GUIDE

BlueCedar

How to Speed Your Microsoft Intune App Security and Deployment Process

Overcome Intune deployment obstacles with no-code

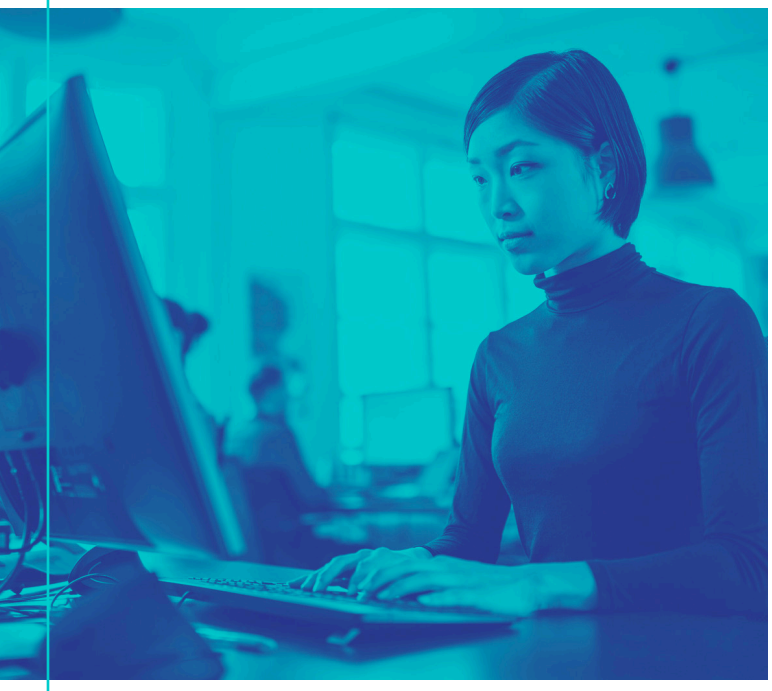
OVERVIEW

Office 365 is the most widely used enterprise cloud service. However, Microsoft Intune, which offers the potential to dramatically boost organization-wide productivity through the use of Office 365 in the Intune mobile app ecosystem, should be as widely used, but isn't. Companies have a significant amount of information in on-premises resources but can't easily enable secure access to it from Microsoft Intune apps. For organizations to realize the full potential of Microsoft Intune, a solution that easily enables secure remote access to on-premises resources from Microsoft Intune-enabled apps is needed.

Remote work accelerates many app deployment roadmaps

Launching innovative mobile apps is on every company's roadmap, whether they develop them internally or customize third-party apps. But for companies whose core business lies outside of information technology, it can be difficult to keep up with changing end-user demands and emerging technologies around mobile apps. This is especially important given **the rise in demand for mobile apps to enable remote work**. Companies are looking to rapidly develop and deploy such apps across multiple operating systems and development frameworks, and have the apps run on mobile devices with diverse device management profiles, to address today's remote and mobile workforce.

We've all seen the headlines and know that the risk of a cybersecurity breach is constant. As more workers access corporate data around the clock, from unenrolled devices, keeping that data secure will continue to be a massive challenge. The big issue that keeps IT operations and security teams up at night is providing strong security, while still delivering on rapid app deployment and upgrade timelines.



Why organizations want Microsoft Intune

Microsoft understands that organizations need a cohesive way to manage their mobile app programs for a diverse digital ecosystem that includes enrolled and unenrolled devices. The promise of Microsoft Intune, which facilitates mobile device management (MDM) and mobile application management (MAM) from a single console, is significant. Intune gives IT admins app-level controls over corporate data in Intune-enabled apps, even on unenrolled devices. Key for these security controls is the protection enabled by the Intune app SDKs and the integration with Azure Active Directory, which provide robust authentication services.

The growth of Intune coincides with the strength of Microsoft 365, which has become the most widely used enterprise cloud service based on sheer enrollment. For companies invested in Microsoft 365, the ability to use Intune-enabled apps at scale—whether built in-house or obtained from third parties—is essential to fostering greater corporate productivity.

When Microsoft 365 is used within the Intune app ecosystem, it allows safe sharing of corporate data between apps, so users can complete complex workflows entirely on their mobile devices. Intune offers a method for encrypting and controlling data at the app level, with access and authentication to Microsoft's identity services. It provides organizations with a single source of app management, whether the device is under MDM controls or not. Workers using Microsoft 365 apps on their personal mobile devices know that they'll never have to sacrifice privacy. Since IT can set policies that allow company data to be only shared between Microsoft 365 and other Intune enabled apps, there is no mixing of corporate and personal data and no reason for IT to need device-level controls.

App-level security controls that don't require device enrollment keep everyone happy—users don't have to sacrifice privacy and IT doesn't have to compromise on security.

The problem? Integration isn't straightforward.

