WHITE PAPER

BlueCedar

Increase Your ROI from Microsoft Endpoint Manager

Use No-Code Integration with Mobile App Deployment Orchestration

bluecedar.com

BlueCedar

WHITE PAPER

Mobile App Deployment is Challenging

Once development of a mobile app is complete, many issues must be addressed before an enterprise organization invested in Microsoft Endpoint Manager and Microsoft Intune will make that app available to its employee and contractor end users. As end users have a mix of devices, with and without mobile device management (MDM), enabling Microsoft Intune app protection policies to control corporate data is required.

Integrating SDKs into an app is not easy. Developers must build expertise for each SDK, gaining familiarity with available classes and methods along with any associated idiosyncrasies such as possible programming constraints. Knowing how to use one vendor's APIs to provide certain functionality does not guarantee that knowledge will translate to implementations using another vendor's APIs to deliver similar functionality.

Correctly integrating security SDKs is more challenging. That is the nature of cybersecurity and it holds true for the Microsoft Intune SDKs, despite the availability of extensive vendor-provided documentation. Mobile apps could come from an internal development team or from third-party vendors. In the latter case, access to app source code is almost always an insurmountable hurdle, which makes it impossible to integrate the Microsoft Intune SDKs through manual coding.

Remote access to on-premises network protected resources is another challenge for organizations. There are tremendous amounts of on-premises data that organizations want to make available to Intune-enabled apps. However, Microsoft doesn't offer an option for accessing on-premises resources from Intune-enabled apps on devices that are not enrolled in Intune.

Security is not the only mobile app deployment challenge. For example, ensuring that app signing and app distribution occur efficiently is difficult, especially when you consider that a reasonable sized enterprise may have a large mobile app portfolio. These apps will need to be updated multiple times a year, due to changes in the app code, the underlying OS or the SDKs. Each change requires resigning and redistribution. If these disjointed efforts are not optimally coordinated, organizational productivity will suffer.

How long does it take to make an app?

The standard answer would be around 4 to 5 months.[1]

1. How long does it take to make an app? Techahead.

BlueCedar

WHITE PAPER

Workflow Orchestration and No-Code Integration Solve the Challenges

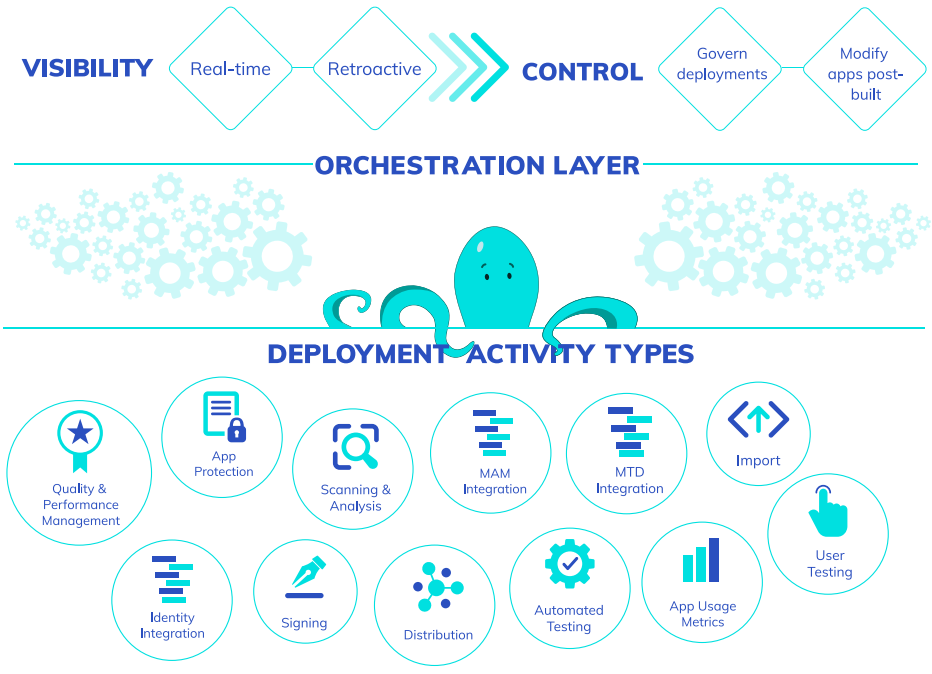
Multiple human and systems tasks are required for mobile app deployment. Current approaches to mobile app deployment are disjointed, spanning teams, systems, and processes. A deployment can be as simple as signing an app for distribution through an enterprise app catalog. Or it can be complex, requiring app scanning and analysis, modification, hardening, signing, testing, and distribution.

