Mobile Application Management (MAM) Whitepaper

Providing enterprises an extra layer of control with AirWatch v7.0

Contents

airwatch®

Catering to the Enterprise App Management Needs

Most of the enterprises across industries have realized and made corporate-liable mobile devices an important IT initiative. Today, organizations and their employees demand mobile applications to connect them to enterprise resources to increase their business efficiency, productivity, competitiveness, and to promote collaboration with their colleagues.

However, due to proliferation of mobile devices, there is a need to secure sensitive enterprise data. Ensuring the delivery of enterprise mobile applications to the end users in a secure fashion with adequate compliance is also very important. This is because the applications have become the sources of corporate security vulnerabilities due to poor data storage, lack of encryption, unauthorized access, and data leakage during data synchronization.

AirWatch, the leader of enterprise mobility, offers simplified **Mobile Application Management (MAM)** solution by distributing, securing, and tracking mobile applications. Easily manage internal, public, and purchased applications across corporate-owned, corporate-shared, and employee-owned devices from one central console. AirWatch also offers flexible MAM options for enterprises with a Bring Your Own Devices (BYOD) program. In addition, AirWatch's MAM solution helps IT overcome the following business challenges:

- When different applications are required depending on employee roles and device types

- To ensure employees have the latest application versions

- To ensure device compliance with organization security regulations

- To separate corporate and personal applications on the device

- To define employee privacy policies for application use

AirWatch not only overtakes the mentioned challenges, but also provides several benefits which are explained in the rest of the document.

Benefits of AirWatch

AirWatch and its simplified MAM solution enable the enterprises to enjoy the ultimate benefits of mobile application management. Some of the key features and benefits of using AirWatch MAM solution are:

- Increased employee productivity and satisfaction

- Centralized web-based console to manage applications

- Simplified application distribution process

- Increased maintenance by automatic updates and crash reports

- Increased data security by reducing the risk of sensitive data leakage

- Ease of users' feedbacks and ratings

- Increased collaboration among users and departments

- Secured support for Bring Your Own Device (BYOD)

- Increased application performance and scalability

- Application Version Management and performance monitoring

- Robust reporting on application inventory and usage

AirWatch's Mobile Application Lifecycle Management

AirWatch MAM enables enterprises a platform to manage the entire lifecycle of applications from deployment to retirement. The lifecycle management begins right from purchasing the applications (including public, purchased, and enterprise mobile applications), to securing, distributing, updating, and tracking the application deployment. AirWatch Mobile Application lifecycle management includes:

- Automating application deployment

- Internal application integration with Enterprise Resources through SDK and App Wrapping

- Streamlined workflow for developing, reviewing, assigning, and deploying internal applications

- Ease of providing applications to a beta group for testing and validation

- Enterprise App store supporting VPP and B2B

- Integrating with public application stores such as Apple and Google Play store

- Creating and enforcing groups for blacklisted, whitelisted, and required applications

- Setting access control for applications

- Performing selective wiping of applications and their associated data

airwatch

AirWatch's Flexible App Lifecycle Management

Developing Internal Applications

For those enterprises which are looking for custom built internal applications; AirWatch offers a Software Development Kit (SDK). The AirWatch SDK enables you to take advantage of the advanced AirWatch security features by embedding AirWatch MDM features and functionality into your custom-built applications. Applications developed with our SDK can include but are not limited to user authentication, compromised status detection, certificate integration, geo-fencing, customizable settings, branding, analytics, logging and reporting.
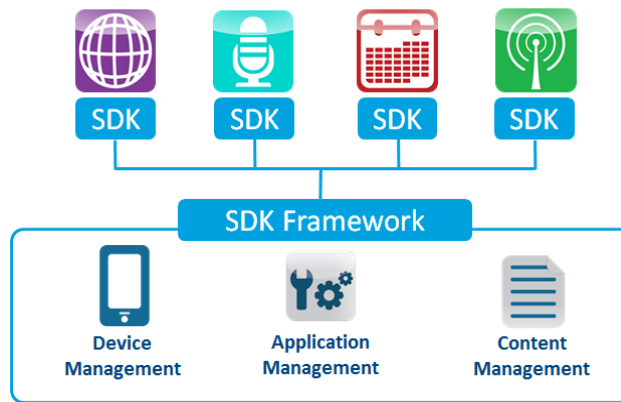
Figure1: Integrating AirWatch features into custom-built applications

