appdome

THREATSCOPE™ MOBILE XDR

Choose the DevOps way to build, test, release and monitor Mobile Threat in Android and iOS apps and save time, money and achive your goals.

FASTEST & EASIEST WAY TO DELIVER AGENTLESS MOBILE XDR

Automate delivery of Agentless Mobile XDR in Android & iOS apps to accelerate mobile DevOps CI/CD pipelines. Deliver consolidated mobile threat and attack telemetry and intelligence and fully integrated, automated response capabilities of attacks and threats in Android & iOS apps with ease. See and solve mobile app threats and attacks fast, in real time. No agent, no code, no SDK, and no added work for the dev team.

DATA-DRIVEN DEVSECOPS™

ThreatScope™ Mobile XDR opens the door to an intelligence-first approach to protecting mobile apps and businesses. Using ThreatScope™ Mobile XDR, developers and cyber-security teams collect, analyze and understand the mobile attack landscape as threats occur and use the intelligence to make data-driven decisions about which mobile app protections to prioritize, build and deliver in Android and iOS apps in each release – all from within the DevOps CI/CD pipeline. ThreatScope™ Mobile XDR combines the power of mobile attack and threat data, telemetry, and intelligence with "click- to-protect" agility inside the mobile DevOps CI/CD pipeline. No code, no SDKs, no agents, no separate apps, and no servers required.

SUPERCHARGED MOBILE DEFENSE AGILITY

ThreatScope™ Mobile XDR enables mobile businesses and brands to enjoy true "see it, solve it, show it" mobile defense agility in DevSecOps. Armed with production-level mobile attack data, intelligence, and telemetry, developers and cyber teams can adjust and update the security model, release-by-release, prioritizing the protections that have a real impact on the mobile business and users, using the data from actual attacks and threats impacting deployed mobile apps and users. After the protections are deployed, ThreatScope™ Mobile XDR enables mobile brands and businesses to monitor and prove the effectiveness of chosen mobile app protections against real-world attacks and exploit attempts.

TURN DATA INTO ACTION

ThreatScope™ Mobile XDR is integrated in Appdome's Cyber Defense Automation Platform, which enables developers to build the required protections in Android and iOS apps in minutes to instantly address the threats detected by Appdome. With ThreatScope, mobile developers and cyber teams gain full 360° lifecycle visibility and intelligence to protect mobile apps against all threat classes, methods and attack vectors targeting Android & iOS apps. When attacks are detected, dev teams can add the relevant no-code, no-SDK protection to the next release automatically, in the same system.

FULL ANALYTICS GRADE INSPECTION

ThreatScope™ Mobile XDR gives cyber-teams full visibility into the full range of threat intel, telemetry and meta-data from all mobile attacks and threats on Android and iOS apps. This allows cyber teams to monitor, analyze, investigate, and respond to attacks against every mobile app in production from a single console which can be tailored to suit the role of the operator. Cyber teams can instantly view top threats, attack vectors, and emerging trends affecting the entire mobile estate, then drill down on any element to access granular details about the event. Using ThreatViews™ , threats can be filtered by any criteria, including threat/ attack type or description, app name, bundle/build ID, release, OS or device information, geo-location, timestamp, date-range, mobile network plus all signals from Threat-Events™ , Threat-Scores™ , Threat-CodesTM and more.

THREAT-STREAMS - LIVE PROTECTION MONITORING

ThreatScope™ Mobile XDR also includes multiple Threat-Streams™ to signal the protection level in place for all apps, color coded for easy identification, filtering and reporting. The 6 available protection levels

1. New Threats (Threat Intel Only).
2. Appdome Protected (In-App Defense).
3. Unprotected (Missing In-App Threat-Events™ in Detection Mode).
4. Defense and Intel (In-App Threat-Events™ in Defense Mode).
5. Intel Missed (Missing In-App Threat-Events™ in Defense Mode).
6. Attacks Detected (In-App Threat-Events™ in Detection Mode).

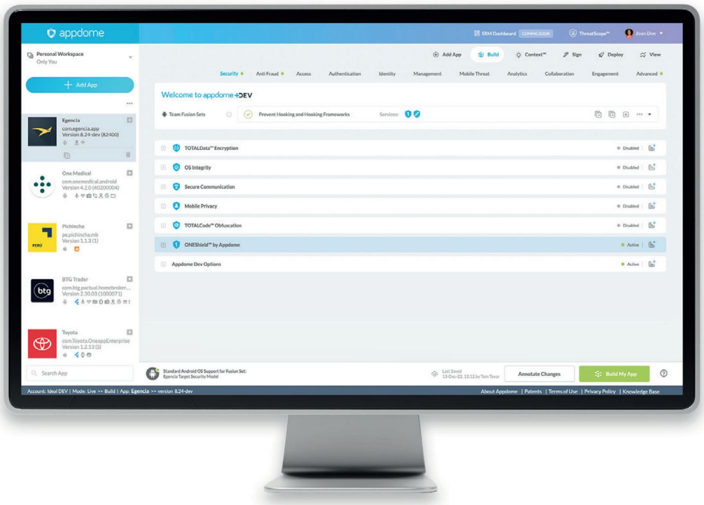
Alerts & protection levels are also available for missing in-app implementations and failed runtime verification of Threat-Events™ in mobile apps. With Threat-Streams, the impact of protections is instantly apparent. With Threat-Streams, the impact of protections is instantly apparent.

HIGH FIDELITY THREAT INTELLIGENCE

ThreatScope™ provides visibility to the entire spectrum of attack and threat detail in a centralized analytics engine, with no additional components needed. This results in faster "out-of-the-box" time to first use. It also eliminates the risk of in-transit exploits, signal spoofing, hijacking or other attacks that can compromise the integrity of the threat signal. Hardened binding between the ThreatScope™ detection code and the protected app eliminate the risk of an attacker disabling the ThreatScope™ signals.

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

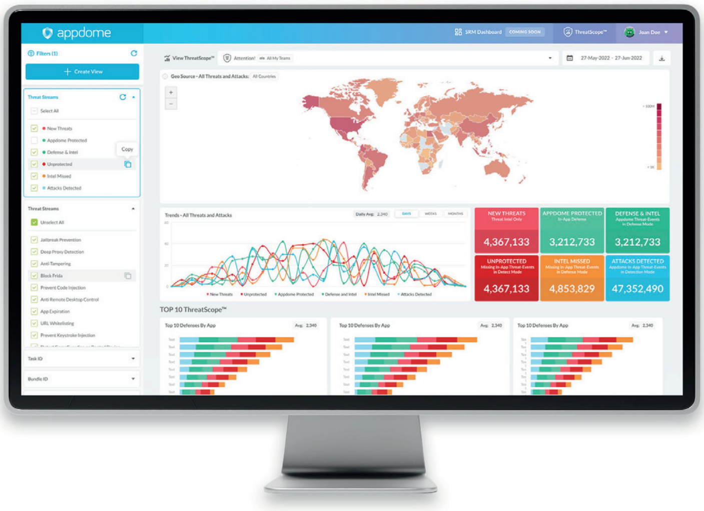
Appdome pioneered the no-code mobile app security market with its one-of-a-kind Mobile Cyber Defense Automation platform. This flagship product provides mobile developers, cyber security and fraud teams a centralized system and configuration as code ease to build, test, release and monitor mobile app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

Appdome patents include 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 pending.