VMWARE AIRWATCH ANDROID IN THE ENTERPRISE

Put Android to Work with Separation of Work and Personal Apps

OVERVIEW

VMware AirWatch® Unified Endpoint Management (UEM) provides organizations a way to confidently enable, manage and secure Android in the enterprise.

KEY BENEFITS

- Separation of work and personal information at the operating system level
- Consistent and native user experience for both work and personal on the same device
- Easy delivery and access to work apps in a unified app catalog
- Protection of enterprise data with security policies

Why VMware AirWatch for Android

Android remains the world's most popular operating system, however, enterprises have been slower to adopt due to security concerns and fragmentation across device manufacturers. Android from Google separates work, personal apps and data to deliver standardized security and management capabilities for IT while maintaining a consistent native experience for end users, regardless of the device manufacturer.

The AirWatch Unified Endpoint Management platform delivers best-in-class architecture that is highly scalable, secure and flexible to meet your Android mobility initiatives across smartphones, tablets, laptops, rugged and peripheral devices. With AirWatch, leverage advanced security, management and productivity capabilities for Android devices. AirWatch provides comprehensive support for Android in the enterprise:

- Separation of work and personal data
- Enablement of productivity apps
- Data security and compliance

Separate Work and Personal

Allow end users to bring their own device (BYOD) to work while preserving the native Android user interface for a familiar user experience. Android separates data at the operating system level by enabling a work profile which creates a dedicated space for only work apps, away from the personal side of the device. Work applications are badged with an icon to signify that the application will only contain work data and end users can easily switch between work and personal apps in a simple click. Provide transparency and peace of mind for users that their personal apps are kept private and separate from the work data that's visible to IT.

Enrollment is simple and consistent across devices through the AirWatch Agent and the intuitive wizard enrollment flow. Admins are also able to bulk enroll devices using NFC technology which passes configurations from device to device with an easy tap.

Enable Business Apps

Give users the apps they need to be productive on Android devices. AirWatch enables administrators to deploy, manage and secure internal and public apps. Integration with Google Play enables approved applications to be accessible on Android devices. Easily configure key business apps like email, calendar and contacts, Gmail or VMware Boxer, and system apps like Chrome, Google Play, Google settings and Camera.

vmware® airwatch®

LEARN MORE

TRY

30-day Free Trial at
air-watch.com/free-trial

CALL
+1 404.478.7500

VISIT
airwatch.com

Distribute apps to user devices for automatic or on-demand install in a unified app catalog for web, native and remote apps with built-in single sign on (SSO). Administrators are able to define blacklists to block installation of unapproved applications and define required apps that are unable to be uninstalled from the device. Admins can track app inventory, versions and user compliance with app policies within the AirWatch console.

Keep Work Data Secure

Android provides comprehensive protection from the device hardware to the data being consumed. Devices in Android enterprise deployments use full device encryption and admin-managed policies to enable business and personal app separation and protection against malware. Data loss prevention policies prevent sharing of data between the personal side and work side of the device.

Configure restrictions to the work profile, including disable screen capture, camera, Bluetooth, USB file transfer and more. For a granular layer of application security, Android delivers a per-app FIPS 140-2 VPN to create a secure tunnel to internal resources. Passcodes and the ability to remotely lock or wipe enterprise data protects devices if they are ever lost or stolen.

For corporate-owned devices, Android can be deployed in a work managed mode which provides full device management. This enables further security capabilities such as preventing outgoing phone calls and SMS, installing or removing apps, factory reset, and restricting changes to Wi-Fi, Bluetooth and VPN.

vmware® airwatch®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com