Orchestration solves these problems by streamlining simple and complex deployments. It also seamlessly coordinates the interplay between manual deployment activities—for example, requiring approval before publishing an app to an app store—and automated deployment activities—such as app modifications.

A requirement for such a solution is that it also performs "no-code integration" to satisfy app modification needs. No-code integration solves the problem of adding new functionality, such as that provided by Microsoft Intune or Blue Cedar Connect in-app VPN, to apps when developers are not available or when source code is not obtainable.

Orchestration with no-code integration ensures the complexities of managing multiple tools and security technologies involved in deployment does not negatively impact productivity.

The Blue Cedar Platform is a cloud solution purpose-built for deploying mobile apps. It orchestrates release activities across people and services, automating tasks where appropriate.



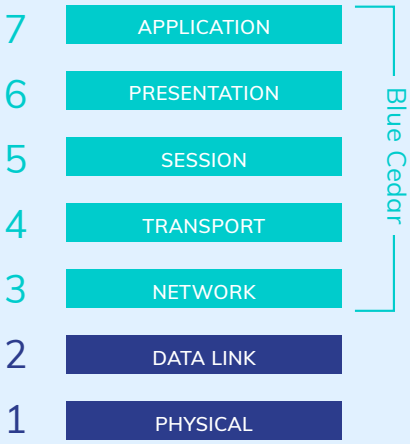
The Platform also includes a unique No-Code Integration service that makes it easy to add new functionality to mobile apps without requiring source code access or having to write code. The service has visibility from the app to the network layer and can intercept tens of thousands of APIs in mobile apps to reliably integrate new functionality. This depth of visibility means the service can be used with mobile apps developed on any app framework. Any combination of mobile application management (MAM) such as BlackBerry Dynamics, in-app VPN, mobile threat defense (MTD), analytics, or authentication can be integrated into already developed iOS and Android mobile apps.

What is an in-app VPN?

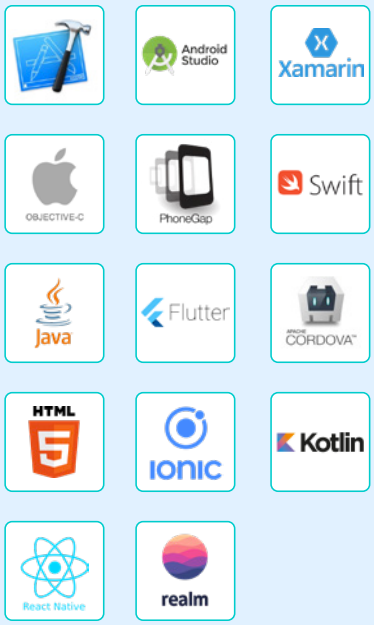
An in-app VPN is a mobile-optimized VPN client that is embedded in a mobile app to enable remote access without requiring MDM. Discrete in-app VPN connections instead of a shared device-level VPN connection work well in a Bring Your Own Device (BYOD) context as different apps can connect via different VPN configurations and servers, depending on the security level designated. Traffic from different apps is kept separate and apps can't exchange data. In-app VPNs ensure that users do not need to remember to turn the device-level VPN on and off, and the use of personal apps is not impacted.

Orchestration enables the Platform to execute efficient and error-free workflows that eliminate deployment delays, while enabling compliance with security policies and regulations. Eliminating deployment delays is important. Since organizations invest significant time and resources to maintain mobile apps, it is in their best interests to realize the benefits from this investment faster. The benefits achieved by using the Blue Cedar Platform to orchestrate deployments with the No-Code Integration service also translates into measurable increases in ROI, as illustrated with the following use cases.

App to Network Layer Visibility



Build Mobile Apps in Any Framework



BlueCedar

WHITE PAPER

Use Case 1: Secure Access from BYOD

App usage is one of the metrics by which organizations measure the success of their mobility programs. Much of the value derived from enterprise mobile apps is dependent on access to, and manipulation of, sensitive data protected by the corporate firewall. Permitting secure access from devices enrolled in Microsoft Intune is straightforward, as MDM policies can control the device VPN. It's a different story for unenrolled devices. Both users and IT have to jump through hoops to enable access to remote resources from an unmanaged device. This means app usage will suffer and can result in user abandonment if setup is too complicated. BYOD support is not something that organizations can ignore because of the savings that it represents.

