

# Leading North American Bank is Rapidly Enabling a Mobile-First Transformation

Driving digital adoption and securing access to sensitive backend systems without compromising user experience

## Challenge

The bank needed a way for branch personnel to access sensitive customer data in real time in order to have an efficient process within each branch, for instance providing loan approvals. As the optimal way to drive sales, the key lines of business (LOB) tasked their app development teams to build a rich customer-focused branch marketing and compliance mobile app for use by employees at retail branches. A primary goal of this app was to enable branches to complete a series of daily compliance workflows as part of the process for delivering financial products. A secondary goal of the app was to assist branch employees with new customer acquisition and increase customer engagement by providing them with a digital alternative to coming into a branch.

Prior to the rollout of this app, the workflows were only accessible via laptops and desktops and the rate of completions was significantly lower than what it needed to be. In addition, the bank operates in a primarily a BYOD environment. Employees are provided with an allowance to purchase mobile devices, which are used to perform the bank's work. Employees are free to install and use personal mobile apps, which are often a vector by which attackers can hack mobile devices.

It was not possible to require device management controls in this BYOD environment and security became a blocker as the bank couldn't ensure protection of data of these devices. Banks are subject to very stringent risk and compliance regulations given the extremely sensitive nature of the data that they handle regularly. The branch marketing and compliance app is powered by the data from the bank's on-premises backend systems of record and applications and collects and presents customer's personally identifiable information (PII) and financial data. A data breach because the bank hadn't taken adequate precautions could cause significant brand and financial damage.



This top 10 North American has over 85,000 employees and almost \$39B in revenue annually. It is known to offer an excellent set of retail, small business and commercial banking products and services to more than 25 million customers worldwide.

**Industry:** Banking

**Situation:** In 2018 a CEO mandate was issued to drive digital adoption throughout the entire organization to improve employee efficiency and enable faster financial product sales. As a part of this initiative the bank needed to move branch employees off of slow, legacy terminal and laptop-based processes to using custom mobile apps—developed by the bank and made widely available. This created two critical challenges—protecting data on employee mobile phones not managed by the bank and enabling secure access to the on-premises backend data and application services that have compliance and risk sensitive information which the bank must protect at all costs.

**Solution:** The Blue Cedar Platform and the Blue Cedar Secure Edge in-app security accelerators

## Results:

- The Blue Cedar-secured app reduces risk by making it easy for branches to complete compliance workflows and is being adopted by all 1,200 branches in Canada.
- Blue Cedar's in-app secure microtunnels provides access to sensitive information in backend systems without needing a device agent or turning on device-level VPN.
- Blue Cedar provides the bank with continuous app-level control over corporate data, even on devices not owned or managed by the bank.
- Blue Cedar no-code security integration frees up time for developers to innovate on features that will increase customer engagement.

## The Solution

The bank conducted a rigorous pilot, in which Blue Cedar was compared against many other vendors. Blue Cedar was selected because of its ability to provide app-level, device-independent security along with its ability to design a Blue Cedar-powered security architecture stretching from mobile devices to the data center.

Blue Cedar's in-app data at rest solution provides protection and control over locally stored app data. Device-independent encryption ensures that the bank retains control over data in the custom apps, including the ability to remotely wipe data, even when the apps are being used on devices not managed by the bank.

Blue Cedar's data in transit solution enable in-app secure microtunnels to highly sensitive information behind the bank's firewall via a VPN gateway without requiring a device agent. The transient nature of microtunnels are essential to accommodate the power conservation and bandwidth optimization needs unique to mobile and edge environments. Agentless in-app connections, instead of a shared device-level VPN connection, work well with the bank's environment which is comprised of Bring Your Own Device (BYOD) for employees and customer's devices. It does not require that employees give the bank any control over their devices or require them to remember to turn the device-level VPN on and off or impact their use of personal apps.

The Blue Cedar mobile app security integration platform allows the bank to embed Blue Cedar's data at rest and data in transit controls into custom-

built mobile apps with a single click. Developers upload unsigned apps to the Blue Cedar platform, click a button and the platform generates Blue Cedar-secured apps that can be managed by IT. Zero coding and zero SecDevOps resources are required to create integrated Blue Cedar-secured apps.

## The Benefits

**Scalable, Compliant Strategy.** By using Blue Cedar to secure the branch marketing and compliance app, the bank is able to fully realize the value of both its BYOD environment, as well as the power of its backend systems by offering a wider range of financial products with decisions about a customer's eligibility being made at the branch level. As branch managers are able to easily perform individual compliance tasks from their mobile devices, the rate of completion of the compliance workflows has skyrocketed. This allows the bank to demonstrate better compliance and significantly reduces risk.

**Increased Customer Engagement.** Blue Cedar provides the bank with continuous app-level control over corporate data, even on devices not owned or managed by the bank. With security taken care of, employees across the country can use the branch marketing and compliance app with real PII to demonstrate the range of available banking services, such as initiating a loan request, paying a bill and transferring money. By demonstrating the digital banking alternatives to customers, as opposed to the time-consuming practice of visiting a branch in-person, the app increases engagement from existing customers and makes it easy to acquire new ones.

**Accelerating App Innovation.** The Blue Cedar integration platform makes it incredibly simple to embed security and enterprise controls into the mobile apps that the bank is developing. The platform continues to deliver value to the bank even after the initial integration as the custom apps are continually being refined, which is common in the mobile app development lifecycle. With every app iteration, Blue Cedar's no-code way to embed security into updated apps saves developers significant time, allowing them to focus on app innovations instead, such as how to extract the most value from the bank's backend assets to increase customer engagement.

## The Future

The bank expects to complete the mobile-first transformation faster, now that security concerns about access to backend systems and applications from devices not managed by the bank have been addressed. The dramatic increase in the completion of compliance workflows in the pilot has provided the bank with the confidence to roll out the branch and compliance app for use across all 1,200 Canadian branches because it can fully adhere with the financial industry's stringent risk and compliance regulations. Additionally, other in-flight mobile initiatives, which were previously limited to only mobile devices managed by the bank, will be expanded to also include BYOD devices and result in a significant productivity increase for the bank.