appdome

Unified Mobile App Defense

BETTER MITM ATTACK PREVENTION IN CI/CD

Continuously build, test, monitor and respond with MitM Attack Prevention and 300+ other defenses in Android & iOS mobile apps in one platform in CI/CD.

DELIVER MITM ATTACK PREVENTION AT DEVOPS SPEED

Mobile DevOps pipelines use systems to drive rapid, automated and continuous integration, delivery and release cycles of Android & iOS apps. Appdome's Unified Mobile App Defense platform lets you do the same, using a factory model to build, test, monitor and respond with MitM Attack Prevention in mobile apps, fast. Here's what you get by combining Appdome with CI/CD:

RAPID RELEASE & DELIVERY, MITM ATTACK PREVENTION

Getting Mitm attack prevention in mobile applications right requires releasing dozens of unique defenses in Android & iOS apps fast. With Appdome, you do just that. Instead of needing engineering resources and work, you build Mitm attack prevention features in Android & iOS apps on-demand. From the CI/CD, trigger the build command in Appdome and release MitM attack prevention in mobile apps either all at once or in an iterative release process to respond to new threats as they emerge and match the needs of the business instantly.

CONTINUOUS SECURITY FOR MOBILE APPLICATIONS

Mobile apps and operating systems change constantly. Coding languages for mobile apps change regularly. New APIs, frameworks, and capabilities are added and updated in mobile apps continuously. Appdome automatically adjusts and adapts each MitM attack prevention feature to the changes in the updated mobile app. Release-by-release, no manual work, retooling, or coding change are needed to make MitM attack prevention features 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 MitM attack prevention feature and other defenses in 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 mobile app, business and users 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 mobile defense choice, 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 MitM attack prevention and other defenses in mobile applications. With Appdome, MitM attack prevention features are delivered without resource dependencies or compatibility limitations. In addition, MitM attack prevention features are instantly interoperable with 300+ other defenses offered via the Appdome platform. Eliminate point products, multi-vendor integration risk and complexity, and streamline release cycles for mobile applications and mobile app defenses alike.

FULL MITM ATTACK PREVENTION FEATURE COVERAGE

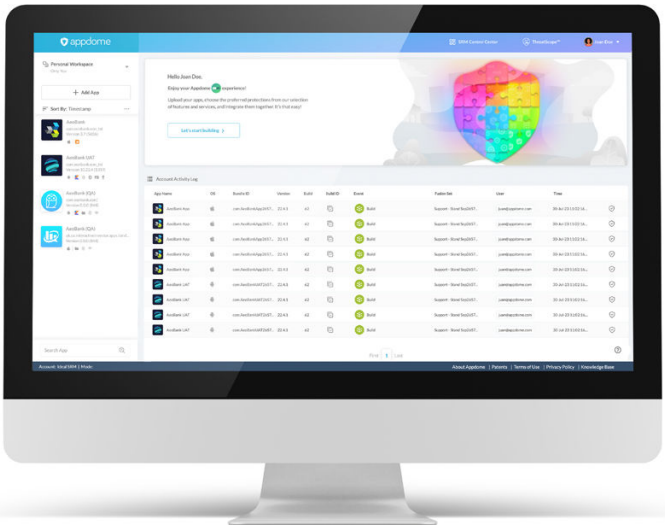
MitM attacks encompass a variety of techniques to secretly intercept a communications session between two parties, which may enable the attacker to read, alter or steal data, take control over the session, or deceive either party by masquerading as the other. Appdome provides a comprehensive set of MitM attack prevention features for Android and iOS apps including:

- **Detect MitM Attacks:** Enforce proper SSL/TLS connections on all or designated hosts and using active MitM attack detection to protect Android & iOS apps and data-in-transit against exploitation and harvesting.
- **Certificate Pinning:** Protects Android & iOS apps from connecting to malicious servers. Ensures the authenticity of the remote server by storing the trusted servers' public key encrypted inside the app.
- **Prevent MitM Attack Tools:** Prevent attackers gaining control over sessions using proxy tools such as Charles Proxy, Burp Suite, NMAP, mitmproxy, Wireshark, Metasploit and others.
- **Stop Session & Cookie Hijacking:** Stop session hijacking, cookie hijacking, and other methods used to conduct MitM attacks by blocking the attacker's ability to read the cookie & session data in transit.

MitM attack prevention defenses are often part of a larger mobile app defense strategy. Combine the above MitM attack prevention features with any or all of Appdome's 300+ other mobile app defenses including mobile app security, anti-fraud, anti-malware, anti-cheat, anti-bot, geo compliance features and more.

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

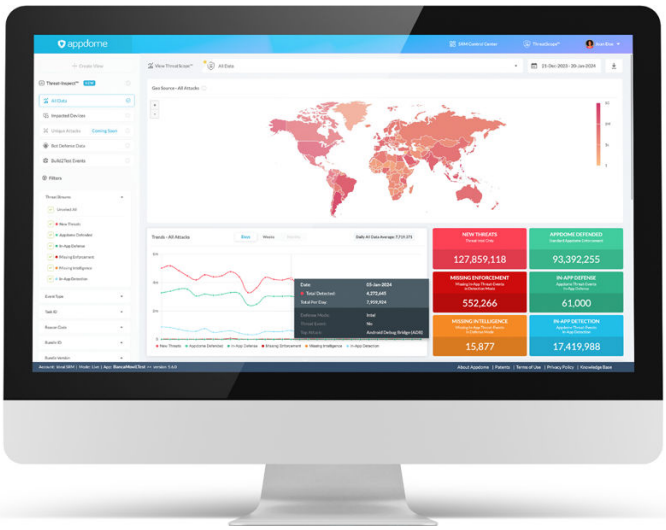
Appdome's patented Unified Mobile App Defense platform provides mobile developers, cyber security and fraud teams a centralized automation, monitoring and control center for protecting mobile apps. With Appdome, choose, build, test, release and monitor any or all of Appdome 300+ mobile app security, 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 beautiful user experiences when 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.



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™ mobile app security, 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.

MITM-SG-03152024