airwatch® by vmware®

Secure Government Mobility

Mobility is changing how government agencies operate inside and outside of agency walls. Civilian federal agencies are looking to mobile to transform the workplace while high defense organizations are concerned with mobile device security. Implementing a secure mobility strategy enables government officials to reinforce productivity, efficiency and responsiveness while maintaining compliance with industry regulations.

AirWatch® by VMware® enables government agencies, civilian and defense, to secure critical data and information while ensuring employees have access to the content, apps and resources they need to perform their jobs. AirWatch® Mobile Device Management Software 6.5 Security Technical Implementation Guide (STIG) Version 1 has been approved by the Defense Information Systems Agency's (DISA) Field Service Operations division. This certification validates that AirWatch meets security requirements for installation on Department of Defense (DOD) networks. AirWatch also meets Federal Information Processing Standard (FIPS) Publication 140-2 compliance standards to ensure confidential data is protected.

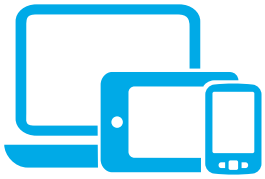
About AirWatch by VMware

AirWatch by VMware is the leader in government mobility management, with more than 14,000 global customers. The AirWatch platform includes industry-leading mobile device, email, application, content and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at www.air-watch.com.

+1 404.478.7500 | sales@air-watch.com | air-watch.com

airwatch by vmware

Comprehensive Government Mobility Management



Manage the Device

Manage the Workspace

Apps

Content

Email

Browsing

Every Mobile Device

Phones & Tablets

Laptops

Rugged Devices

Printers & Peripherals

Every Mobile Platform

Every Mobile Deployment

Corporate Multiuser

BYOD

Line of Business

How We Are Different

- Manage multiple operating systems, device types and mobile deployments from a single admin console
- Prevent unauthorized devices from entering mobile environment with strict enrollment policies and security
- Manage devices by geographic function, role and location with strict role based access controls
- Secure and track devices with FIPS 140-2 validated modules and automated compliance engine
- Meet security requirements for installation on DOD networks with AirWatch STIG approval
- Enforce strict security settings specific to employee function with highly scalable, multitenant architecture
- Secure management and distribution of internal and public apps available to employees for official use
- Maximize data loss prevention and secure content collaboration with AirWatch® Secure Content Locker®
- Encrypt, secure and containerize email with AirWatch® Inbox as an alternative to native email clients on devices

+1 404.478.7500 | sales@air-watch.com | air-watch.com