App Wrapping

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

| Start with a developed internal app | Wrap your app from the AirWatch Console | AirWatch security features are added to your app | Deploy your application to mobile devices |

Figure2: Securing enterprise Applications with Wrapping

Shared SDK Profile Options

AirWatch can apply its SDK functionality not only to your custom applications but also to other AirWatch applications including AirWatch App Wrapped applications, the AirWatch Browser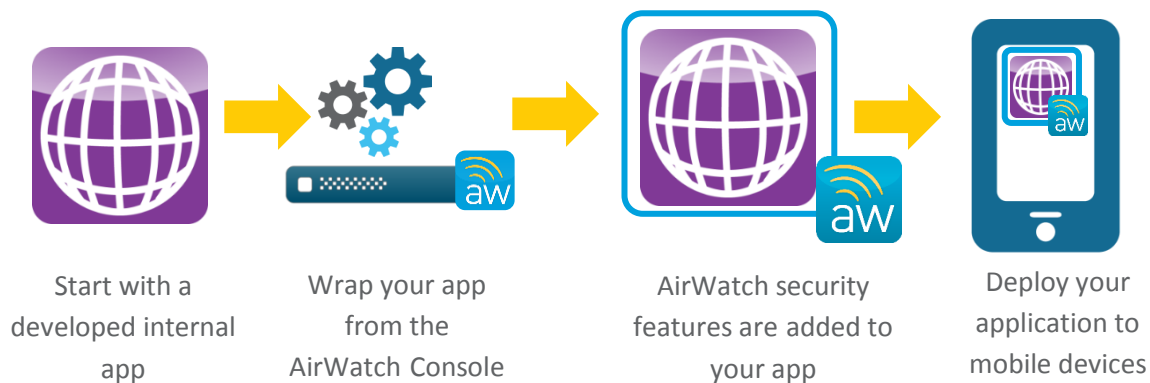, and the AirWatch Secure Content Locker. Choose to apply SDK profile settings and policies across an Organization Group (OG) or customize SDK profiles for SDK, App Wrapped, and other applications. If sharing SDK profile settings, control and maintain functions such as Single Sign-On, App Tunneling, Authentication and Data Loss Prevention from a single location.

Public Applications

AirWatch integrates with public app stores, such as 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 applications allows you to allocate and distribute redemption codes to users, confirm redemption and installation of applications, track purchase orders and monitor licenses, all from the AirWatch Admin Console.

Deploying Applications

The AirWatch MAM solution allows enterprise administrators to distribute, install, update and remove managed applications over-the-air. Using AirWatch, organizations can:

- Deploy multiple versions of the same application (including beta)
- Assign different versions of applications to different groups/devices
- Allow devices to 'roll back' to a previous version of the application
- Send direct download links for applications
- Send custom messages to alert users of new and updated applications
- Recommend applications to users which are available in a central location

Enterprise App Store

With AirWatch, administrators can ease the mobile work in enterprise using Enterprise App Store/App Catalog by installing, updating, and removing the applications over-the-air. Enterprise App Catalog is the vital location where employees find approved or recommended applications. It is the place to view, browse, search, install, update and rate public, internal, recommended and web applications. Authenticate users and customize application categories. Make applications available based on user, device or group. AirWatch also allows you to deploy multiple versions of the same application to test new applications and versions. App Catalog integrates with public app stores and third-party file shares. Likewise, AirWatch also offers Book Catalog, where users can view, browse, search, and install public, internal, and purchased ibooks.

Sending Application Configurations (iOS)

Pre-configure managed applications and send them to iOS devices so that users do not have to manually configure specified values. Configure network environment settings or other parameters for end-users to make application deployment easier. Entering information once in the AirWatch Admin Console can reduce the potential for wrong entries and reduce application deployment time.

