BlueCedar

The Blue Cedar Platform

The Blue Cedar Platform is transforming mobile app deployment by orchestrating release activities across disparate teams and systems, to minimize deployment delays and enable compliance with security policies and regulations. The Platform, built on cloud-native technology, easily integrates with existing mobile security and deployment tools, preserving existing investments and extending these tools with workflow support and Blue Cedar's unique No-Code Integration service.
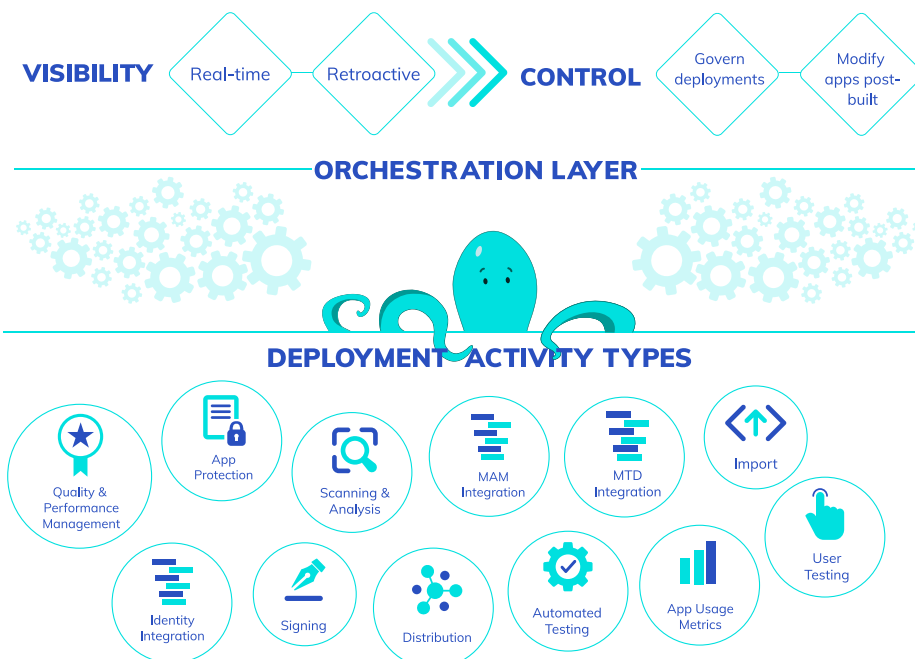
Workflows

A Platform subscription includes standard workflows, listed below, that orchestrate the activities for common deployment use cases so organizations can realize value from the Platform immediately.

- **No-Code Integration:** Add controls to an already developed mobile app without requiring source code, developers, or compatibility between SDKs and app frameworks.

- **Apps for Multiple UEMs:** Deploy apps in situations with more than one unified endpoint management (UEM) solution by performing post-build adaptations of a mobile app to produce multiple app variants, each compatible with a different UEM.

- **App Distribution:** Streamlines app distribution by publishing variants of an app through different distribution channels, with each variant appropriately customized for a channel.

Benefits

- Jump-start mobile app deployments with standard workflows that are available for common use cases

- Extend the reach of workflows by taking advantage of integrations with your mobile technology stack

- Add new functionality to already developed mobile apps without writing code

- Rapidly respond to stalled workflows via a global dashboard that provides visibility about app deployments

- Provide evidence for compliance by using the automatically recorded history of all deployment data

VISIBILITY — Real-time — Retroactive — **CONTROL** — Govern deployments — Modify apps post-built

ORCHESTRATION LAYER

DEPLOYMENT ACTIVITY TYPES

Quality & Performance Management · App Protection · Scanning & Analysis · MAM Integration · MTD Integration · Import · Identity Integration · Signing · Distribution · Automated Testing · App Usage Metrics · User Testing
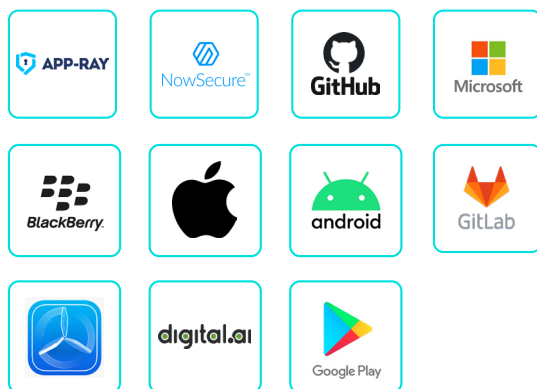
Integrations

The Platform integrates with existing mobile security and deployment tools to extend the reach of deployment workflows. Steps, which are the activities performed on apps to progress them through workflows, are how the Platform accesses these tools. Steps can be grouped into the following functions.

- **Import:** Import apps via integrations with build systems (CI/CD) or other app sources.
- **Scanning & Analysis:** Scan app binaries to provide information about implementation details and identify security vulnerabilities.
- **No-Code Integration:** Add new functions into already compiled apps without the need to write code.
- **App Hardening:** Protect app binaries by applying techniques including code obfuscation and anti-tampering.
- **Signing:** Digitally sign iOS and Android apps.
- **Testing:** Collect user feedback and results from mobile testing services for apps.
- **Distribution:** Push apps to app catalogs, app stores, or other distribution mechanisms.

Third-Party Integrations

No-Code Integration Service

A unique No-Code Integration service adds new functionality such as mobile application management (MAM), an in-app VPN, mobile threat defense (MTD), analytics, and authentication to mobile apps without requiring source code access or writing code. The ability to intercept function calls from the app to the network layer means that the service can be applied to mobile apps developed on any app framework.
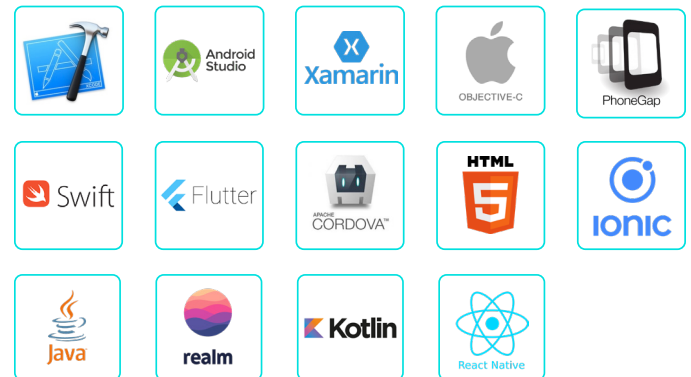
Global Dashboard

The global dashboard provides organization-wide visibility of stalled workflows, enabling rapid response from development and operations teams. The dashboard is customizable through the addition or deletion of dashboard widgets.

Digital Audit Trail

The Platform automatically captures all data generated by execution of workflows, including events and statuses associated with an app, workflow activities, and artifacts, such as app binaries and reports. This digital audit trail can be used to demonstrate that a deployment complied with security policies and regulations, and also provides traceability. Normalized deployment data can also be exported from the Platform for use by other IT systems.

325 Pacific Avenue, San Francisco, CA 94111

info@bluecedar.com / bluecedar.com

12022020