BlueCedar

# Accelerate Security Integration for Your Mobile Apps

Deploy Microsoft Intune-enabled apps faster

# What's getting in the way of rapid mobile app deployment?

Mobile apps drive critical business functions, and developing and launching them is a top priority for companies across industries. But even as DevOps teams make their internal processes more agile and efficient, there's one critical step that can add weeks to deployment cycles: the process of securing mobile apps.

Securing apps before release is essential, but that's not the only time it must be done. Every time an app or its associated components are updated–including the OS, third-party libraries, open source software, or security SDKs–it must be secured again.

Organizations are forced to weigh the risks of prioritizing innovative new apps over security, a trade-off that is fraught with risk.

It's a choice they shouldn't have to make.

# Why DevOps teams dread the process of securing apps

### It's time-consuming.

Keeping up with updates, patches, and changing security requirements requires huge amounts of time. Developers want to build new apps and improve existing ones. Instead, they have to spend hours protecting the products they've already created.

### It's costly.

Developer time is valuable, and the hours they spend securing apps comes with a high price tag. Outsourcing the process is a logical alternative–and an expensive one. But even if cost is no obstacle, there simply aren't enough mobile security developers to meet the ever-growing demand.

### It comes with significant risks.

The traditional way of securing mobile apps requires a lot of manual coding, and even the smallest error can create new security vulnerabilities. In addition, many developers depend on reusable software components, which can pass vulnerabilities between apps.

**6 weeks**
the average time it takes to secure a mobile app before launch[1]

**48% of IT leaders**
reported a security skills shortage[2]

**Nearly 70%**
of every application is comprised of reusable software components–such as third-party libraries or open-source software–causing applications to "inherit" their vulnerabilities[3]

[1] Top 100 Financial Services Provider
[2] Salesforce, State of IT Report
[3] WhiteHat Security, 2018 Application Security Statistics Report

