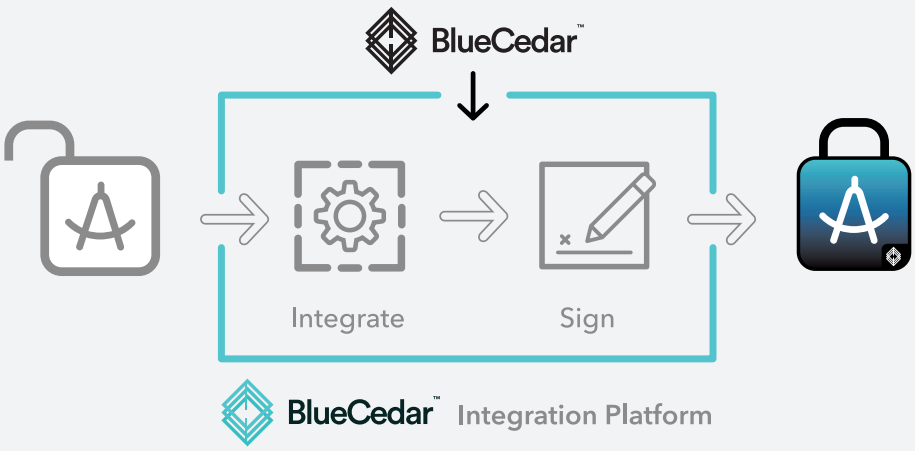
BlueCedar™

DATA SHEET

Blue Cedar Accelerator for Secure Edge Data

Blue Cedar is the leading mobile app security integration platform that secures and accelerates the deployment of native and third-party mobile apps through an automated, no-code solution. The Blue Cedar Accelerator for Secure Edge Data automatically embeds security to protect and control app data stored locally on the device. The integrated solution provides a frictionless method to rapidly secure mobile apps with military-grade cryptography and enable enterprise-level controls, while saving substantial development hours and IT budget.



NOTE: The Blue Cedar platform can be deployed on-premises or in the cloud.

One-Click Integration

With Blue Cedar, enabling device-independent encryption and policy control over app data stored locally on the device is an incredibly simple process. Simply upload an unsigned iOS or Android app to the Blue Cedar platform, click a button and the platform generates a Blue Cedar-secured app that will ensure protection of locally stored app data, even if the device passcode is compromised. Zero coding and zero SecDevOps resources are required to create the integrated app.

FEATURES

- **Deployment Options.** Blue Cedar can be deployed on-premises or in the cloud.
- **Mobile OS Support.** Blue Cedar can integrate apps built for iOS v10 and higher, and Android v5 and higher.
- **Security Controls.** The Blue Cedar Accelerator for Secure Edge Data embeds the following security controls over apps.
  - Data Encryption
  - Fingerprint Authentication
  - Jailbreak/Root Detection
  - PIN/Passphrase
- **Development Frameworks.** Blue Cedar can integrate apps created using any development framework, including Xcode, Android Studio, Xamarin, Cordova, Adobe PhoneGap, HTML5, and React Native.

Spend Time On Innovating

Blue Cedar makes the complex process of app integration appear to be trivial. The process of intercepting tens of thousands of function calls, overriding classes and methods, making static changes in the app binaries, enabling runtime trapping, and more, is completely invisible to the developer and is performed automatically without introducing faults. Other than security-related changes to the user flow that the Blue Cedar Accelerator for Secure Edge Data introduces, integrated apps function exactly the same way as they did before. Blue Cedar enables developers to spend more time on app innovations instead of on integrating security because of updates to the app or security libraries.

Develop Your Way

Blue Cedar provides enterprise developers with choice. The Blue Cedar platform can be deployed on premises, a requirement for many enterprise customers, or can be used in the cloud. The platform can integrate the enterprise-grade security enabled by this accelerator into any app, regardless of the app framework and databases used for development.

Granular Policy Controls

The Blue Cedar Accelerator for Secure Edge Data provides all the security controls needed to protect the app and its locally stored data, regardless of whether the device is managed by MDM or not. Master policy profiles, which are collections of individual policies, provide a streamlined way to create multiple integrated apps that have the same set of policy controls. Details about the policies available with this accelerator are provided below.

Policy Name	Description
Data Encryption	Secure locally stored app data with device-independent encryption.
Fingerprint Authentication	Allow users to access the app using fingerprint biometric authentication.
Jailbreak/Root Detection	Prevent app from launching or running if the device is jailbroken or rooted.
PIN/Passphrase	Specify whether a PIN or a passphrase is required to access the app. The configuration options available for this policy are listed below. • Require a minimum length for the PIN/passphrase. • Configure the amount of inactive time after which a user must authenticate into the app. • Require a passphrase to contain one or more of the following: alphabet, lowercase letters, uppercase letters, numbers and/or special characters. • Prevent a user from using a prior PIN or passphrase. • Configure the interval at which the app passphrase must be changed and when to remind the user. • Require users to select a complex PIN or password. • Specify the number of failed login attempts after which a user will be locked out.

325 Pacific Avenue, San Francisco, CA 94111
info@bluecedar.com / bluecedar.com

04232019