

SUPPORT AGENT

Use Agentic AI to support end users and resolve threats that arise in Android & iOS apps fast.



WHY SUPPORT AGENT

At any given time, hundreds of mobile devices and OSs are used actively by billions of users. Millions of mobile threats, exploits, malware, and Trojan apps are distributed and installed on end-user devices. Mobile end users who face threats need support that is tailored to the device, OS, and threat that interrupts their experience.

RAPID RESOLUTION OF MOBILE THREATS

Appdome's Support Agent is an agentic-AI agent built to deliver rapid and precise resolution instructions for on-device threats, ensuring Android & iOS users can swiftly eliminate any threat and get back to using the app without risk. Mobile app support teams or end-users can directly use Support Agent to understand, find, and resolve threats, guaranteeing high satisfaction, improved trust, and positive user experiences.

AI-GENERATED REMEDIATION FOR SPECIFIC THREATS

Support Agent provides resolutions to the mobile end user, with the user's mobile app, device, and operating system in mind, addressing a huge gap left by legacy security products that focus solely on defending the app or backend. Each Appdome detection is fingerprinted with a unique Threat-Code™ that encapsulates the mobile app, device, operating system, and threat experienced by the user. Support Agent uses the Threat-Code in a RAG-based AI model to generate remediation instructions that are tailored to the specific app, device, OS, and threat faced by the users. This alleviates the burden on support teams to research and provide the necessary details to resolve threats manually.

AI-GUIDED RESOLUTION JOURNEY

Threat remediation in the mobile industry faces major challenges due to the complexity and fragmentation of the mobile ecosystem, users' technical proficiency, and myriad threats, device manufacturers, and OS versions. Manual remediation or guesswork methods are too slow and impose time-consuming, error-prone, and inconsistent resolutions on the end user experience – leading to churn and abandonment. Support Agent provides fast and accurate step-by-step instructions to understand the threat, find the threat, and remediate the threat on the specific user's device and OS

(including hidden and masked threats embedded deeply on the device). Support teams and users can ask for different options or more details on resolution paths, leveraging the full power of agentic AI to guide users through the remediation journey.

IN-APP OR PLATFORM LEVEL ACCESS

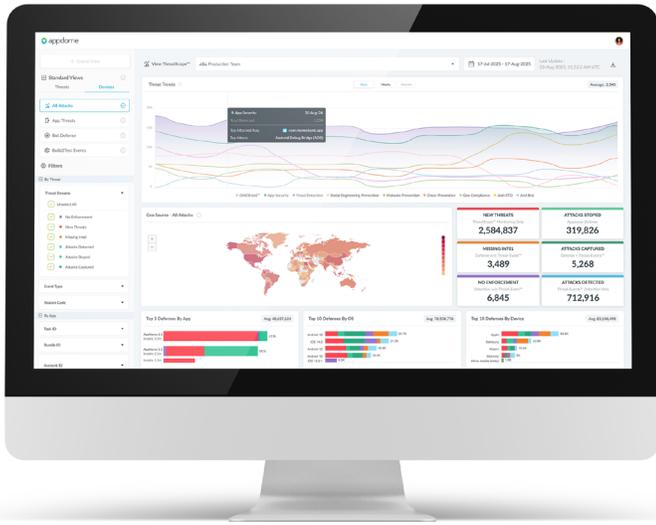
Support Agent is available on the Appdome platform or via an API for integration into the mobile app experience. Via the Appdome platform, Support Agent democratizes the cyber support process by allowing anyone. Including support, engineering, and cyber teams, to easily identify and resolve mobile threats for end users. Inside a mobile app, Support Agent can be used to provide in-the-moment, step-by-step instructions, inside the mobile app experience. This implementation allows users to self-remediate any threat they face while the app remains running, and can also include app and satisfaction ratings.

AGENTIC AI CENTER OF EXCELLENCE

Agentic AI is transforming end-user support workflows and being used to empower customer support teams, speed up resolution times, reduce costs, and maintain a high-quality mobile experience. Support Agent complements this AI-transformation, leveraging the power of agentic-AI to inform, instruct, and guide support teams and end users on resolving diverse and sophisticated mobile threats. Support Agent highlights the risks each threat poses to the user's data, transactions, and accounts and guides them on solving this threat fast. In doing so, it allows threat remediation to play an important part in a larger strategy to improve and maintain user loyalty and brand attachment and overcome the fear and anxiety associated with mobile threats when they arise.

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 any of 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.

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. Agentic AI Agents provide security operations teams threat assessment reports and analysis and 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.

© 2025 Appdome

SUA-SG-12092025

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.

