appdome

AI-Native Mobile App Protection

APP, API AND IDENTITY PROTECTION IN ONE

Leverage a single platform to pre-empt, monitor, and respond to fraud, ATOs, and cyberattacks in mobile apps, APIs, and Identity fast.

CONSOLIDATED MOBILE PROTECTION & DEFENSE

Leverage AI inside a centralized command and control center to deliver, monitor, and respond with 400+ mobile defenses on demand. Consolidate vendors. Protect mobile apps, APIs, and Identity in one.

AI SPEED & EFFICIENCY

With AI, the DevOps pipeline is accelerating. Cyber and anti-fraud teams need their own AI platform to keep up and gain the required speed and efficiency in their operations. Engineering teams also don't have the resources to prioritize cyber projects while racing to get new functionality into the market. Appdome allows mobile brands to meet security, anti-fraud, and other objectives, all while not disrupting engineering release cycles. Appdome automatically adapts the customer's chosen protection model to each app's code, language, and framework. This ensures the business can address any risk that arises in its production environment fast.

ANTI-FRAUD, ATO & API PROTECTION

Mobile brands and businesses face several ongoing risks, including fraud, ATOs, social engineering, deepfakes, API abuse, and cyberattacks at the application, API, and Identity level. These days, it's not enough to employ simple security or RASP methods in an app, and it's too complex and expensive to employ multiple vendors to address every risk a mobile business will face. Appdome provides mobile brands a suite of protections in a single platform that unifies cyber and anti-fraud data, reduces training and resource requirements, and solves multiple cyber and business objectives in one.

MULTI-CONTEXT THREAT SIGNALS

Mobile attack surfaces involve 100s of ever-changing security, fraud, malware, bot, geo-spoofing, social engineering, and other threats to user identity, data, revenues, and accounts. With Appdome, mobile brands and developers can harness to power of 400+ threat signals anywhere they like, in any context needed to keep the business and user secure. Configure and send threat signals to the application, API gateway, Web Application Firewall, or Identity workflow. The signals provide detailed threat decisioning data to facilitate clean and safe account creation, onboarding, login, transaction processing, redemption, service enrollment, and account changes.

MULTI-DIMENSIONAL ENFORCEMENT

Appdome empowers mobile brands with multiple enforcement options to create any user experience needed to keep users and businesses secure. With Appdome, mobile brands can use Appdome's out-of-the-box enforcement options, customize threat notifications or leverage Appdome's Threat-Events™ intelligence framework to take full control over how and when detections are determined and/or the mitigation workflows used in the app to reduce transaction or account exposure when threats and risks are present. Threat-Events™ provides granular control and data over Appdome's detection logic, allowing developers to deeply integrate threat detections in the application lifecycle and workflows.

ZERO-DAY DETECTION & RESPONSE IN ONE

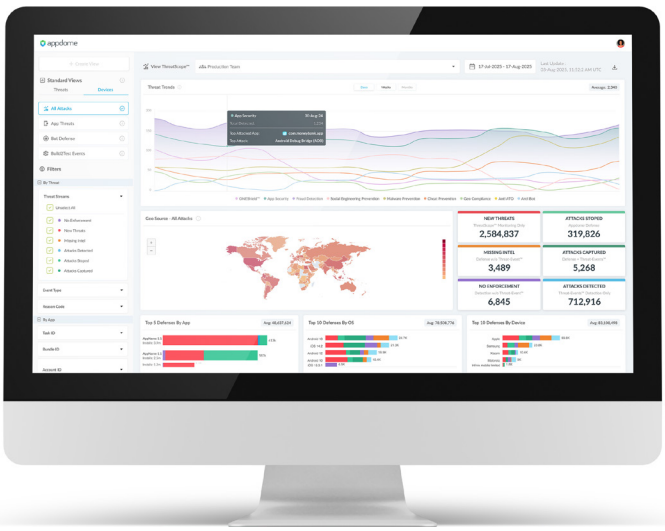
Mobile app developers and fraudsters alike are in a constant race to innovate and take full advantage of new mobile tools, OSs, and devices. To keep up, Appdome offers AI-generated implementations of 400+ mobile defenses, complete with guaranteed interoperability to any mobile application, API gateway, Web Application Firewall, and CI/CD pipeline —eliminating massive amounts of engineering work and ensuring cyber and anti-fraud features can be easily delivered inside the existing mobile app release cycle. Using one system or process to detect and another to respond to attacks in mobile apps wastes time and gives an advantage to attackers. Worse, relying on automated detection but manual resolution puts the resolution out of synch with the attack. Appdome's is the only system that combines fully automated detection and defense into one system.

