

MOBILE APP SECURITY WITH DEVSECOPS SPEED AND AGILITY

Accelerate mobile app security projects, integrate security into CI/CD and secure more mobile apps fast.

WHY AUTOMATE MOBILE APP SECURITY

Today, mobile development is a highly automated process with developers using powerful coding and low-code development environments, frameworks and pre-built open source libraries as well as CI/CD systems to rapidly build and release Android and iOS apps to the public. Likewise, hackers and malicious actors rely heavily on automated tools to hack, disassemble, extract, decompile, interfere, and exploit mobile apps individually and at scale. No developer really codes an app line-by-line. No hacker really attacks apps, app-by-app. Building mobile apps and attacking mobile apps are both, done at scale.

MOBILE APP SECURITY AT SCALE

Appdome-DEV brings the power of DevSecOps automation to Android and iOS app security, accelerating mobile app security projects, simplifying security release cycles and improving secure mobile app delivery. With Appdome-DEV, dev, security or DevOps teams can seamlessly build any number of custom or pre-defined sets of mobile app security features into 1, 100, or 1000s of mobile applications simultaneously. With Appdome-DEV, Appdome's product can be integrated to an organization's Continuous Integration/Continuous Delivery (CI/CD) systems, allowing continuous and consistent security implementations, team collaboration and automated and secure app signing and more. With Appdome-DEV, every build is guaranteed to meet the security requirements demanded of your business and users.

WHY CHOOSE APPDOME-DEV

Appdome-DEV brings the power of DevSecOps automation to the challenge of securing Android and iOS apps. Appdome-DEV is the only mobile app security automation tool designed and built to secure mobile apps, build-by-build, at scale. This eliminates the bottleneck and challenges that often come with securing mobile apps within an automated development pipeline. It also reduces the risk that security features and objectives will hold up release cycles, bridging the gap between development and security compliance.

Appdome-DEV expands Appdome's no-code mobile security capabilities, providing all the tools needed to accelerate mobile security lifecycles and meet mobile security objectives fast. Inside Appdome-DEV, organizations will find a rich set of APIs used to integrate Appdome's no code security platform with, and generate security builds of mobile apps, directly from CI/CD tools (such as Jenkins, Travis, Fastlane and GitLab CI). In addition, Appdome-DEV provides unlimited mobile security templates, Release-Team Workspaces and team management, automated app signing and validation, automated app publishing, as well as the ability to track, report and verify security builds across Android and iOS mobile app lifecycles.

Appdome-DEV also provides Appdome's highest level of support SLAs including response and the industry's only security resolution SLA.

KEY FEATURES AND BENEFITS OF APPDOME-DEV

Mobile Release Teams

Appdome Teams & Workspaces provide roles, segregation of duties, and collaboration across the organization and speed mobile app security releases. Appdome Teams and Workspaces allows owners of a specific organizational responsibilities to come together to complete mobile security projects. For example, team members can include experts on development, security, IAM, delivery and other areas related to the mobile app lifecycle. Appdome supports two models of Teams: Organization (internal users only) and Open (internal and external users). For example, using the Open Team Model, an organization that builds mobile apps for customers, can invite the customer to become a member of the team so that they can add the right network configurations to the Fused app and sign it with their enterprise developer certificates. Appdome Teams are unique separate entities that exist in a secure, private, multi-tenant environment.

Release Team Management

Appdome supports two entitlement models for Release Teams: Collaborate and Manage. *Collaborate* allows release team members to claim and assign responsibilities in an open flexible system of entitlements. This collaborative workflow empowers diverse functional areas to perform the work needed to release an app. *Manage* allows a team leader to assign entitlements to different release team members, according to their expertise for the different steps in the mobile integration workflow. For example, app-signing entitlements can be given to team members who are not part of the development organization. Manage also allows approvals of mobile integration and publication. Organizations can use different models for testing and production to improve mobile app delivery.

Security and Integration Templates

Mobile developers and DevOps teams can create re-usable mobile security templates, called Fusion Sets™ on Appdome. Fusion Sets allow organizations to specify the security features needed in each Android and iOS app, using these Fusion Sets to consistently meet mobile app security objectives, meet compliance objectives and more. Fusion Sets can include any combination of Appdome and third-party features, SDKs or APIs available on Appdome. Using Feature-Freeze™, an individual user or authorized Appdome team member can lock a Fusion Set for production use, guaranteeing that the approved Fusion Set will not be changed. Organizations can subscribe one or more Android or iOS app to each Fusion Set, to complete end-to-end mobile security lifecycles automatically, build-by-build.

Flex-Release™ - Shareable Security Projects

With Flex-Release, key members of the DevOps team can test and determine the correct integrations and approve Fusion Sets and/or Fused Apps, before sharing them with a different production team. Once in production, that Fusion Set is fully integrated in the automatic build system, without impacting the workload for the production DevOps team. Build-by-build, the organization can guarantee that the required third-party services are integrated into the app.

Sign-Right™ App Signing & Auto Publishing

Appdome offers the mobile industry's first automatic secure app signing and sign verification service. It automates the app signing process and ensures that Fused apps are signed correctly, thus eliminating common signing errors which plague manual mobile integration projects. In addition, inside Appdome-DEV, organizations can use Appdome to published Appdome secured apps directly to public and private app stores.

Appdome-DEV APIs and CI/CD Integration

An optional feature, Appdome-DEV APIs are a collection of APIs that connect all key steps in Appdome's no-code security process, such as Build, Fuse, Sign, Publish and Fusion Notify, to CI/CD automation systems (such as Jenkins and GitLab CI). This allows development teams to integrate one or more Appdome processes into existing workflows without impact. With Appdome-DEV APIs, developers can choose to rely on Appdome for security features only and/or extend use of Appdome for automatic signing and publishing of Android and iOS apps to any public app stores (like Apple's AppStore or Google's Google Play) or private app stores (such as Microsoft Intune, and VMware Workspace ONE).

Appdome-DEV Events™

An optional feature, Appdome's DEV-Events lets developers code unique app outcomes based on the security event triggered by Appdome. DEV-Events offers the full-range mobile defense and threat events for each security feature on Appdome such as jailbreak and rooting, MiTM violations, tampering, debugging, emulators, simulators. DEV-Events use industry standard notification methods to pass events between the Appdome layer to the app, informing the app any time a malicious event occurs against or in respect of the Appdome protected app. These notifications can be used inside apps to alter the behavior of an app when a threat event occurs, such as closing the app, disabling functionality in the app, scoring the threat and/or using the event in external threat management systems.

Appdome-DEV PLUS™

An optional feature, Appdome-DEV PLUS is an enhanced offering that lets customers meet the requirements of high-volume and/or multi-app rollouts. For pre-release testing and verification, Appdome-DEV PLUS provides Appdome Certified Release™, a dedicated Appdome release team that conducts pre-release app security and workflow testing, and enhanced response times. For high-volume production deployments, Appdome-DEV PLUS also provides Appdome's API Enterprise Suite, to scale up simultaneous security builds across 100s or 1000s of mobile apps. Customers requiring support for older mobile OSs or device list, can also purchase Appdome-DEV PLUS Extended Support. These powerful options ensure that high-volume release schedules will be achieved consistently with the highest level of security.

Learn more about Appdome at www.appdome.com or open an Appdome account at fusion.appdome.com.

ABOUT APPDOME

Appdome changes the way people build mobile apps. Appdome's industry defining no-code mobile solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new security, authentication, access, enterprise mobility, mobile threat, analytics and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 150+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.

*Yehuda et al. Method and system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.