

# BETTER MOBILE THREAT RESOLUTION

Resolve Mobile Threats & Attacks on Android & iOS Devices Fast Using GenAI to Improve Customer Satisfaction and Maintain Loyalty and Trust.



## MOBILE APP THREAT REMEDIATION AT THE SPEED OF DEVOPS

Mobile app support teams use systems to drive rapid responses to user concerns and complaints to ensure high satisfaction rates and positive app reviews. Appdome Threat Resolution Center lets you do the same. Appdome Threat Resolution Center uses Generative AI (GenAI) to deliver rapid and precise data for on-device threats and specific remediation steps, ensuring users can swiftly eliminate threats and continue using your app without interruption. Here's what you get by using Threat Resolution Center in your support workflows.

## RAPID RESOLUTION OF MOBILE DEVICE THREATS

Getting the right balance of mobile app defense while ensuring a great customer experience requires coordination with cyber and front-line support teams handling user issues. Appdome's Threat Resolution Center is designed with the user in mind, addressing the gap left by traditional threat response products that focus solely on defense. Appdome provides specific threat data and actionable steps to help users quickly and efficiently remove threats, leading to higher satisfaction and loyalty. RAG-based GenAI makes threat resolution faster and more efficient, reducing downtime and minimizing the impact of cyber attacks. It also alleviates the burden on support centers and cyber teams, by providing the necessary details to resolve threats and get customers back to using the app quickly.

## THE MOBILE APP SECURITY SUPPORT CHALLENGE

Current threat resolution processes used by mobile brands face major challenges due to the complexity and fragmentation of the mobile ecosystem, which includes numerous threats, device manufacturers, and OS versions. Also, sophisticated malware delivery mechanisms can cause users to make innocent mistakes, leading to significant consequences for app usage. Resolution methods are time-consuming, error-prone, and inconsistent amidst rapidly evolving threats like malware and phishing. User experience suffers as many users lack awareness of mobile security best practices and find existing remediation steps overwhelming. This scenario can damage brand reputation and trust due to ineffective threat resolutions and dissatisfied users.

## FAST & SIMPLE THREAT RESOLUTION

Threat Resolution Center revolutionizes how support teams identify and resolve mobile threats by transforming the interaction between mobile brands and users. By providing clear, step-by-step instructions, Appdome empowers users to protect their devices and mobile apps confidently and proactively. This accelerated detection improves support workflows reducing the time and cost associated with remediation.

## TAILORED RESPONSES BASED ON DEVICE & OS

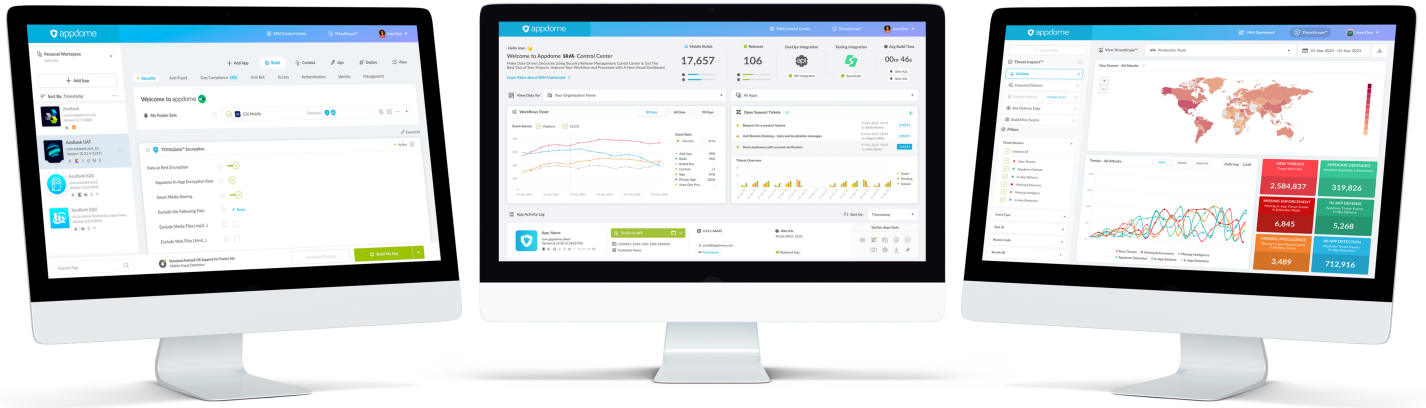
Threat Resolution Center uses advanced GenAI to provide real-time, automated responses to remove mobile app and device threats. Tailored remediation steps deliver precise, step-by-step instructions based on threat type, device type, and OS version, ensuring efficient threat resolution and a smooth user experience. The user-friendly guidance can be delivered verbally or via PDF and offers detailed, easy-to-follow remediation steps, helping even less experienced users navigate the resolution process effectively. Support teams benefit as well because they get access to automated, streamlined threat remediation steps that eliminate guesswork and reduce support costs and time to resolution.

