VMWARE AIRWATCH PRIVACY FIRST PROGRAM

Protecting End User Privacy at Every Level

AT A GLANCE

VMware AirWatch award-winning Privacy First Program is changing the way companies and their employees think about privacy and security by establishing trust through technology architecture, programs and end user education.

KEY BENEFITS

- Provides access with the least amount of device management
- Establishes and builds trust through transparency and education
- Ensures that personal devices leverage a clear separation of work and personal data
- Delivers the best user experience by hooking into the native controls of the OS
- Empowers the end user with choice
- Allows IT to protect corporate data without invading end user privacy

AWARD WINNING PROGRAM

END USER EDUCATION

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

Extensible, Built-in Privacy Framework

App-Level Security | Admin Privacy Settings | End User Control | Educational Tools

Today, people are working in a blended environment, with access to both work and personal apps and data from all of their mobile devices, regardless of ownership. While mobile platforms are providing more robust privacy controls at the OS level, they are still not enough to fully protect the end user. It is crucial that enterprises have a security model that incorporates an intuitive privacy control framework.

VMware AirWatch® puts privacy first by providing an architecture that enables a more granular approach to filtering data to protect end user privacy. Through our "privacy by design" model, we have built safeguards and functionality right into the framework of our solutions, allowing us to deliver the most features while preventing IT from accidently over-managing a device.

Why Privacy by Design?

Privacy by Design is the philosophy of building privacy into the design, operation and management of IT systems, networks and business processes from the outset. It minimizes risk of privacy infractions, security breaches and associated reputational impacts. It also treats privacy as a competitive advantage to earning customer loyalty and trust, while enabling wider adoption of new technologies. AirWatch has woven this philosophy into every aspect of our solution:

- Ensuring complete separation between work and personal apps
- Providing privacy features and controls at the admin level
- Providing transparency and choice for end users
- Delivering educational tools to garner trust and support adoption

App-Level Security Separates Work and Personal Data

App containerization has risen to the top of the list as the best way to ensure that IT can access and manage only work-related apps and settings, safeguarding end-user privacy by making personal apps and data inaccessible. At the same time, BYOD owners remain fully in charge of their device, personal apps and data.

- Keep work and personal apps separate and restrict flow of information between them
- Install only IT-approved, authorized apps in the corporate container
- Detect jailbroken or rooted devices and take compliance action to protect company data
- Take advantage of data loss prevention (DLP) and privacy features offered within the OS itself, such as limiting lock screen data

Built-In Admin Controls Protect Privacy

The AirWatch admin console itself contains embedded privacy features that help enterprises deliver the most accessibility without being intrusive to the end user.

- Enables customizable privacy educational notices for user device activation, app downloads and policy updates to answer common privacy concerns
- Provides remote file storage for countries with data residency laws
- Enables anonymized API calls to de-identify and generalize app lists
- Assigns a Privacy Officer role to ensure that only those authorized can access and edit privacy policies

End User Transparency and Visibility

AirWatch puts privacy first by providing transparency, access and choice to end users, and delivers the best user experience by hooking into the native configuration controls of the operating system. AirWatch actively practices respect for user privacy by putting the end user in control with:

- Visual warnings or cues when a profile is activated or an action is taken on the device
- Ability to delete any data that has previously been collected
- Ability to delete apps, including management profiles that have been placed on their device
- Privacy is the default setting—no action is required by the end user to opt-in to protection.

Educational Tools Build Trust

While IT understands what can and cannot be tracked on a personal device, employees often mistakenly think of the software as spyware, which can hurt user adoption and hinder the transformation to a mobile workstyle. The AirWatch privacy initiative provides tools for enterprises to educate users on concerns that can be a barrier to adoption.

WhatisWorkspaceONE.com

VMware Workspace ONE™ is a solution that gives users secure access to all the apps and data they need to work wherever, whenever and from whatever device they choose. To help educate users about this solution, we have created WhatisWorkspaceONE.com, a public website designed to address privacy concerns and answer questions they may have about downloading VMware Workspace ONE onto their personal device. End-users can watch a video that shows exactly what IT can and can't see from the console, dispelling the "big brother" myth.

Privacy App

AirWatch deploys a dynamically-generated privacy app to end users' devices that shows exactly what their company policy is regarding personal features such as texts, emails, photos, apps, location and phone calls. The app gives the user specific, real-time information about what IT can and cannot access on their device, and is accessible at any time with a single tap.

vmware® airwatch®

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