Leading Global Bank's Mobile Chat App Secured with Zero Coding

Enables global user-first mobile strategy, while complying with the bank's zero-risk security requirements for enterprise mobile apps

Challenge

The End User Computing division procures, provisions, and manages mobile devices for the bank, along with other solutions that improve employees' experience. One of these is a high-trust industry standard messaging solution for compliance-sensitive organizations, which was rolled out in mid-2019 for access via laptops and desktops. The bank is experiencing viral user adoption of the solution across its target users—it now processes over 200,000 messages per day and supports thousands of active groups.

In late 2019, to fully realize the messaging solution's potential, the bank devised plans to offer a mobile option. However, the messaging solution's native mobile apps do not fully comply with security requirements of the bank's cybersecurity organization. As a result, the cybersecurity organization required use of its standard mobile app management (MAM) solution, BlackBerry Dynamics, with these apps, in order to ensure that all mandatory policies and controls are enforced when the app is in use.

In order to run the messaging apps within its MAM container, the End User Computing division needed to write code to manually integrate BlackBerry Dynamics SDKs into the mobile apps. This would have required hiring developers to perform this task, which would have negatively impacted time to market and cost of solution rollout. In addition, because the mobile apps are developed in React Native and communicate via WebSocket, a framework and communication protocol not natively supported by the BlackBerry Dynamics SDKs, hand coding this integration was not a practical solution for the bank.

Even if hiring developers were a practical solution for the bank, the cost of managing the changes over time of the mobile apps, the mobile OS or the SDKs via manual integration would have been prohibitive. The End User Computing division needed a solution to quickly create security-compliant versions of the mobile apps that could be offered to employees, in a manner that addressed these challenges.

This global bank is one of the world's leading financial institutions with close to $100B in annual revenue. It has a large global workforce and serves both businesses and consumers through operations across 35 countries.

Industry: Banking

Situation: The bank's End User Computing division was tasked with providing their employees with a mobile app for an industry standard secure messaging service, which had been virally adopted via laptop and desktop. The goal was to provide employees with an experience similar to that delivered by consumer mobile apps. This was a challenge, as the bank's security organization requires any mobile app that accesses corporate data to be managed by BlackBerry Dynamics, the bank's mobile app management (MAM) standard. The End User Computing division faced a quandary: how to rapidly deliver an ergonomic mobile user experience for the secure messaging service, while fulfilling the bank's security requirements, within the necessary timeframe?

Solution: The Blue Cedar Platform

Results:

- Delivered BlackBerry Dynamics-secured versions of the messaging apps for iOS and Android within the necessary timeframe, in advance of the bank's holiday freeze for new solution rollouts. Blue Cedar's in-app interception addressed technical incompatibilities between the BlackBerry Dynamics SDKs and the mobile apps.

- Supported the End User Computing division's user experience-focused mobile and collaboration strategy and the bank's stringent security requirements.

- Established a cost and time-efficient approach for managing mandatory updates to the mobile messaging apps, devices, mobile OSs, and SDKs.

The Solution

The End User Computing division selected Blue Cedar, which has a platform that orchestrates post-development mobile app deployment workflows for efficiency and compliance through a blend of platform services and technology integrations. The no-code service that is available through the Blue Cedar platform provides the ability to embed BlackBerry Dynamics SDKs into mobile apps without coding. The End User Computing division evaluated the Blue Cedar platform and found that the process to integrate BlackBerry Dynamics SDKs into the mobile apps was easy and almost instantaneous. All the team had to do was upload unsigned mobile app binaries to the Blue Cedar platform and click a button to generate BlackBerry Dynamics-enabled versions of these mobile apps.

The Blue Cedar platform invisibly addresses the technical incompatibilities between the mobile apps, which are developed in the cross-platform React Native framework and use the WebSocket protocol for two-way communication with its secure backend, and the BlackBerry Dynamics SDKs, which do not natively support React Native or WebSocket. This is possible because the Blue Cedar platform has deep visibility into apps, going all the way from the network to the application layer. This depth of visibility enables Blue Cedar to reliably intercept tens of thousands of mobile OS APIs to perform no-code integration of security SDKs, such as the BlackBerry Dynamics SDK, and other controls into mobile apps, regardless of the framework used to develop the apps, or the protocols by which these apps communicate.

The Benefits

Increase Organizational Productivity. The End User Computing division expects about 10,000 employees to almost immediately start using the mobile version of the messaging solution, with the remaining mobile user population adopting it over the next few months. The team expects viral adoption, with minimal internal marketing or inducements needed. Since Blue Cedar generates secured versions of the app for iOS and Android, the End User Computing division can address the need for secure workplace communication for the bank's entire mobile population.

Enable Seamless User Experience. Upon the first launch of the native mobile apps, users are required to enter the URL of the messaging solution's server deployed in the bank's infrastructure to which the apps must connect. This is a problem, as most users will not know the correct server path and there are significant chances of an error being made as users fumble through the process of correctly entering a long server URL on a small screen. Since Blue Cedar can also embed BlackBerry AppConfig into the BlackBerry Dynamics-enabled version of the mobile apps, the End User Computing division can preconfigure the app with the correct server to which it must connect. This feature improves app ergonomics and usability, and removes a source of user frustration that could negatively impact adoption of the solution. Eliminating a potential source of user calls to the help desk is also of tremendous value, as the End User Computing division is already being inundated with other mobile-related help desk calls. Over time, the team intends to use Blue Cedar to create versions of other third-party ISV apps that comply with security policies, given the ease with which the team was able to do this for the messaging app.

Support Zero-Risk Corporate Security Strategy. Blue Cedar enables the End User Computing division to balance their target mobile strategy, which is to foster widespread use of mobile apps and deliver a native experience, with the need to also meet the cybersecurity team's security requirements. The cybersecurity team had previously conducted a rigorous security assessment of BlackBerry Unified Endpoint Management (UEM), which includes BlackBerry Dynamics, and given it a stamp of approval as the corporate mobile security standard. As a result, the BlackBerry Dynamics-enabled apps generated by the Blue Cedar platform immediately met the cybersecurity team's requirement for robust app-level security. The fact that Blue Cedar is a tier one BlackBerry partner, sold and supported globally by BlackBerry, and has successfully applied its no-code technology to hundreds of other mobile apps provided the cybersecurity team with additional confidence about the efficacy of the Blue Cedar platform.

Contain Mobile Security Integration Costs. Blue Cedar was able to embed BlackBerry Dynamics SDKs into the mobile apps, despite them being written in a framework, and based on a communication protocol not supported by the BlackBerry Dynamics SDKs. As a result, the End User Computing division did not have to incur the cost and associated time delay of having the messaging solution's vendor modify the architecture of its out-of-the-box mobile apps in order to offer it to their employees. In addition, given the cybersecurity team's low risk tolerance, without Blue Cedar, the End User Computing division would have to incur the cost of app change requests multiple times a year, every time the mobile messaging apps, mobile operating systems, or BlackBerry Dynamics SDKs are updated. In addition to enabling the End User Computing division to avoid these development costs, Blue Cedar's automated integration ensures that lack of developers does not delay making compliant mobile apps available to users upon release, and every subsequent update.