appdome

Agentless, Serverless, & Codeless Mobile EDR & MTD

BETTER MOBILE THREAT DETECTION & RESPONSE

Continuously build, monitor and respond to enterprise mobile threats
with 300+ mobile defenses in Android & iOS apps in one platform in CI/CD.

DELIVER MOBILE EDR / MTD AT DEVOPS SPEED

Appdome's Unified Mobile App Defense platform lets you use systems to achieve rapid, automated delivery and release cycles of Android & iOS enterprise apps, using a factory model to build, test, monitor and respond with Mobile Endpoint Detection & Response and Mobile Threat Defense in mobile apps, fast. Here's what you get by combining Appdome with CI/CD:

RAPID RELEASE & DELIVERY OF MOBILE EDR

Getting enterprise mobile applications right requires releasing Mobile Endpoint Detection and Response (EDR) in Android and iOS apps fast. With Appdome, you do just that. Instead of needing engineering resources to code an SDK or deal with agents or separate apps, you build EDR and mobile threat defense (MTD) capabilities into Android and iOS apps on-demand. From the CI/CD, trigger the build command in Appdome and release mobile threat defenses in enterprise mobile apps on demand and match the needs of the business instantly.

CONTINUOUS SECURITY FOR MOBILE APPS

Mobile apps and operating systems change constantly. Coding languages for mobile apps change regularly. New EDR and MTD SDK capabilities are added and updated continuously. Appdome automatically adjusts and adapts the threat defense model to the changes in the updated mobile app. Release-by-release, no manual work, retooling, or coding change are needed to make mobile EDR and MTD defenses work in the new app. Instead, Appdome does that for you and provides continuous security across all mobile app versions and releases with ease..

CONTINUOUS DETECTION & RESPONSE

DevOps requires real-time data and feedback on each iterative release of a mobile app. Appdome provides real-time data and feedback on each detected threat or attack on the mobile app. With Appdome, mobile brands and organizations monitor all attack vectors impacting the mobile app, revealing the impact of each defense and the total active attack surface in real-time. Armed with this data, brands click-to-add new defenses or update enforcement models in existing defenses to keep the enterprise mobile app, business and employees safe.

COMPLIANCE TRANSPARENCY & CONTROL

Continuous compliance transparency and control over each step of the build, test, and release lifecycle for mobile apps and defenses alike is critical. Without Appdome, compliance is a leaky bucket and gaps arise. Appdome provides enterprise-grade (1) access, version, and change control, (2) role-based and team entitlements, and (3) tracking for each implementation, change, detection, and enforcement event. Build by build, each mobile app is Certified Secure™ compliant in the CI/CD pipeline.

"BEST OF SUITE" COST SAVINGS & CONSOLIDATION

Appdome offers unparalleled cost consolidation and TCO savings for mobile threat defense in mobile apps. With Appdome, mobile MTD defenses are delivered without resource dependencies or compatibility limitations, providing a choice of 300+ defenses offered via the Appdome platform. Eliminate point products, multi-vendor integration risk and complexity, and streamline release cycles for mobile apps and mobile app defenses alike.

FULL MOBILE EDR & MTD COVERAGE

Using Appdome MobileEDR, build enterprise mobile apps with EDR and MTD features without any burden on the mobile engineering team:

- **Agentless EDR for Mobile Devices:** Deploy mobile EDR with unparalleled flexibility and ease – no agents, no servers, no SDKs, no management profiles and no separate apps.

- **Comprehensive MTD:** 300+ defenses are available with MobileEDR for the most comprehensive threat detection on the market.

- **Anywhere Enforcement:** use mobile threat detection and defense data across the entire enterprise infrastructure, including the mobile app, server, IAM, UEM, or WAF.

- **Adaptive Mobile Trust:** Choose from a Zero Trust model (always verify) or Dynamic Trust model (evaluates device state dynamically throughout lifecycle).

- **ThreatSource™:** Application userID and sessionID provide deeper investigation and telemetry on threats and attacks.

- **Zero Server Continuous Evaluation:** All mobile device evaluations are performed throughout the lifecycle of use for each mobile app without servers or external attestation, improving stability and responsiveness and eliminating signal spoofing.

Mobile EDR and MTD are often part of a larger enterprise mobile app defense strategy. With Appdome, B2B and work apps achieve complete protection to protect corporate data from threats and attacks using any or all of Appdome's 300+ mobile app defenses including mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance features, and more.

appdome

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.

THREATSCOPE™ MOBILE XDR

ThreatScope™ Mobile XDR provides mobile brands, developers and cyber professionals extended detection and response (XDR) for Android & iOS mobile 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. Inside ThreatScope, organizations can (1) see and analyze the top mobile app threats and attacks impacting the mobile channel, (2) prove the value of the Appdome defenses deployed in mobile apps (3) make data-driven decisions of what protections to deploy in each release, and (4) create customized views and comparisons to report on threats and attacks impacting different parts of the mobile business.

UNIFIED MOBILE APP DEFENSE

Appdome's patented Unified Mobile App Defense platform provides mobile developers, cyber security and fraud 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, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and other defense features 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.

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 experienceswhen each attack occurs.

CERTIFIED SECURE™ DEVSECOPS CERTIFICATION

Build-by-build, mobile apps are Certified Secure™ to guarantee the mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance and threat intelligence features are embedded, active and protecting the mobile app. Cybersecurity and mobile dev teams use Certified Secure™ as a continuous record of compliance and as the DevSecOps artifact to clear mobile apps for release and save money and time vs. using code scans and penetration tests in the release process.

MEDR-SG-05052024

 appdome