SECURELY MOBILIZE AND MODERNIZE GOVERNMENT IT TO ADVANCE MISSION OUTCOMES

MANAGE USERS AND SECURE DATA ACROSS ANY ENDPOINT—INCLUDING DESKTOPS

VMware AirWatch® Unified Endpoint Management combines traditional desktop management with a modern enterprise mobility management (EMM) framework to manage users and data across any endpoint and application from a single platform

- Support major mobile operating systems including Android, iOS, QNX, Tizen, Windows CE, Windows 10, and frameworks like Android for Work and Samsung Knox
- Manage the full lifecycle of macOS and Windows desktop and laptop devices alongside mobile and rugged devices
- Manage the full lifecycle for all endpoints from on-boarding to retirement, including deploying security patches, remediating vulnerabilities, installing software and consolidating processes across devices on and off the domain
- Protect data through device restrictions, multi-factor authentication, FIPS 140-2 inside validation, CAC and PIV card integration, AES 256-bit encryption, advanced data loss prevention (DLP) policies and remote lock or wipe
- Enforce conditional access policies based on identity, authentication strength, data sensitivity, user location, device compliance and more
- Revoke access automatically if compliance policies are violated
- Prevent unknown devices from connecting to corporate networks and configure certificate-based access to corporate VPN and Wi-Fi networks

The Secure Digital Workspace for Government by VMware

As the world's processes and workflows become more mobile, governments are competing with the desire to enable remote access to internal resources against the realities of managing sensitive data across disparate mobile devices, applications, identities and networks. Agencies should not have to compromise service delivery in exchange for security and with VMware AirWatch®, they don't have to. As part of the industry's most comprehensive end-user computing portfolio across infrastructure, apps, devices and identity, AirWatch enables federal, state and local government agencies—from defense to civilian—to securely take advantage of enterprise mobility while maintaining compliance with stringent national standards bodies.

Security from the Data Center to the Device

From identity-based conditional access to network micro-segmentation, VMware compliments your agency's mobile deployment with advanced security across the entire computing landscape.

VMware Identity Manager™ extends identity-based conditional access to web apps, virtual desktops, published applications, Windows packaged apps, native mobile apps and devices with full Active Directory integration and federation.

VMware AirWatch® App Tunnel™ provides a secure method for organizations to allow both internally built and public apps to access corporate resources residing in a secure internal network on a per-app basis.

VMware AirWatch® and NSX delivers security from the device to the data center with granular security policies and network enforcement across mobile applications and workloads.

VMware TrustPoint™ enables next-generation threat protection and remediation across endpoints and cloud services at unparalleled speed and scalability.

VMware AirWatch: Public Sector Ready

DISA STIG: Available for VMware AirWatch® 9.X Version 1
In partnership with the Defense Information Systems Agency (DISA), AirWatch has released a Security Technical Implementation Guide (STIG) for the AirWatch MDM Architecture and AirWatch MDM agent for version 9.X.

FedRAMP: AirWatch is an EMM FedRAMP Compliant System
AirWatch has been granted an Authority to Operate (ATO) by the Federal Risk and Authorization Management Program (FedRAMP) with an impact level of Moderate.

SUPERCHARGE SECURITY IN 5 STEPS WITH VMWARE AIRWATCH

1. Trust the User
Establish identity-based trust between the user, device and the enterprise

2. Manage the Endpoint
Protect information through advanced device security and DLP policies

3. Secure the App
Enable enterprise-grade security and control across applications

4. Safeguard the Data
Secure access to data from any device, any app and any network

5. Protect the Network
Configure certificate-based access to enterprise networks and allow both internal and public apps to access internal resources on a per-app basis

FIPS 140-2 Inside Validated: for AirWatch MDM architecture and VMware Boxer, Browser and Content Locker applications on iOS, Android and Windows 10 devices
AirWatch contracted Booz Allen Hamilton (a CMVP Certified Laboratory) to inspect and validate AirWatch source code for the MDM Architecture, iOS SDK, Android SDK, and Windows SDK. This SDK is utilized across VMware Boxer®, VMware Browser®, and VMware Content Locker® applications for encryption operations.

NIAP Common Criteria: AirWatch is "In Evaluation" for Mobile Device Management and MDM Agent Protection Profile version 2.0 for iOS
AirWatch expects to become a NIAP validated vendor and achieve a Commercial Solutions for Classified Listing (CSFC) for iOS 9.2 in early 2017.

CJIS: The AirWatch EMM platform aligns with NIST 800-53 revision 4 controls and supports Criminal Justice Information Services (CJIS) Security Policy version 5.5 requirements
VMware enlisted audit partner Coalfire Systems to test and evaluate VMware products and solutions against CJIS Security Policy requirements. The AirWatch EMM platform supports CJIS Security Policy 5.5 requirements, available as a set of reference architecture documents here.

NIST SP 800-157 Derived Credentials: Integration is available for MDM managed profiles for native mail clients, WiFi and VPN as well as VMware apps such as Boxer and Browser
AirWatch provides direct integration with various Certificate Authority (CA) vendors to generate and/or deliver a derived credential securely to the mobile device and/or mobile application that will utilize it. In addition, AirWatch is currently undergoing integration with Purebred which is utilized by the Department of Defense (DoD) as well as top tier commercial off the shelf (COTS) derived credential solutions such as Entrust Identity Guard and Intercede MyID.

NIST SP 800-163 App Vetting via AirWatch Mobile Security Alliance
800-163 defines the processes ensuring that mobile applications used in public sector are free from design vulnerabilities and that vulnerabilities cannot be inserted into the application throughout the application's lifecycle. Through the AirWatch Mobile Security Alliance (MSA), multiple AirWatch partners such as Lookout, Appthority and Zimperium are able to provide real-time application vetting and reputation scoring analysis, helping agencies comply with NIST SP 800-163.

FOR MORE INFORMATION ON AIRWATCH ENTERPRISE MOBILITY MANAGEMENT FOR GOVERNMENT, VISIT: www.air-watch.com/industries/federal-government

vmware® airwatch®

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