BLUE CEDAR

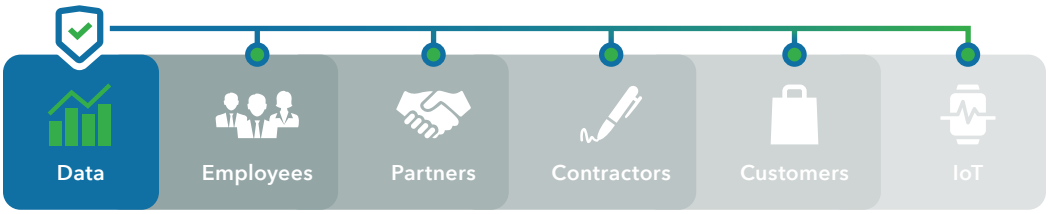
SOLUTION BRIEF

SECURE THE APP, NOT THE DEVICE.

Accelerate the Benefits of Mobility

SECURITY SHOULD ACCELERATE MOBILE ADOPTION, NOT PREVENT IT

Mobile apps are no longer just a tool to improve productivity for employees with company-owned devices. The modern enterprise relies on mobile apps to provide secure access to sensitive data for both employees and "extended enterprise" workers like franchisees, seasonal workers, partners and contractors who all have their own devices. In addition, the most innovative businesses are extending mobility to customers in order to enable highly efficient self-service operating models. Enterprises must also deal with the rise of a new breed of data-hungry IoT devices. How can CISOs ensure security for all of these new access points without inhibiting mobile adoption?



With the ever increasing number of access points, security becomes more complex to manage.

Current-State Security Limits Mobile App Adoption

Until now, securing access to sensitive data was dependent on securing the device, typically with an app container. There are many drawbacks to this approach. First, apps must be coded to work within the container, which adds cost and deployment friction. Second, these approaches require the installation of an agent on the device, so they don't easily extend to BYOD or new-generation devices. Finally, users must deal with constant authentication friction and invasion of privacy. Perhaps this inconvenience and lack of privacy is why nearly two-thirds of users silently abandon enterprise apps. These controls are time-intensive to deploy and require hours of custom coding on the part of app developers and ISVs. What's more, current mobile security solutions can't offer the flexibility needed to access trusted data sources that reside both on-premises and in the cloud, hampering enterprise cloud adoption.

BYOD accounts for 80% of the 1.62B mobile devices in use in the workplace[1]

Businesses and organizations can only gain the true efficiency and productivity benefits of mobility if the apps are secure, easy to use and accessible from any device. To get there, we'll need to evolve our thinking around mobile security. We need a new model that secures access to data, while it encourages mobile app adoption across a wide range of new users and device types.

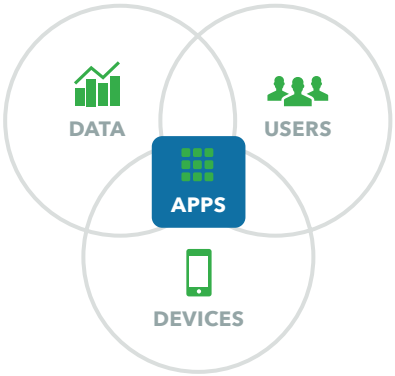
Nearly 65% of enterprise apps get deleted or are under-utilized[2]

The Mobile App is the New Point of Control

With industry experts projecting that more than 75% of mobile devices will be unmanaged by 2020[3], and another 20 billion IoT devices will be in use by then[4], the days of device-level control are over. Enterprise professionals need to devise a new strategy for providing secure access to their high-value data that does not place an unrealistic burden on users or compromise their privacy. The answer lies in app-level control.

The app sits at the intersection of devices, users and data.

By enforcing security policy at the app level, enterprises can maintain granular control over sensitive data, regardless of the user or device that's accessing it.

