appdome

AI-Native Mobile App Protection

# MOBILE TROJAN PREVENTION FOR MOBILE APPS

Use AI to continuously build, monitor, and respond with Mobile Trojan Prevention in Android & iOS apps with ease.

## WHY APPDOME

Mobile development increasingly relies on AI and automation to drive rapid and continuous integration and delivery of new and updated features into Android and iOS apps. With Appdome, you can utilize a single factory model for new features and Mobile Trojan Prevention in one unified pipeline, maintain agility, and save money.

## RAPID RELEASE, MOBILE TROJAN PREVENTION

Getting fake app and Trojan defense in mobile applications right requires releasing dozens of unique defenses in Android & iOS apps fast. With Appdome, you do just that. Instead of needing engineering resources and work, you build fake app and Trojan defense features in Android & iOS apps on-demand. From the CI/CD, trigger the build command in Appdome and release fake app and Trojan defense in mobile apps either all at once or in an iterative release process to respond to new threats as they emerge and match the needs of the business instantly.

## CONTINUOUS SECURITY FOR MOBILE APPLICATIONS

Getting Mobile Trojan Prevention right requires releasing a complex array of Mobile Trojan defenses in every release of an Android or iOS app. With Appdome, a system builds these Mobile Trojan Prevention features in the apps as a standard part of the CI/CD pipeline. Your pipeline, or CI/CD, triggers the Appdome build process. Once triggered, Appdome generates the Mobile Trojan Prevention code and integrates it into the mobile apps in minutes, all without any SDK, manual coding, or engineering work.

## ZERO-MAINTENANCE, MOBILE TROJAN PROTECTION

Mobile apps and operating systems change constantly. Coding languages for mobile apps change regularly. New APIs, frameworks, and capabilities are added and updated in mobile apps continuously. Appdome automatically updates the Mobile Trojan Prevention features. Release-by-release, there's no manual work to maintain or refactor the Mobile Trojan Prevention features. Appdome maintains the Mobile Trojan Prevention features for you.

## REAL-TIME DETECTION & RESPONSE

DevOps requires real-time data and feedback on each feature released in a mobile app. Appdome provides real-time data and feedback on each Mobile Trojan Prevention feature added to the mobile app. Monitor all cyber, fraud and other attack vectors impacting the mobile app, reveal the impact of each defense, and click-to-add new defenses or update enforcement models in existing defenses to keep the mobile app, business, and users safe.

## GUARANTEED MOBILE TROJAN COMPLIANCE

As a platform, Appdome builds, tracks and records each configuration, change, build, and release of Mobile Trojan Protections in Mobile apps. To guarantee compliance, Appdome provides enterprise-grade (1) Certified Secure™ DevSecOps certification for each Mobile Trojan Prevention build, (2) defense version and change control, (3) role-based access and team entitlements, (4) tracking for each admin, configuration, change, build, and release, and (5) real-time data on each detection and enforcement event. This ensures that mobile teams have the visibility and control needed at all times.

## BEST-OF-SUITE CONSOLIDATION & SAVINGS

Mobile Trojans are both malicious programs that disguise or conceal themselves to perform their true malicious actions against users. Appdome provides a comprehensive set of Mobile Trojan Prevention features for Android and iOS apps, including:

- **Detect Bank Trojan Apps:** Secures your mobile banking app by detecting and closing it if a Banking Trojan threat is identified, ensuring protection against malicious attacks.

- **Detect Mobile Remote Access Trojan:** Detects attempts by Mobile Remote Access Trojans to infiltrate mobile apps, safeguarding data and preventing unauthorized control and access to user information.

- **Prevent Trojan Spyware:** Detects the presence of malicious Trojan spyware that may compromise your mobile app's security.

- **Prevent Logging Attacks:** Disable log function calls to prevent data leakage and attacks (such as log4j).

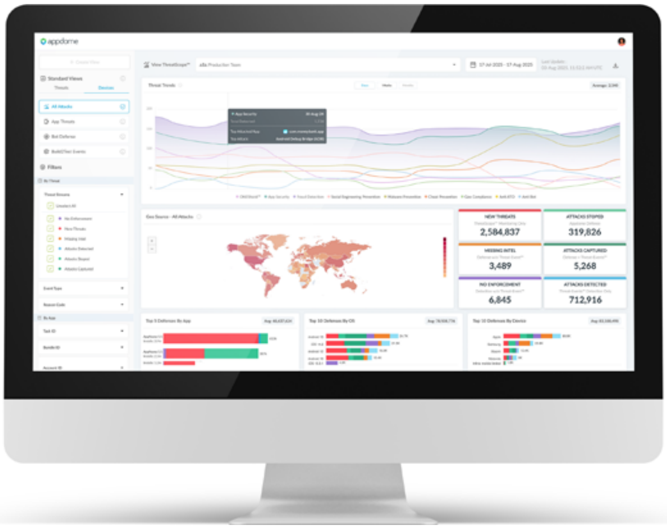
- **Prevent Task Hijacking:** Lock app activities to block malware or other external processes from performing task injection when the app is running in the foreground.

- **Detect GoldPickaxe:** Monitors Mobile Device Management (MDM) profiles, including MDM.plist and related files, to detect stages of Gold Pickaxe malware installation.

