appdome

Choose Cyber Defense Automation

BLOCK MAGISK & ROOT HIDING

See how easy it can be to build, test, release and monitor Block Magisk and Root Hiding in Android apps in a Mobile Cyber Defense Automation platform.

FASTEST & EASIEST WAY TO DELIVER ANTI-MAGISK & ROOT HIDING DEFENSE

Automate delivery of anti-Magisk and anti-root hiding in Android apps to accelerate mobile DevOps CI/CD pipelines. Deliver Certified Secure™ protection against Magisk, Magisk Manager, Magisk Hide, Zygist, and other community incarnations of Magisk in Android 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 ANTI-MAGISK & ROOT HIDING

Magisk is powerhouse hacking tool, rooting system and malware bridge used by attackers and mobile app penetration testers. Magisk has the power to root, hide root and customize Android OS resources, alter system-level apps, load software, instrument Android apps. Magisk has a huge number of variants, and independent branches supported by open-source projects and communities. With over 100M downloads, Magisk is the most popular method Android users, developers, hackers, and mobile app pen testers to take control of the Android OS. Magisk and Root Hiding are used to attack and avoid root detection, usually to install modules, frameworks, apps and tools to interact with Android apps, change or exploit the functionality in Android apps, and access data stores used by Android applications running on a rooted device, including installing and launching malware aimed at Android apps installed on that device.

DELIVERING ANTI-MAGISK DEFENSE IN CI/CD

With Appdome, mobile developers can deliver Certified Secure™ Anti-Magisk and root hiding detection, defense, and Mobile XDR inside any Android mobile app in the CI/CD pipeline – no code, no SDK and no attestation service required. Create self-defending Anti-Magisk Detection in Android apps. Monitor Android OS in runtime. Detect root, root hiding and malware bridging tools methods actively in the app lifecycle. Fully compatible with all Android Apps including Java, C++, C#, Flutter, JS, Kotlin, Cordova, Unity, React Native, Xamarin and more.

DETECT MAGISK HIDE & ZYGISK DENYLIST

Appdome detects Magisk, root hiding and Google SafetyNet bypass methods from inside the Android app with no reliance on external servers of attestation services. This includes Magisk's attempts to hide itself, such as Magisk Hide and Zygisk DenyList, as well as Magisk Manager, Bootloader, Magisk SU (Super User), SELinux in permissive mode, props and more. With or without DenyList, Appdome detects Zygisk (Magisk in Zygote) which allows module developers to run code directly in an Android app process. Running code directly in an Android app process increases risk from malicious modules. Appdome detects and blocks Zygist, DenyList, Shamiko and other community incarnations.

DETECT MAGISK MANAGER & MODULES

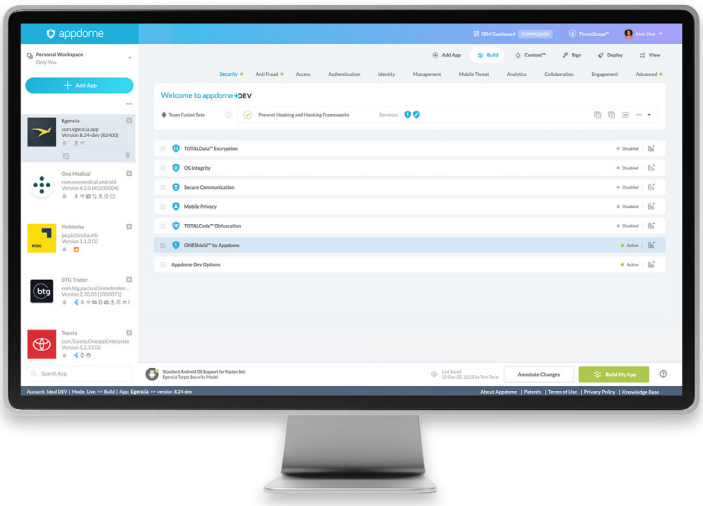
Appdome detects when any of 100s of Magisk modules or Magisk Manager is used with a protected Android app. Modules are tiny apps used to change and add functionality to Android devices. With Magisk, anyone can create a custom module for whatever functionality they have in mind, including Google Safety Net bypass, game cheats, hacking, password attacks, app systemizer, and malware to attack Android apps.

DETECT MAGISK, VARIANTS & CANARY RELEASES

Appdome detects Magisk Canary releases as well as community sponsored forks of Magisk and Zygisk, including Magisk Delta, Magisk Alpha, Shamiko, Universal SafetyNet fix and others. On top of that, Appdome detects use of Magisk with other packages like Riru, MomoHider, LSPosed and more.

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

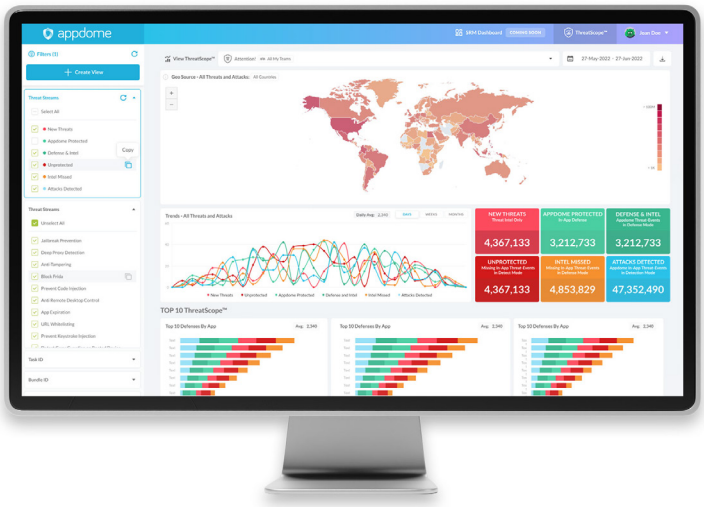
Appdome pioneered the no-code mobile app security market with its one-of-a-kind Mobile Cyber Defense Automation platform. This flagship product provides mobile developers, cyber security and fraud teams a centralized system and configuration as code ease to build, test, release and monitor mobile app 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!

MRH-DS-20230531