Managing Applications

With the aid of AirWatch MAM solution, enterprises can manage applications by enforcing device policies over-the-air throughout the mobile fleet.

Mobile Application Compliance and Enforcement

With AirWatch, enterprises can set security and compliance policies and enforce the policies to the devices. The compliance policies ensure the devices are compliant with the company security regulations and help to prevent data leakage.

Using AirWatch Compliance policies, enterprises can enforce the below rules when the device is non-compliant:

- Blacklist and whitelist required applications

- Limit native applications on the device

- Restrict device access for jailbroken or rooted devices

- Block email access, restrict network resources, and perform a remote wipe

- View security and compliance history in graphical representation

- Enable a secure app tunnel connection to corporate resources

Reputation Analysis (for Android)

Use the AirWatch App Reputation Cloud Service to scan applications with the Reputation Analysis feature on applications for Android devices. The service scans applications for privacy and behavioral risks and reports potential vulnerabilities. Use scan results to decide to deploy or remove applications to protect you mobile. You can also use it as a central repository of scan results for your most commonly used applications.

Managing Feedback (iOS)

Application feedback can help end-users perform job duties as well as enrich their personal lives. Manage feedback for iOS applications from a central location in the AirWatch Admin Console so that end-users and Admins can review feedback and select helpful apps. AirWatch retrieves the feedback data from the device and lets you request, clear and view the data from the AirWatch Admin Console. Use feedback management to choose the most useful apps for the enterprise.

Securing Applications

AirWatch provides ultimate security to the applications with full operational and security management. With AirWatch, administrators can imply ultimate application security to the existing applications, create whitelist and blacklist applications, and enforce device compliance policies. AirWatch can restrict the access to pre-installed applications on a device, such as Bluetooth or camera, as well as limit access to public app stores. Through AirWatch MAM, enterprises can prevent data loss through user authentication, data encryption and restricting data backup outside of the application. Additional security features can be added to existing applications using AirWatch App Wrapping

airwatch

functionality. Further, applications can be uninstalled automatically when user unenrolls or when device is compromised.

AirWatch's Additional MAM Functionalities

AirWatch App Dashboard

AirWatch MAM solution offers enterprises with application dashboard providing a quick overview of all internal, public, and purchased applications deployed to the devices. Dashboards also give administrators the visibility into the number of users including:

- Application inventory
- Application version
- Workflow Status
- Ratings
- Number of applications installed on the device
- Number of applications assigned to the device

Feedback and User Ratings

With AirWatch App Catalog, end users can rate and review internal, public, and purchased applications. Comments and ratings are visible to other users and administrators in the App Catalog. When an application crashes, AirWatch captures the crash log and automatically sends it to the application developers for detailed diagnosis (requires the AirWatch SDK).

Terms of Use

AirWatch enables enterprises to require users to accept a Terms of Use agreement before granting access to the App Catalog as well as individual internal and public applications. End users are notified about what data administrators have access to and their Terms of Use acceptance is recorded with a time stamp.

Support for Apple Volume Purchase Program (VPP)

AirWatch integration with Apple VPP enables enterprises to purchase publically available applications, iBooks, custom B2B applications, and some specifically developed third-party applications in bulk using Apple VPP Portal. Integration with VPP allows administrators to easily distribute redemption codes and for new Apple OS versions to specific users and devices with little end-user interaction.

Monitoring and Tracking

AirWatch enables enterprises to enable and disable native or restricted applications and track applications and its data including:

- Name and description
- Version and change log

airwatch

- User ratings

- Number of users installed application

- Number of users assigned application

- Number of blacklisted and whitelisted applications

- Workflow status

Analytics and Reporting

Using AirWatch enhanced analytics and reporting feature, enterprises can:

- Create and export application reports

- View entire application inventory

- Track application version and update history

- Track application usage

Conclusion

This comprehensive set of mobile management solution from AirWatch helps enterprises deliver advanced mobile capabilities. AirWatch supports and protects wide variety of mobile devices across the organization. Thus, using AirWatch MAM, enterprises can utilize the advanced array of application development, distribution and management potentialities.

airwatch®