Use these and other Appdome defenses in a variety of out-of-the-box enforcement modes or plug into Appdome's Threat-Events™ intelligence framework to gain real-time threat intelligence and full control over the user experience in your app when Mobile Trojan attacks occur.

# UNIFIED DEFENSE FOR THE MOBILE BUSINESS.

Appdome leverages the power of AI to provide a one-stop shop to protect your mobile business. Eliminate point products, unify your mobile defense strategy, save money, and deliver the right user experience when attacks strike.



## PROTECT APPS, APIS & IDENTITY IN ONE SOLUTION

With Appdome, you can automate the work out of delivering Mobile Trojan Prevention and 400+ defenses in your mobile business. Appdome provides granular attack detection and defense control for the widest range of mobile threats in the industry, including anti-fraud, anti-bot, anti-malware, deepfake, ATO, social engineering, geo compliance, API, and Identity protection. Use Appdome's threat-signals to inform your mobile app, identity provider or mobile backend when mobile device, application, or user threats are present. Or, leverage Appdome's in-app defense options to design the best protection model for your business.

## THREAT-EVENTS™ INTELLIGENCE FRAMEWORK

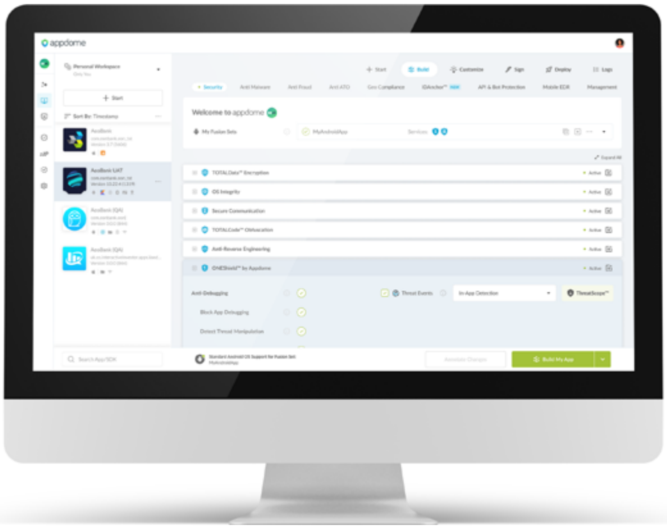
Threat-Events™ is an in-app intelligence and control framework designed to empower mobile brands to gather detailed meta data on each attack and use that data to deliver the right user experiences when an attack occurs. With Threat-Events™, mobile developers can read from/write to the Appdome Security Framework™, leverage threat data on demand, and tailor and control enforcement to fit the threat posed. Threat-Events™ can be configured with Appdome's Threat Scores™ to get device and/or transaction-based risk scoring from Appdome.

## THREATSCOPE™ EXTENDED THREAT MANAGEMENT (XTM)

ThreatScope™ XTM combines threat detection, investigation, and response for Android & iOS apps into one solution. Appdome-protected mobile apps send real-time mobile device, app, and threat data and telemetry for 1000s of unique attack vectors to each brand's ThreatScope™ instance (no separate profile or app required). From there, mobile brands can use ThreatScope's powerful SecOps AI Agent and analytics engine to investigate and respond to attacks. ThreatScope also provides an AI-generated Mobile Risk Index™, to benchmark the mobile business' defense posture against other brands and businesses in the industry and region.

## AI-NATIVE PROTECTION & COMPLIANCE

Appdome uses AI to create a true continuous defense pipeline for your mobile business. Appdome's AI codes all defense and threat intelligence features into mobile apps, instantly accommodating app changes and updates easily. Appdome's AI also validates all defenses, delivering a Certified Secure™ record of compliance in the CI/CD pipeline, allowing mobile brands to save money and time vs. code scans and pen tests in the release process. Appdome's AI also helps brands investigate, monitor, and respond to threats pre-emptively and proactively, so the business is always protected and always compliant – no matter what.



## ABOUT APPDOME

Appdome's mission is to protect every mobile business and user in the world from scams, fraud, bots, and attacks. Appdome's patented AI-Native XTM Platform is designed to protect every aspect of mobile business now and in the future. From mobile DevOps to mobile applications, networks, APIs, and Customer Identity, Appdome uses AI to generate Android & iOS defense plugins for 400+ mobile app security, anti-fraud, bot defense, anti-malware, geo compliance, social engineering, deepfake and Customer Identity defenses on demand. Appdome also uses AI inside its ThreatScope™ Mobile XTM, to continuously calculate a Mobile Risk Index™ for businesses and applications as well as rank and preempt attacks in real-time. In Appdome's Threat Resolution Center™, Agentic-AI provides customer support and care teams a quick and easy way to provide end-user threat resolution and remediation. Appdome's Threat-Events™ framework gathers threat and attack metadata, and can be used to inform the application, application SDKs and back-end network components when threats are present or to create customized threat responses inside Android & iOS apps. As a platform, Appdome functions as a continuous compliance center, tracking all builds, changes, teams, users, defense configurations, events, and more for quick and easy audit of the mobile defense lifecycle.

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.