Companies favouring BYOD make an annual savings of $350 per year, per employee.[2]

How No-Code Integration and Workflow Orchestration Helps

No-code integration provides an option for embedding a preconfigured in-app VPN into the mobile app being secured and addresses the problem of secure connectivity from unenrolled devices. Users no longer have to perform a separate action to establish a separate VPN session before accessing protected applications or resources (e.g., viewing paycheck stubs, helping customers, updating financial records). Not having to repeatedly create a VPN session each time access is needed delivers a better experience for business users on unenrolled devices. App usage will increase since users now only have to click on the app icon to gain access to protected resources.

ROI Example

About 2,400 employees at a North American Bank were customer-facing and used personal devices to perform work tasks. These employees valued their privacy and would not permit MDM controls over their personal devices. Independent research commissioned by the Bank showed that BYOD users worked an extra three hours per week. The Bank had purchased licenses for a VPN mobile app for these users for a total annual cost of $215,000. The initial intent was to enable them to use internal-facing custom apps that provided access to the corporate intranet and enabled viewing of training material.

2. 3 Big Risks of BYOD, Cisco.

Adoption of those custom corporate apps had been abysmal because of challenges with using the VPN client mobile app. There were many reasons for this including: employees didn't know that they had to install the VPN app; they couldn't find the app in the public app stores; those that successfully installed the app often ran into configuration issues and the app kept dropping the connection; and privacy conscious employees did not want all network traffic going through the corporate internet.

The Bank spent many months and $350,000 in developing a new banking app that would enable frontline employees to process home, auto or personal loans faster. The app permitted employees to complete the entire loan process, from qualification to disbursement, from anywhere, not just the branch offices. However, given the prior low-adoption rate of corporate app usage on BYOD, the Bank knew it needed a different approach in order to have high app usage and demonstrate a return on its investment.

With the no-code approach, the Bank was able to rapidly generate a new version of the app that had app-level security controls and an in-app VPN, which connected to its existing VPN infrastructure. BYOD users were educated about the security and privacy benefits with this app: that the bank only had visibility and control over the app and the data within, not their personal data elsewhere on the device. Since users can now launch the app to have seamless yet secure access to protected resources, app usage has soared.

Within a month of it being rolled out, all frontline employees started using the app. In the first six months, the bank has been able to demonstrate that these users are working an extra two and a half hours per week on average. This translates into an annualized benefit of $6,912,000.[3] Without a no-code solution that embedded the in-app VPN, the Bank would not have seen this tremendous adoption.

Since the Bank had spent $400,000 on the app, including all engineering costs as well as license costs for 3rd-party app security, as well as the no-code solution, the benefit represents an ROI of 1975%.

No-code integration of an in-app VPN translates into an annualized benefit of $6,912,000.

3. Assumes a $40 hourly rate across customer-facing employees, each of whom works 48 weeks per year

Use Case 2: Avoiding Vendor Lock-In

An enterprise's mobility needs will evolve over time. The capabilities offered by the enterprise's initially chosen Unified Endpoint Management (UEM) solution may no longer meet the enterprise's needs as its digital landscape transforms. Moving to another UEM is not a trivial undertaking. There are significant costs for transitioning both devices under MDM-controls and apps built with the incumbent UEM's app security SDKs.

Manual coding is an option if the app's source code is available. Those coding costs scale proportionally with the number of apps being secured. When it is just one or two apps, those costs may be palatable to the enterprise. But when an enterprise wants to secure twenty or more mobile apps, which is a likely scenario at most enterprises, relying on manual coding to port apps will give any enterprise pause.

How No-Code Integration and Workflow Orchestration Helps

No-code integration used with workflow orchestration provides a unique opportunity—giving the enterprise greater flexibility to easily switch to another UEM platform, should their current platform no longer meet their needs. By automating the process for enabling app-level security and codifying it into a reliable and repeatable deployment workflow, enterprises can focus their mobile app resources on app innovations that translate into increased app usage, that in turn increases overall organizational productivity.

ROI Example

A leading bank had secured 90 mobile apps using the app security SDK from UEM Vendor A. The bank wanted to allow users of a popular business software package that includes spreadsheets and presentations to seamlessly transition working between mobile and laptop endpoints, and share data between the mobile version of the business software and the 90 apps it had secured. A significant proportion of mobile workers use personal devices for work, which the bank does not manage. The bank wanted a single solution to permit the seamless and secure sharing of data between all mobile apps on corporate issued managed devices and unmanaged personal devices. The only way the bank could achieve this goal was by transitioning to UEM Vendor B, which permitted the seamless use of the same business software across both mobile devices and laptop endpoints, and the secure sharing of data between apps built on its app security SDK and the mobile version of the business software.