Despite the obvious benefits of Intune, many organizations aren't using its MAM functionality. Manually integrating Intune SDKs into apps and enabling secure backend connectivity to assets that live behind the firewall (and not on Azure) has proven to be a challenge—one that has prevented many organizations from realizing the true benefits of Intune. Many organizations are still struggling with several key issues, such as access to on-premises resources, enabling Intune in third-party apps when source code isn't accessible, single sign-on (SSO), and organizing the myriad tasks in the post-development deployment process.

The last barriers to Intune adoption

IT organizations trying to solve security concerns and enable ease-of-use often discover that deploying Intune-enabled apps that satisfy the needs of all constituents can be a lengthy, complicated process. Some challenges are common to all mobile app deployment processes, such as seamlessly obtaining apps from build systems (CI/CD), app signing, and app distribution. Others are unique to Intune.

Accessing On-Premises Resources

First, there's the on-going issue of giving authorized users on unenrolled devices access to firewalled data. Today, every time a user on an unenrolled device wants to access a backend system, such as a database, they must manually start a device-level VPN and authenticate to the corporate VPN gateway. This has the effect of routing all data, including personal data, through the corporate network.

Currently, organizations cannot use Intune-enabled apps to securely access on-premises resources without bringing devices under management. This is especially challenging in a time where many employees are working remotely and may be using their own devices that are not under management.

The problems with this are:

- **There's nothing simple or seamless about enabling remote access.**
- **It compromises users' privacy.**
- **It defeats the original purpose of a mobile app.**

Instead of helping end users accomplish something faster and more effectively, it makes them more frustrated and more likely to try solutions that aren't secure.

App Integration

Second, there's the process of integration with the Microsoft Intune SDKs and Microsoft Azure ADAL, to secure the mobile app and enable SSO. As with all SDKs, there is a steep learning curve to integrate the Intune SDKs into apps. Developers are already suffering from SDK fatigue and the Intune SDK makes it worse. Why?

- **Initial integration takes weeks of developer time.** This costly process often delays the launch of new apps.
- **Ongoing updates continually drain resources.** Every time an app is updated, which happens multiple times a year, it must be secured all over again.

Secure SSO

Many organizations want a secure way for users to access multiple apps using SSO, without bringing devices under management. In today's complex environment with remote work and BYOD devices, this simplified user experience is difficult to attain without sacrificing security.

A simple, value-adding security and orchestration solution

Fortunately, there's a way to solve the Intune-specific issues, as well as challenges common to all mobile app deployments with The Blue Cedar Platform, which has been tried and tested by leaders across industries, including finance, insurance, healthcare, government and energy. The Blue Cedar Platform is purpose-built for deploying mobile apps and also provides a No-Code Integration Service that adds new functionality to apps without requiring source code access or writing code.

1. **No-Code Integration Service.** Organizations use Blue Cedar's No-Code Integration Service in mobile app deployment workflows to add the app protection policies of Intune and the SSO enabled by Microsoft Azure ADAL to mobile apps. An optional in-app VPN can also be added to enable secure remote access. The No-Code Integration Service has proven to be particularly valuable for organizations deploying third party apps, for which they don't have source code.
2. **Mobile App Deployment.** Blue Cedar is streamlining mobile app deployment by orchestrating release activities across people and services through workflows that apply to apps post-build. Codifying releases activities into workflows, and automating tasks where appropriate, eliminates deployment delays while enabling compliance with security policies and regulations.

A straightforward solution that solves complicated problems

Solved: Rapid App Integration

By using Blue Cedar's No-Code Integration Service in workflows, organizations can dramatically speed the integration of Microsoft Intune into internally developed or third-party ISV mobile apps, reducing deployment time from months to minutes. No weeks-long process, no developer dependencies, no expensive outsourcing required, and a much lower risk of manual coding and security errors. It even integrates apps when an organization doesn't have the app's source code, or if the SDK being integrated is incompatible with the framework used for developing the app. Organizations can now rapidly deploy and upgrade apps to speed deployment times and respond to today's business needs.