## COMPLETE RESOLUTION FEATURE COVERAGE

Add mobile threat resolution for your Android and iOS app support workflows and empower customer support teams with a powerful GenAI tool that speeds up the support workflow, reduces cost, and maintains a high-quality mobile experience.

- When a threat is detected, Appdome dynamically generates a context-specific ThreatCode™ encoded with the DNA of the threat, attack method, device, OS and other information.
- Support, IT and Cyber teams use the ThreatCode inside Appdome Threat Resolution Center to identify and understand the attack, discover how to find the attack, and retrieve step-by-step instructions to remediate or remove the mobile threat in real time.
- Appdome dynamically combines the encoded data in the ThreatCode with Appdome's platform data to generate smart prompts for GenAI step-by-step responses that are provided to the user.

Mobile app threat resolution is often part of a larger strategy to improve and maintain user experience. Combine 300+ mobile app defenses to protect your app and customers with Appdome Threat Resolution Center to give support teams an easy-to-use tool that can be easily integrated into support workflows.



## BUILD

Appdome eliminates engineering work and point products by using machine learning to code any or all of 300+ mobile app security, anti-fraud, anti-malware, anti-bot, geo-compliance and other defenses into Android and iOS apps in the CI/CD on demand.

## MONITOR

Appdome Security Release Management Center™ delivers enterprise-grade visibility, transparency and control across the entire mobile app defense lifecycle. Monitor and audit defense work and activity in the DevOps pipeline, CI/CD, test, validation, release and production.

## RESPOND

Appdome ThreatScope™ Mobile XDR provides continuous detection and response for 1,000s of threats and attacks in 17 attack categories. With ThreatScope, organizations see, isolate, investigate and respond with “click to defend” ease in real time using manual or automated settings.

## ONE SOLUTION FOR ALL YOUR MOBILE APP DEFENSE NEEDS.

Appdome’s Unified Mobile App Defense platform provides a one-stop shop to protect your mobile apps, save money on mobile app defense, and deliver beautiful user experiences when attacks happen.

### UNIFIED MOBILE APP DEFENSE

Appdome’s patented Unified Mobile App Defense platform provides mobile developers, threat response teams and mobile customer support teams a centralized automation, monitoring, and control center for protecting mobile apps. With Appdome, choose, build, test, release and monitor any or all of Appdome 300+ mobile app security, social engineering prevention, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and other defenses in Android or iOS apps with ease. Maintain full compliance control over the defense lifecycle and enjoy complete compatibility with the entire tech stack used in mobile development, DevOps, and DevSecOps.

### CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Build-by-build, apps are Certified Secure™ to guarantee the defense and threat intelligence features are embedded, active and protecting the mobile app. Cyber and mobile dev teams use Certified Secure™ as a record of compliance and as the DevSecOps artifact to clear mobile apps for release and save money and time vs. code scans and pen tests in the release process.

### THREATSCOPE™ MOBILE XDR

ThreatScope™ Mobile XDR provides mobile brands, developers and cyber professionals extended detection and response (XDR) for Android & iOS apps. ThreatScope Mobile XDR uses dedicated sensors inside mobile apps, not a separate agent or app on the end user’s mobile device. These sensors provide real-time, continuous monitoring of 1000s of unique attack vectors, giving mobile brands real-time visibility into the entire range of threats and attacks impacting their mobile app and users. As an XDR, ThreatScope also provides the power to respond to attacks instantly, build-by-build, and release-by-release.

### THREAT-EVENTS™ CONTROL FRAMEWORK

All of Appdome’s runtime and dynamic protections come enabled with Threat-Events™, Appdome’s in-app attack intelligence and 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 deliver beautiful user experiences when each attack occurs.

## ABOUT APPDOME

Appdome is the mobile app economy’s one-stop shop for mobile app defense. Appdome is on a mission 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’s only fully-automated, Unified Defense Platform, powered by a patented coding engine, used by mobile brands to eliminate complexity, save money and deliver 300+ Certified Secure™ Social engineering prevention, anti-malware, anti-fraud, MOBILEBot™ Defense, Geo Compliance, anti-cheat, MiTM attack prevention, code obfuscation and other protections in Android and iOS apps with ease, all inside the mobile DevOps and CI/CD pipeline. Appdome’s Unified Mobile App Defense platform also comes with Threat-Events™ for UX/UI Control and ThreatScope™ Mobile XDR. Leading financial, healthcare, mobile games, government and m-commerce brands use Appdome to protect Android and iOS apps, mobile customers and mobile businesses globally.

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.  
© 2024 Appdome

TRC-SG-07302024