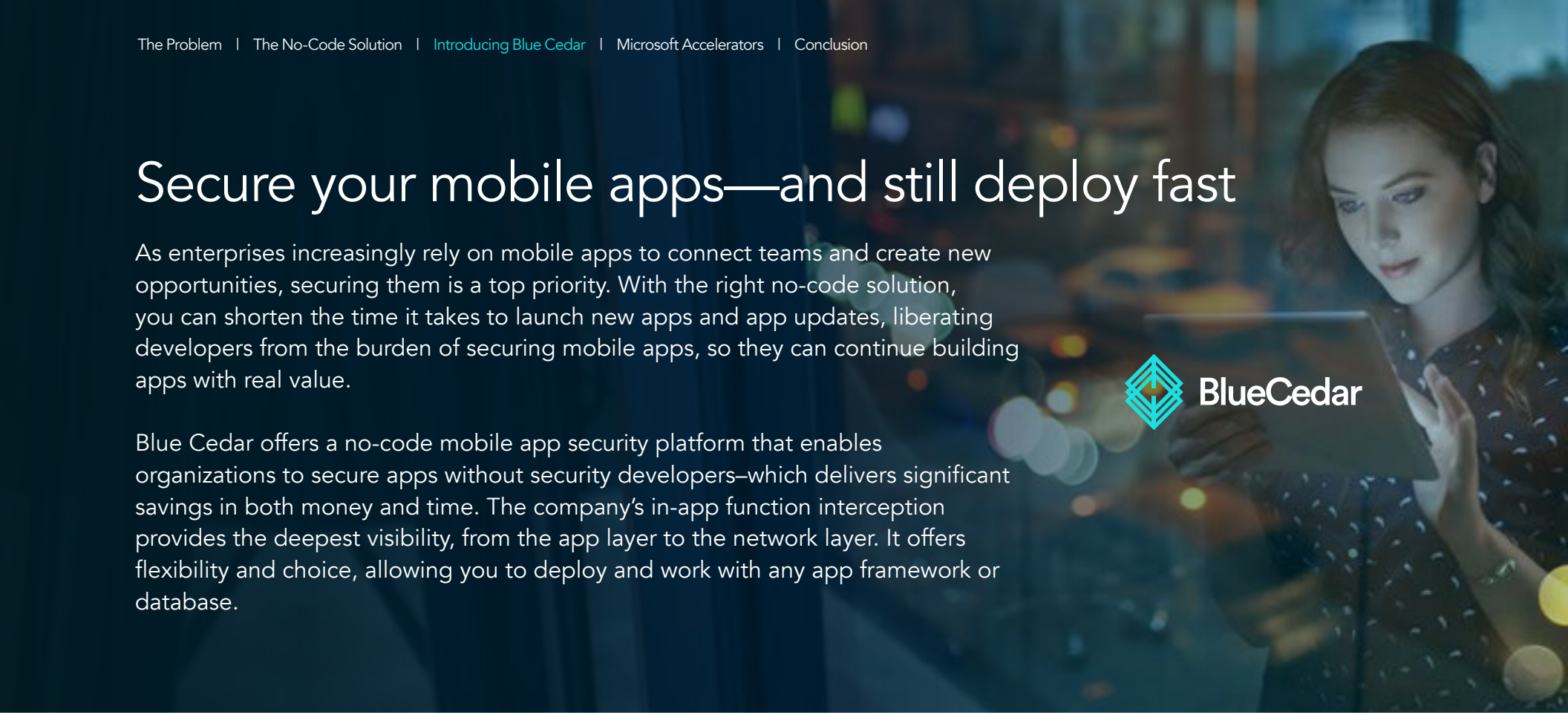
# The solution? A no-code approach

While securing mobile apps creates a number of challenges, it's a crucial line of defense against growing threats to enterprise data. How can DevOps balance the need for security with the urgent need for apps that support business growth?

No-code solutions are a compelling answer, providing a shortcut for specific aspects of the development process. With a no-code solution, teams can speed up labor-intensive tasks, while allowing developers to stay focused on what they do best.

## Gain an edge with a simple no-code solution for securing mobile apps

- **Speed app release and update cycles.** Shorten the time it takes to secure your apps from six weeks to hours–so you can launch new apps and updates faster.
- **Reduce dependence on costly development resources.** Secure your apps more affordably, without reserving hours of developer time.
- **Keep up with changing security regulations.** With shorter, less complicated cycle times, you don't have to dread new security requirements.
- **Ensure accuracy and consistency across all applications, all the time.** Even the best developers are human, and automation helps eliminate mistakes, integrating the right code in the right place.
- **Allow developers to focus on high-value tasks.** Energize your teams by giving mobile developers the freedom to keep building and customizing innovative apps.



# Secure your mobile apps—and still deploy fast

As enterprises increasingly rely on mobile apps to connect teams and create new opportunities, securing them is a top priority. With the right no-code solution, you can shorten the time it takes to launch new apps and app updates, liberating developers from the burden of securing mobile apps, so they can continue building apps with real value.

Blue Cedar offers a no-code mobile app security platform that enables organizations to secure apps without security developers–which delivers significant savings in both money and time. The company's in-app function interception provides the deepest visibility, from the app layer to the network layer. It offers flexibility and choice, allowing you to deploy and work with any app framework or database.

BlueCedar

Deploy apps faster

Lower the risk of human error

Save hundreds of developer hours

Cut the cost of development resources

# Not all no-code solutions are created equal

The complex, multi-layered nature of digital environments creates a wealth of opportunities for attackers–and developers must address each one of them. Mobile apps can be used on a variety of devices, which are sometimes outside of enterprise control. Reducing exposures and closing gaps requires the ability to go deep into the network layer and integrate the necessary controls.