Blue Cedar gives your business an edge

10x
cost savings

3x
faster time to value

Reduces
coding errors

BlueCedar

GUIDE

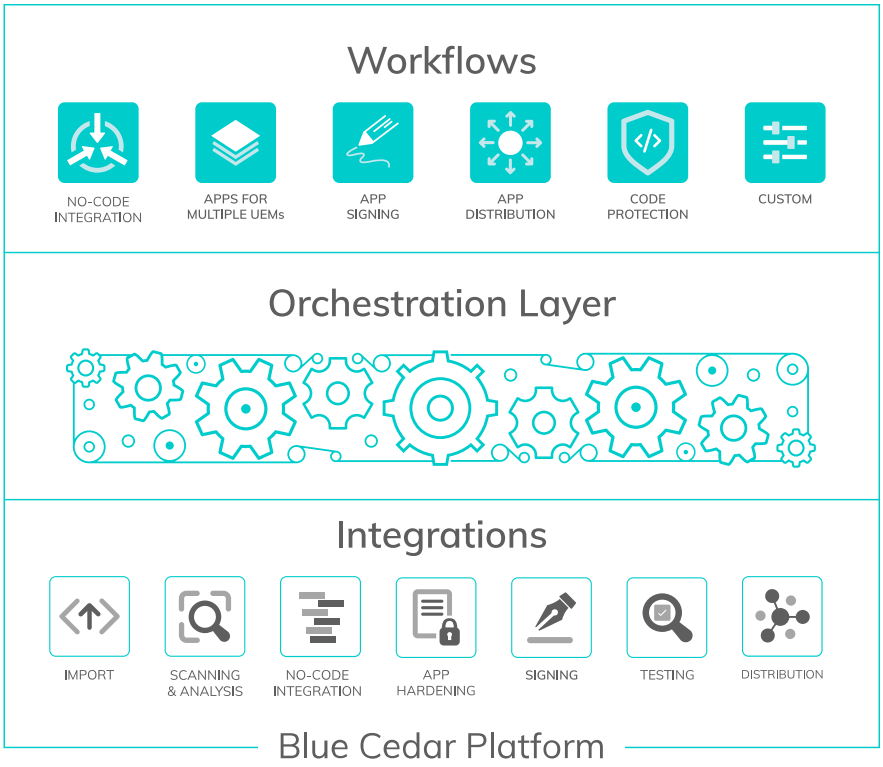
Solved: Remote Access to On-Premises Resources with SSO

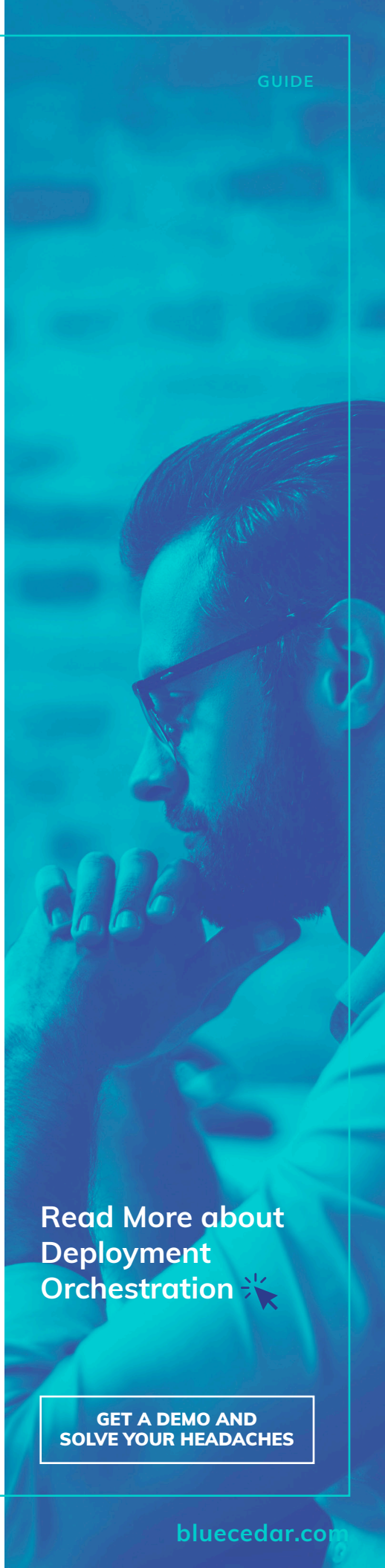
Blue Cedar provides Intune-enabled apps with secure VPN access to both on-premises and cloud databases without bringing devices under management. It also enables SSO to enhance the user experience, still without requiring organizations to bring devices under management. Organizations can now solve the backend challenges that were restricting access to valuable data and create a better, more efficient user experience.

Solved: Streamlined Mobile App Deployment

Blue Cedar addresses the challenges that are common to all mobile app deployments by coordinating activities across people and systems through workflows, cloud-based collaboration, and automation. Transform and streamline the app deployment orchestration process with central management of people and process.

- **Standard workflows:** Speed time to market and provide replicable processes for faster, more efficient mobile app deployment and upgrade management.
- **Third-party integrations:** Use existing security and deployment tools to extend the reach of workflows and the value derived from these tools.
- **Global dashboard:** Visibility about all app deployments enables rapid response from development and operations teams.
- **Activity audit trail:** Automatic capture of all deployment data provides evidence for compliance and supports traceability.





Read More about Deployment Orchestration

GET A DEMO AND SOLVE YOUR HEADACHES

bluecedar.com

BIAC Representing BlueCedar in Canada.
biacbroadband.ca (866) 941-5119 Ext. 120

Member of
Microsoft Intelligent Security Association
Microsoft

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.

10192020