airwatch®

We Simplify Enterprise Mobility™

Bring Your Own Device (BYOD)

A recent study conducted by an AirWatch partner found that 40 percent of workers use personal devices to access business applications and resources. With the consumerization of enterprise mobility, many enterprises are turning to “Bring Your Own Device” (BYOD) models or a hybrid of corporate and employee-owned programs.

By implementing a BYOD program, or a hybrid of corporate- and employee-owned programs, enterprises can allow employees access to corporate resources and ensure that their data is protected and secure. AirWatch provides unprecedented choices over the types of devices you deploy and the device ownership models, without compromising the security and management of your mobile fleet. AirWatch provides a flexible model for asset management, policy enforcement and distribution of profiles and apps based on device ownership.

Enable Device Choice

AirWatch supports all major mobile platforms, allowing you to implement a flexible BYOD program. Allow your employees to choose from the latest makes and models for their smartphones, tablets and laptops. Control the devices that are able to enroll in your environment with device whitelists and blacklists.

Enroll Devices Easily

With AirWatch, your employees can easily enroll their employee-owned devices without help from IT. Users designate the device as employee-owned, and all users are authenticated via AD/LDAP integration. Profiles, applications and content configure automatically based on the user and device ownership type. Limit the number of employee-owned devices enrolled by setting a maximum number of devices allowed per user. Enable employee-owned devices with access to corporate email, VPN and Wi-Fi networks.

Mitigate Business Risks

AirWatch allows you to avoid the business risks that are presented when employee-owned devices are allowed access to corporate content. Customize a Terms of Use agreement to inform users about the data that will be captured and what they are allowed to do with the device, and require users to accept when they enroll a device. Track who has agreed to the Terms of Use, generate reports on compliance, support multi-lingual agreements and update the Terms of Use agreement at any time. Assign and enforce agreements based on user role, ownership type, device platform and group membership.

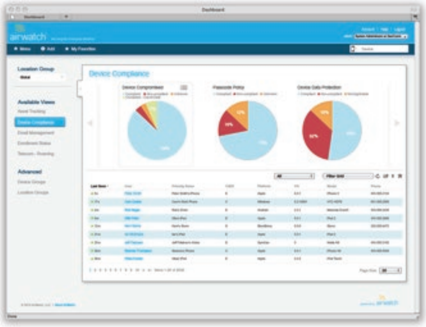
Protect Employee Privacy

With AirWatch, you can separate corporate and personal data on devices and customize privacy policies based on device ownership. Configure policies so that data is not collected from personal email, content or applications on an employee-owned device. Use policies to prevent collection of GPS location, personal user information and telecom data.

+1.404.478.7500 | sales@air-watch.com | air-watch.com

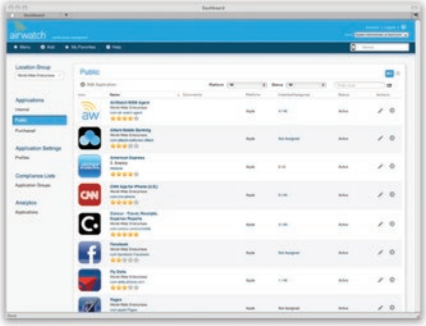
Manage Personal Devices

Device Management



With AirWatch, you can manage all enrolled devices from a central location in the AirWatch console. Profiles can be configured to give users access to corporate email, Wi-Fi, VPN and more. Users are authenticated during enrollment, and devices are automatically configured with profiles, apps and content based on the user's organization group. Administrators can track compliance and view real-time information for enrolled devices via the interactive dashboards in the AirWatch console.

App Management



AirWatch integrates with public app stores and Apple's Volume Purchase Program (VPP), making it easy to purchase apps for your users. For internal apps, you can embed AirWatch security features into your applications with our Software Development Kit (SDK) and app wrapping capabilities. Our Enterprise App Catalog allows you to distribute apps and provides users with a central place to view, browse, search, install, update and rate public, internal, recommended and web applications.

Content Management

AirWatch offers flexible content storage, either in the cloud or on-premise and supports Microsoft Office, iWork, image, audio, video and other files. AirWatch allows users anytime access to corporate content with Secure Content Locker™. Both content repository integration and manual uploading are supported, and users can quickly search using keywords or browse content through smart views, folders and categories. Users can view, edit, email and print files from Secure Content Locker and save files for offline viewing.

Enable Self-service Management

AirWatch empowers your employees and reduces the burden on IT with our self-service portal. From the portal, employees can enroll additional devices, view detailed device information and perform remote actions. Users can see installed profiles, applications and GPS locations, query the device and clear passcodes. Users can also make requests for apps, profiles and technical support through the portal.