VMWARE AIRWATCH BRING YOUR OWN DEVICE (BYOD)

Separate and Protect Corporate Data on Employee-Owned Devices

AT A GLANCE

VMware AirWatch® provides organizations deploying BYOD programs with flexible mobile application management (MAM) solutions that enable employee access to corporate resources while protecting sensitive corporate data.

KEY BENEFITS

- Protect corporate information by separating work and personal apps and data
- Give users access to critical business apps through a single catalog across any device
- Leverage MAM-only frameworks for BYO devices without managing the device
- Drive adoption with customizable BYOD program communication assets

LEARN MORE

END USER EDUCATION

Send end users to www.whatisworkspaceone.com for a clear understanding of AirWatch from the end-user perspective, focusing on separation of data and the benefits of our productivity apps.

Why VMware Workspace ONE for BYOD

Work Data Separation | User Productivity | Privacy First

The consumerization of mobility is leading many enterprises to turn to Bring Your Own Device (BYOD) programs to enable employees to use personal devices for both business and work purposes. Employees prefer to choose the device they work from so they can be productive anytime, anywhere. Although BYOD can significantly help organizations reduce costs, it could prove to be very expensive if the program is not securely implemented, as mobile apps can contain sensitive company data.

VMware Workspace™ ONE™, powered by AirWatch, provides organizations a comprehensive platform to create productive mobile work environments for employees while protecting sensitive corporate information and keeping it isolated from personal apps and data. Workspace ONE enables IT to only manage the work apps and data with mobile application management (MAM) frameworks, and not the full device, or mobile device management (MDM). Work apps and data are kept completely separate from personal apps and data, and privacy tools within Workspace ONE provide controls to enforce corporate privacy policies. End users are able to easily access all their work apps – native, web, remote – in a single application catalog that is secured and managed by IT.

Separate and Protect Work Data

A company's biggest challenge when deploying a BYOD program is to protect sensitive corporate data accessed from a personally-owned device. With mobile application management, AirWatch enables containment of work and personal apps and data and prevents the flow of data between the two. Work apps and data are securely encrypted and containerized, and admins can easily remove only the work data if the device is compromised, leaving the user's personal apps and data intact.

AirWatch provides flexible MAM options for organizations looking to deploy a BYOD program: standalone MAM containers and OS-level MAM. With AirWatch standalone MAM, companies can deploy a proprietary container to secure and protect enterprise apps with data loss prevention (DLP) policies built directly into the apps. Standalone MAM requires the app to be built with the VMware AirWatch® Software Development Kit™ (SDK) or app wrapping technology.

To expand standalone MAM to third party apps that may not have an SDK, turn on native, operating system level MAM on the device with a workspace profile. A workspace profile is activated through an adaptive management workflow on a user's device when accessing apps in Workspace ONE that require additional security policies. Activation of this profile provides a MAM-only approach, as opposed to MDM, that does not allow IT to track or report BYO-sensitive information.

vmware airwatch

DOWNLOAD

The campaign kit assets are available and ready to use today within myAirWatch.

Other solutions in the market enable BYOD through MDM or using standalone MAM using proprietary SDKs or application wrapping. The challenge with these approaches is they either have privacy implications or only work with a limited set of business apps – limiting user productivity outside of those apps. With Workspace ONE and OS-level MAM solution, these concerns and barriers are removed to enable BYO users access to any work app while maintaining autonomy with app-only management.

Increase User Productivity

Productivity is a major benefit of BYOD enjoyed by both the company and the end user, and it starts with being able to easily access the right apps.

Workspace ONE combines identity and mobility management to provide frictionless and secure access to all the apps and data employees need to work, wherever, whenever and from whatever device they choose – all from a single enterprise app catalog. With Workspace ONE:

- Enable BYO users with easy self-service onboarding workflows
- Eliminate password complexity with built-in single sign on (SSO) across apps
- Deliver any app – native, web, remote – to users in a single catalog
- Enable in-the-moment user productivity with email, browser and content apps
- Secure corporate data with contextual user and device-based policies

Drive Adoption and Engage End Users

A BYOD program is only successful if your employees use it. AirWatch has developed several tools for building trust and driving participation in the program, as well as techniques to spark everyday engagement in the valuable IT services offered through the AirWatch platform.

Self-Service User Experience

For end users to adopt any IT service, it has to be easy and provide value to their productivity. Workspace ONE makes it easy for users to self-service onboard to quickly gain access to work apps through a unified catalog. Built-in SSO eliminates the need for complicated logins and passwords. The ability for users to have self-service access to work apps helps to reduce the amount of help desk tickets as they can easily get to the work apps they need.

Put End User Privacy First

The AirWatch industry-first mobile privacy initiative provides tools for enterprises to address end user privacy concerns that can be a barrier to adoption. The AirWatch platform is built on the notion of “privacy by design” to help organizations safeguard company data and implement tools to enforce company privacy policies on devices.

WhatIsWorkspaceONE.com is a public site designed to educate end users on the benefits of mobile app management and addresses some of the commonly asked end user questions about EMM.

Our built-in **privacy app** is dynamically-generated to end users' devices, and shows in very simple terms what their company-specific policy is regarding personal stuff such as texts, emails, photos, apps, location and roaming.

The AirWatch console allows IT to assign a **privacy officer role**, which gives an individual or small group the exclusive privilege to manage user privacy settings. Separating the privacy settings by policy within IT allows for better checks and balances, and helps provide an additional layer of security over corporate privacy controls.

Drive Adoption with a Customizable Toolkit

To help educate end users and promote the program, AirWatch offers a turnkey BYOD adoption kit. This "campaign-in-a-box" includes best practices and pre-produced assets designed to speak to the productivity, privacy and accessibility benefits with targeted messaging that will resonate with end users. The kit contains videos, email templates, posters and table tents, presentations, FAQs, and more, ready to be used as-is or customized with an organization's own policies, logo and branding.

Push Messages and Notifications

Keep employees engaged and informed of the latest apps and information. Push relevant and contextual messages, offers and alerts to employee-owned devices form the AirWatch console via text, email or pop-up notifications. Leverage the AirWatch custom messaging framework to tailor system messages to suggest new apps based on user roles and profiles or remind users to update existing apps.

vmware airwatch

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

9/16