The bank estimated the cost for manually porting the apps to UEM Vendor B would require about 9 FTEs working for a year, at a cost of at least $2,000,000. This does not reflect the complete cost, as the bank had not assigned a value to the negative impact on productivity that would result by requiring mobile workers to continue using apps secured with UEM Vendor A during the year that the apps were being ported to UEM Vendor B.

Automating the process reduces that year long porting delay to a click of a button. Now, instead of $2,000,000, the cost for porting the apps to UEM Vendor B is the cost of the workflow orchestration subscription, which is a fraction of the initial estimate for manually porting the apps. The bank estimates that just the ROI for porting the apps is 200%. If it factors in the ongoing annual costs of reintegrating security, which arise when there are updates to the apps, the mobile OS platforms, or the app security SDKs, the savings from automation, when compared to manual integration, represents an annual ROI of over 500%.

The bank estimates that just the ROI for porting the apps is 200%.

Use Case 3: Eliminate SDK-Imposed Development Constraints

When an enterprise's IT department mandates that all corporate apps that access enterprise data must be secured with a particular vendor's app security SDK, it unwittingly causes significant ripples in the mobile app development lifecycle. Suddenly, app developers must build apps that conform with the constraints imposed by the mandated app security SDK. For example,

- If the app security SDK does not support a particular framework, app developers cannot develop in that framework despite all of its associated benefits.
- An app security SDK may only support an older version of a network protocol stack, which means that any developer who is manually integrating the app security SDK must make sure that her/his app is using the version of the network protocol stack that is supported by the SDK.
- The app security SDK may not provide strong enough encryption on one of the mobile OS platforms. This could mean that though the enterprise believes the app is secured, corporate data is actually vulnerable to malware that can get installed on non-managed devices.

The issues associated with the constraints imposed by app security SDKs is exacerbated with third-party ISV apps. The different Lines of Business (LOB), such as sales, marketing and HR, often want employees, contractors and consultants to use apps acquired from third parties. If the ISV app does not conform to the requirements of the mandated app security SDK, the LOB is in a quandary. The ISV will not rewrite the app to meet the constraints of a specific SDK but without app-level security IT will prevent rollout of the app.

How No-Code Integration and Workflow Orchestration Helps

The No-Code Integration service provides a translation layer between the mobile apps and the app security SDK being integrated. There is no change in the expected result of the no-code process, even if the app security SDK does not support the framework in which the app has been developed, if the app is using a network protocol stack or a UI that is not supported by the app security SDK, or anything else.

What's happening under the hood is transparent to the enterprise mobility team doing the no-code integration. With the No-Code Integration service, resources are not needed to download and install the SDK; to have developers learn about the SDK or the available classes or methods; or to understand the requirements of the SDK and possible programming constraints. And when all deployment activities, including no-code integration, are codified into a deployment workflow, all that is required is the click of a button to generate and distribute a secured app.

ROI Example

A department in a government organization wanted all of its mobile workers, including those on devices not managed by the IT department, to use a third-party secure messaging solution. Unfortunately, the app security SDK of the UEM solution that was being used did not support the framework in which the mobile app version of the secure messaging solution was written. Switching to another vendor was not an option. The IT department was satisfied with the incumbent UEM vendor and had also just recently renewed a multi-year subscription.

To integrate the UEM vendor's security, the ISV informed the organization that it would cost around $30,000 per app change request. The government organization realized that such an approach would be expensive, with their minimum eight planned annual app updates for each mobile OS. Android and iOS also each have one major annual update. The UEM vendor had planned for two updates per year to the app security SDK for each mobile OS platform. Considering all of this, the annual cost would be about a million dollars at the ISV's quoted cost per change request.

With the no-code integration approach, the government organization only had to account for the annual subscription cost of the solution. This was just a fraction of professional services costs estimated by the ISV. The government agency also quickly realized that this fraction would be even smaller, which translates into a higher ROI, than the option of going with the ISV as they used deployment workflows with the no-code integration service to secure more of the apps being used by mobile workers.

BlueCedar

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

The Blue Cedar Platform is transforming mobile app deployment by helping Fortune 500 companies, governments and independent software vendors orchestrate all app modification, security, compliance, and release activities in unified deployment pipelines. The Platform includes a no-code integration service that adds new functionality to mobile apps without requiring source code access or writing code. Blue Cedar integrates with popular tools and systems used in mobile app deployment, including GitHub, GitLab, Microsoft Endpoint Manager, BlackBerry UEM, Digital.ai, Google Play and the Apple Custom Store. Founded in 2016, Blue Cedar is funded by leading venture capital firms and is headquartered in San Francisco. For more information, visit www.bluecedar.com.

03022021