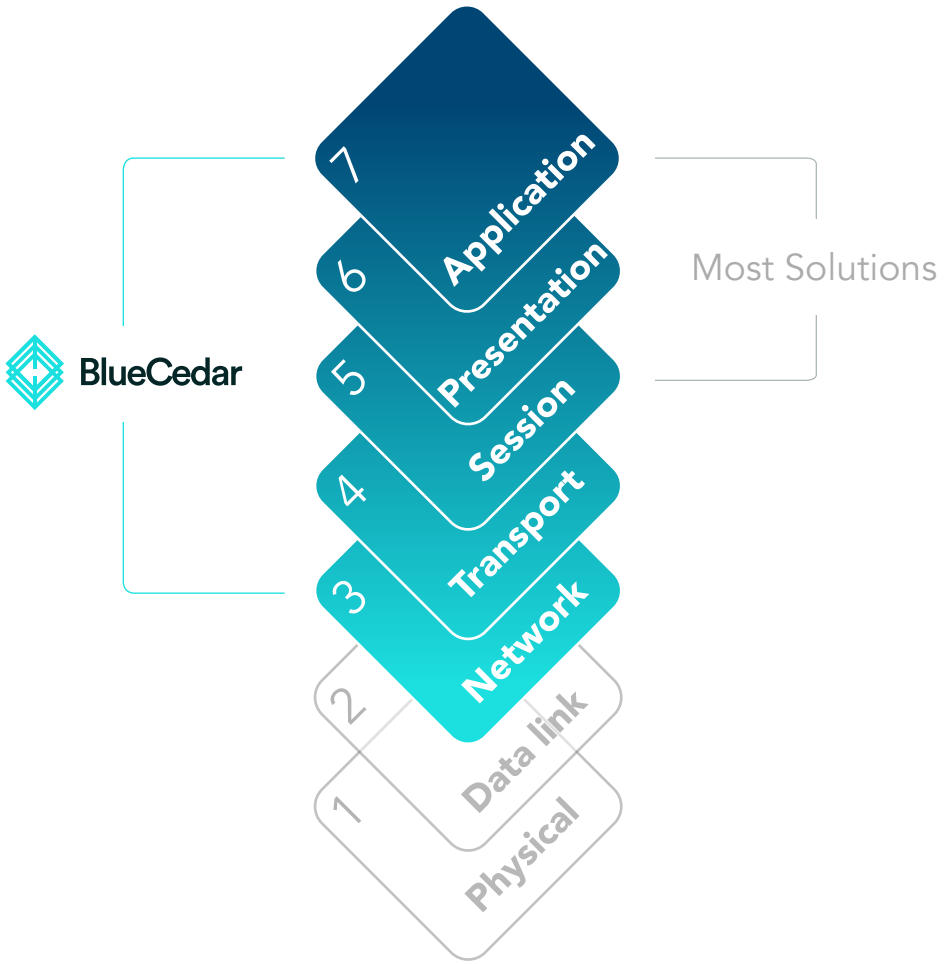
To secure mobile apps, developers must reliably intercept tens of thousands of function calls, override classes and methods, make static changes in app binaries, enable runtime trapping, and more. Solutions that only automate some of these functions still require a significant amount of developer time and intervention.

## The Blue Cedar difference: deep visibility

Blue Cedar streamlines the complex, error-prone manual process of integrating security libraries into mobile apps with a robust solution that addresses every layer. Its depth of in-app function interception sets it apart, providing deep visibility from the app (Layer 7) to the network (Layer 3).

This allows Blue Cedar to automate the many complex tasks that ensure robust app security–for better accuracy and faster completion times.

Get visibility down to the network layer



# Launch Microsoft Intune-enabled mobile apps faster


Enabling Microsoft Intune app protection policies for custom apps or third-party ISV apps is essential for secure mobile app management (MAM). But embedding those security controls into an app has traditionally been a time-consuming manual process.

With the Blue Cedar Accelerator for Microsoft, anyone can integrate Microsoft Intune app protection and a single sign-on (SSO) into apps. Blue Cedar also provides no-code embedding of pre-configured in-app VPN clients, which allows Microsoft Intune-enabled apps to securely connect to your firewalled resources without requiring end-user configuration.

## With Blue Cedar you can:

- Enable integrated apps on unenrolled devices to access network-protected resources
- Integrate Microsoft Intune SDKs & Azure ADAL into custom or ISV apps without coding
- Drive usage of apps that may be technically incompatible with Microsoft Intune SDKs

Not only does Blue Cedar allow you to accelerate adoption of your apps, but it also lowers the burden on IT teams, greatly reducing the number of required development hours and lowering associated costs.

# The Blue Cedar Advantage

**10%**
cost savings

**3x**
faster time
to value

**ZERO**
dependence on
skilled developers

Save time and money by integrating with Blue Cedar.

REQUEST DEMO

BlueCedar