appdome | Microsoft Intune

No-Code UEM & MAM Integration

BUILD MICROSOFT INTUNE-READY APPS - FAST

Build Microsoft Intune into internally developed and 3rd party mobile enterprise apps in minutes; deploy & monitor in one automated platform in CI/CD.

DELIVER WORKSPACE ONE INTEGRATION 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 Intune integration in enterprise mobile apps, fast. Here's what you get by combining Appdome with CI/CD:

RAPID RELEASE & DELIVERY OF WORKSPACE ONE APPS

Getting enterprise mobile applications right requires releasing Intune integration Android and iOS apps fast. With Appdome, you do just that. Instead of needing engineering resources to code the SDK or use unreliable wrappers, you integrate Intune features in Android and iOS apps on-demand. From the CI/CD, trigger the build command in Appdome integrate Intune controls into enterprise mobile apps on demand and match the needs of the business instantly.

CONTINUOUS SECURITY FOR MOBILE APPLICATIONS

Mobile apps and operating systems change constantly. New UEM and MAM capabilities are added and updated by Microsoft continuously. Appdome automatically adjusts and adapts each Intune feature to the changes in the updated mobile app and operating system version. Release-by-release, no manual work, retooling, or coding change are needed to make Intune features work in the new app. Instead, Appdome does that for you and provides continuous Intune feature-functionality across all mobile app versions and releases with ease.

FULL SUITE OF INTUNE SERVICES

Using Appdome, organizations can bring Android and iOS apps built in any environment into the Intune environment quickly and easily. Appdome delivers an instant implementation of the Intune into native and hybrid mobile apps, providing organizations immediate mobile app management and security in minutes, all without any coding. Appdome also allows organizations to combine the Intune SDK with other services including a broad set of authentication services, VPN, connections to secure browsing, email and more, to tailor-make applications and support critical use cases inside the enterprise.

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.

DEPLOY WORK APPS TO PRIVATE & PUBLIC STORES

Appdome makes it fast and easy to secure and manage enterprise mobile apps with Microsoft Intune. Add Microsoft Intune to any mobile app, including internally built or 3rd party enterprise apps without coding, SDKs or app wrappers. Build Intune-specific apps and deploy them in the Intune store or in public iOS App and Android Play stores. Eliminate engineering work, integration complexity and compatibility gaps by leveraging machine learning to build Microsoft Intune into Android & iOS mobile apps - fully automated.

FULL MICROSOFT INTUNE ONE FEATURE COVERAGE

Extend your seamless Microsoft access, authentication and management experience to all your non-Microsoft mobile apps without any burden on the mobile engineering team.

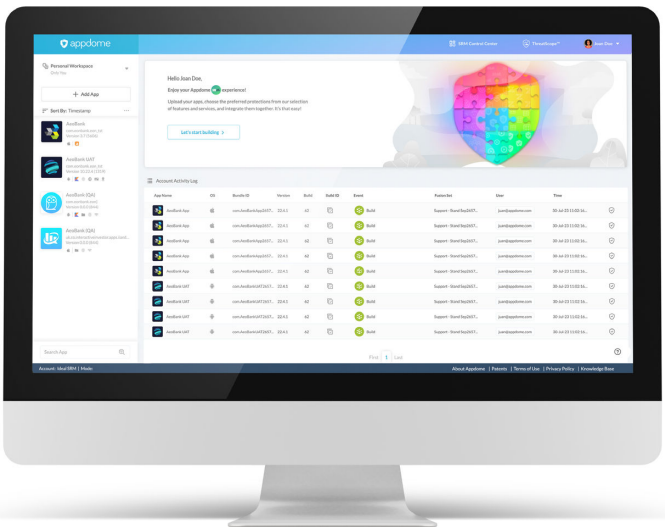
- **Data Protection:** Leverage data-at-rest encryption, data loss prevention (DLP) policy protection, privacy camera and blur screen and more.
- **Authentication:** Achieve password compliance and tie into enterprise authentication services.
- **Tunneling:** Achieve MAM/UEM in-app tunneling to ensure secure data in transit.
- **Extended Controls:** Use Appdome MAM/UEM add-on features like BoostEMM™ and Mobile Permission Control™ for secure browser, email, document sharing, limiting local contacts and calendars, and more.

Included with every Intune implementation, Appdome adds ONEShield protection to each app, providing a wide range of advanced security features that protect the logic, structure and code of the app itself. This comprehensive feature set includes anti-tampering, anti-debugging, anti-reversing and other app hardening tools.

With Appdome apps for the workplace can achieve complete protection for all managed and unmanaged endpoints and protect corporate data from security attacks. Protect mobile users, remote work and WFH employees from social engineering, mobile malware, data breaches 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

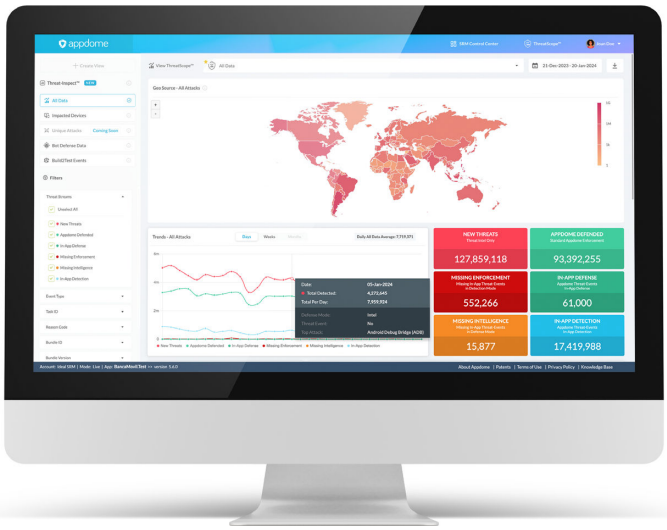
Appdome's patented Unified Mobile App Defense platform provides mobile developers, cyber security and fraud teams a centralized automation, monitoring and control center for protecting mobile apps. With Appdome, choose, build, test, release and monitor any or all of Appdome 300+ mobile app security,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

MII-SG-04152024