

## Mobile Application Management

The AirWatch® Mobile Application Management (MAM) solution addresses the challenge of acquiring, securing, distributing, and tracking mobile applications. Whether you utilize MAM with our Mobile Device Management (MDM) solution or as a stand-alone solution, you can easily manage internal, public and purchased apps across employee, corporate and shared devices from one console.



### Public Applications

AirWatch integrates with public app stores, like the Apple App Store, Microsoft Store and Google Play, making it easy to purchase applications for your employees. AirWatch integration with the Apple Volume Purchase Program (VPP) and with Apple custom B2B apps allows you to allocate and distribute redemption codes to users, confirm redemption and installation of apps, track purchase orders and monitor licenses, all from the AirWatch console.

### Internal Applications

#### Software Development Kit (SDK)

Embed AirWatch MDM features and functionality into your custom-built applications with the AirWatch Software Development Kit (SDK). Applications developed with our SDK can include user authentication, compromised status detection, certificate integration, geofencing, customizable settings, branding, analytics, logging and reporting.

#### App Wrapping

AirWatch App Wrapping™ secures and protects your existing internal applications. Simply wrap your application from the AirWatch console and AirWatch security features are added to your app.

### Application Security

AirWatch enables administrators to control which apps users install with whitelists, blacklists and app compliance policies. You can restrict access to pre-installed apps on a device, like Bluetooth or camera, and disable public app stores. Authenticate users before allowing them to view and download internal apps, encrypt data and prevent data backup. Prevent access to apps on compromised devices and automatically uninstall apps when a user un-enrolls.

### Enterprise App Catalog

With AirWatch, administrators can install, update and remove apps over-the-air. Enterprise App Catalog provides a central place for users to view, browse, search, install, update and rate public, internal, recommended and web applications. Authenticate users, customize app categories and make apps available based on user, device or group. AirWatch also allows you to deploy multiple versions of the same application to test new apps and versions.

### Tracking and Analytics

With the AirWatch console, you can track installed, whitelisted and blacklisted applications by device and user. AirWatch gives you visibility into installed apps, usage time and more by capturing application analytics, but without collecting private data from personal apps. You can also view application ratings and comments.

	Enterprise App Catalog	App Management with MDM	Advanced App Management with MDM
<b>Application Purchasing</b>			
Public app store integration	●	●	●
Volume Purchase Program integration	●	●	●
<b>Application Security</b>			
User authentication	●	●	●
Set whitelist, blacklist and required app list		●	●
Disable non-market app installation		●	●
Block app access for compromised devices		●	●
<b>Application Distribution</b>			
Support internal, public, purchased and web apps in the App Catalog	●	●	●
Install and update apps over-the-air	●	●	●
Remove managed apps		●	●
Install enterprise apps	●	●	●
Apply license key for purchased app	●	●	●
Silent removal of managed and public apps		●	●
Application versioning	●	●	●
<b>Application Tracking</b>			
View installed apps	●	●	●
View application versions	●	●	●
View application status	●	●	●
<b>User Experience</b>			
On-demand app installation	●	●	●
Rate and review applications	●	●	●
View installed blacklisted apps		●	●
View available updates	●	●	●
View app descriptions	●	●	●
Search apps by name and category	●	●	●
<b>Software Development Kit (SDK)</b>			
User authentication			●
Require passcode			●
Compromised device detection			●
Certificate integration			●
Geofencing			●
Logging and analytics			●
Branding			●
<b>App Wrapping™</b>			
User authentication			●
Restrictions			●
VPN			●