOUT CODING

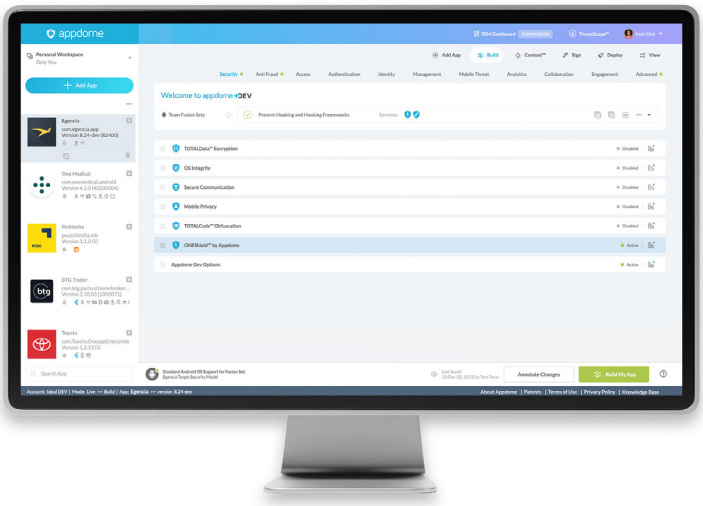
Appdome is the best, fastest, and easiest way to shield and harden Android and iOS apps. Using Appdome's Mobile Cyber Defense Automation platform, developers and security teams can protect mobile apps and everything inside the app bundle, including all native and non-native code, external components, 3rd party libraries and SDKs and more, using sophisticated runtime application self-protection (RASP) features like anti-tampering, anti-debugging, anti-reversing, multi-layered checksum validation and more.

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 must 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 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.

ONE SOLUTION IS ALL MOBILE DEVSECOPS NEEDS.

Appdome delivers mobile app protection, certification, XDR, and cyber release management in one unified, fully integrated platform.



THREATSCOPE™ MOBILE XDR

ThreatScope™ Mobile XDR provides mobile brands, developers and cyber professionals extended detection and response (XDR) for in-production Android & iOS mobile apps. ThreatScope Moible XDR gives mobile brands a consolidated view and real-time visibility into the entire range of threats and attacks impacting the mobile brand, apps and users, including full visibility into 1000s of threat streams covering mobile app security, mobile fraud, malware, cheat and bot attacks. As an XDR, ThreatScope also provides the configuration as code power to remediate attacks instantly build-by-build, and release-by-release. With ThreatScope, organizations can (1) see and analyze the top mobile app threats and attacks impacting the native mobile channel, (2) prove the value of protections deployed in mobile apps by version, OS, device or other parameters (3) make data-based decisions of what protections to deploy in each release, and (4) create customized views and comparisons that track the most relevant threats and attacks impacting the mobile business. Stay one step ahead of attackers, fraudsters and hackers with ThreatScope!

MOBILE CYBER DEFENSE AUTOMATION

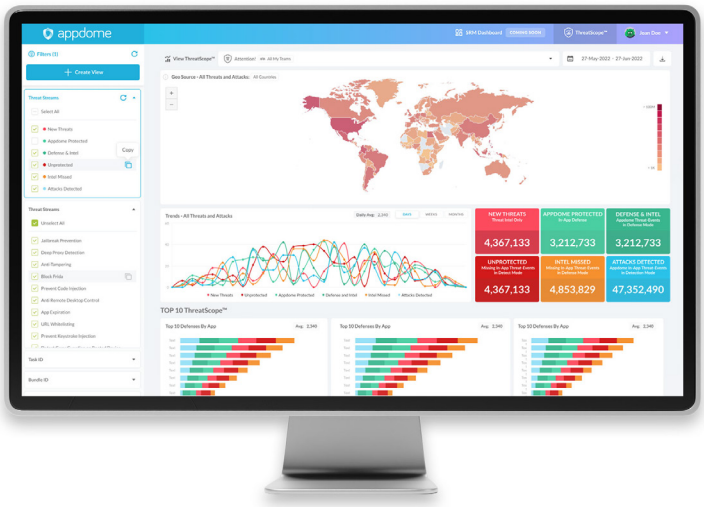
Appdome pioneered the no-code mobile app security market with its one-of-a-kind Mobile Cyber Defense Automation platform. This flagship product provides mobile developers, cyber security and fraud teams a centralized system and configuration as code ease to build, test, release and monitor mobile app security, anti-fraud, anti-malware, anti-cheat and anti-bot features in Android or iOS apps. Patented cyber 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-EVENTS™ THREAT AWARE UI/UX CONTROL

All runtime and dynamic protections come enabled with Threat-Events™, Appdome's in-app attack intelligence and UI/UX control framework. Threat-Events empower developers to read/write from the Appdome Security Framework™, gather data on each attack inside the app and use the detection and defense data to create and control beautiful user experiences when attacks occurs.

CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Each protected build generated on Appdome comes with a Certified Secure™ certificate that guarantees the mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot and threat intelligence features protecting the mobile app. Moible Dev Teams use Certified Secure™ as the DevSecOps artifact to clear apps for release and save money and time vs. using code scans and penetration tests in the release process.



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 Mobile Cyber Defense Automation Platform simplifies and accelerates mobile app protection, delivering rapid, no-code, no-SDK implementation and configuration as code ease, Threat-Events™ in-app threat intelligence and UI/UX control, and ThreatScope™ Mobile XDR all to detect, control and defend mobile apps when security, fraud, malware, cheat or bot attacks occur. As a platform, Appdome also serves as the centralized system of management, visibility and compliance control for all mobile app security, anti-fraud, anti-malware, anti-cheat and anti-bot initiatives, providing full release orchestration, user-build-event logging and guaranteeing Certified Secure™ mobile apps in the CI/CD pipeline. 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. 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.
© 2023 Appdome

RASP-DS-20230531