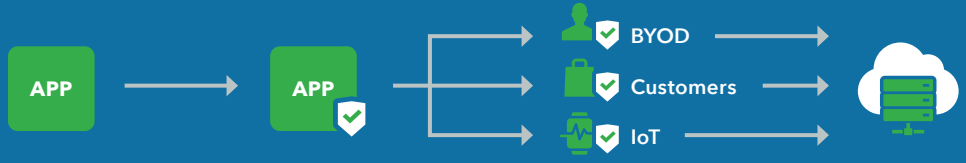


By eliminating the need to deploy containers or develop to specific container SDKs, app-level security simplifies the critical task of securing the data itself and extends the reach of mobile app security to any device type. By selectively extending security to only the apps that require it, enterprises can eliminate the friction and privacy intrusions that cause users to abandon enterprise apps in the first place. Once security controls are tied to the app, only then can enterprises realize the full promise and productivity of mobility for any user or device type.

Blue Cedar: Mobile App Security That's Easy and Everywhere

With Blue Cedar's patented, agent-less technology, you can apply granular security policies to any app on any device, simply and without compromising usability or user privacy. We do this by **injecting** security code deep inside the app either pre or post-compilation—with no coding required.

Easily enforce consistent policies across all your apps, users, and devices.



Your App
- Native, web, hybrid
- ISV or home-grown

Inject
Injection of Blue Cedar embedded security

Enforce
Your secured app, deployed via enterprise or public apps stores

Connect
Your data location, on-premise or cloud

KEY BENEFITS
- **Easy to adopt**
  Transparent and non-invasive to privacy
- **Easy to deploy**
  Any device, any user
- **Easy to manage**
  Low cost of change, use existing SDLC

The Blue Cedar embedded code then **enforces** app-specific policies that keep data safe. For example, Blue Cedar encrypts data-at-rest with cryptography that is FIPS 140-2 Level 1 certified. It protects against data exfiltration by dictating how data can be shared or used, including prevention of cut/copy/paste actions. It even safeguards against running the app on a device that may be vulnerable or compromised. These secured apps can then be easily deployed to users through either public or enterprise app stores.

Any data flowing over the network is encrypted in transit by establishing per-app microtunnels to the Blue Cedar gateway, allowing apps to **connect** securely to trusted back-end resources either on-premises or in the cloud, without significant architectural change. These layer 3 microtunnels ensure that the connection between the app and the data is secure and critical infrastructure is not exposed to the public network. It all adds up to significant benefits for security staff, end users and your extended enterprise. Most of all, the Blue Cedar solution fuels broad adoption of mobility even as it secures high-value data.

It's a solution that will keep all of your stakeholders happy.

Users

"Easy to use and protects my privacy."

Head of Mobility

"Encourages adoption so we realize the benefits of mobility faster."

Architect

"Flexible enough to support our route to cloud and next- gen endpoints."

CISO

"Consistent security policy across all users and device types. Less expensive and complex to manage."

[1] Invasion of the Mobile Monster, Rapid7, https://www.rapid7.com/resources/invasion-of-the-mobile-monster/

[2] Enterprise Mobility: User Adoption Is Key to Success, Business 2 Community, http://www.business2community.com/strategy enterprise-mobility-user-adoption-key-success-01224809#AXz87O0bitRKBYf2.97

[3] 451Research

[4] Forecast: Internet of Things – Endpoints and Associated Services, Worldwide, 2016, Gartner, http://www.gartner.com/newsroom/id/3598917

ABOUT BLUE CEDAR

Blue Cedar is a leading provider of enterprise mobile security solutions. Unlike traditional solutions that secure mobile devices, Blue Cedar uses a patented injectable technology to secure the mobile app itself. This approach delivers better, more granular security for any device, without impacting user productivity or privacy. As a result, enterprises can easily and cost-effectively develop and deploy secure mobile apps to keep pace with the speed of business. Set your apps free with Blue Cedar.

+1 (415) 329-0401 20 California St, San Francisco California 94111 www.bluecedar.com

BLUE CEDAR