SYSTEM-LEVEL CONTINUOUS COMPLIANCE

On average, mobile brands release apps 42x per year. Brands can't rely on word of mouth, emails or periodic penetration tests to guarantee compliance. At the speed of DevOps, brands need a dedicated and continuous system of compliance and version control to deliver, manage and record the defense posture in every release of each mobile app. With Appdome, brands gain management, visibility and audit control over the defense posture in the mobile business. Appdome is the only enterprise-grade platform, complete with role-based access, defense templates, build tracking, version, change, and access control, as well as code freeze, personal/team workspaces, and more to create, validate, and release defenses fast.

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

The Appdome platform lets mobile developers and cyber and fraud teams automate the work out of delivering mobile app defense with a centralized system to protect mobile apps, APIs, and Identity in one. With Appdome, prevent fraud, ATOs, deepfakes, social engineering, malware, bots, API attacks, location spoofing, and other threats against Android or iOS apps, mobile APIs and Identity with ease. With Appdome, deliver 400+ defenses in Android or iOS apps, or configure threat signals in mobile apps, in MobileBOT™ API Protection profiles, or IDAnchor™ Customer Identity Protection profiles, all to create a layered defense model for the mobile business—in minutes.

THREAT-EVENTS™ INTELLIGENCE FRAMEWORK

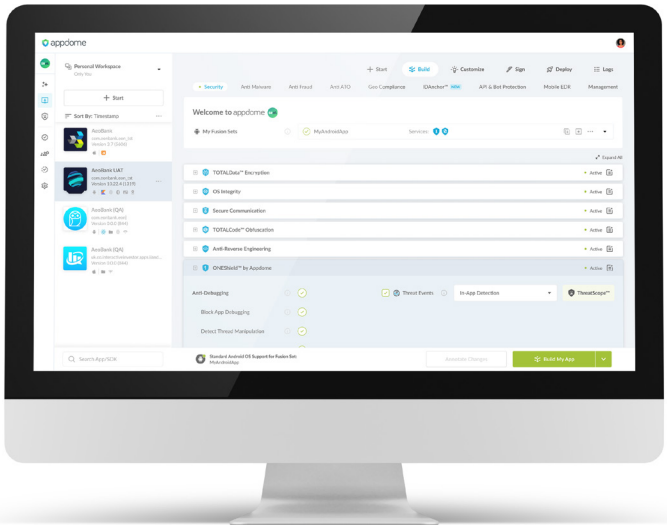
Threat-Events™ is an in-app intelligence and control framework designed to empower mobile brands to gather detailed meta data on each attack and use that data to deliver the right user experiences when an attack occurs. With Threat-Events™, mobile developers can read from/write to the Appdome Security 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.

APPDOME AI SUPPORT AGENT

Mobile end users who face threats need help remediating and resolving threats on their mobile devices. The mobile brand's interests are in getting each user past any threats that place in-app experiences at risk. Appdome's Support Agent leverages the power of Appdome's ThreatCode™ threat fingerprinting and AI to provide mobile end users with step to find and resolve threats on their devices. Support Agent can also be deployed as part of in-app chat-bots or agents to allow users to self-remediate any on-device threats.



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.

PLAT-SG-12302025