WINDOWS MANAGEMENT FOR THE MOBILE CLOUD ERA

Deploy, Manage and Secure Windows 10 with VMware AirWatch

OVERVIEW

AirWatch features a new – and more efficient – approach to Windows lifecycle management. The unified endpoint management platform introduces a full set of Windows 10 capabilities enabling OS deployment, application and updates distribution, and end-to-end security. By combining the requirements of traditional management and the modern enterprise mobility management (EMM) approaches, AirWatch reduces the costs and burden on your IT, and helps you smoothly transition to the most secure and productive Windows platform yet.

Why AirWatch for Windows 10

Traditional approaches to Windows management are costly, complex and restrictive. Provisioning devices requires time consuming rip-and-replace imaging. Management is largely driven by Group Policies (GPOs), done on-premises, and only possible for network or domain-joined PCs. Pre-Windows 10, major OS updates were less frequent, and feature and security patches were put through extensive compatibility testing. Users had little or no self-service capabilities (e.g. installing apps) – resulting in high-touch IT and higher support/help-desk costs.

Using VMware AirWatch® and Windows 10, a fundamentally different cloud-centric and mobile-centric approach to simplify management and security is possible. Windows 10 drastically simplifies the process of device enrollment on any network and across different use-cases without the need for imaging for individual use cases. The unified set of APIs across PCs, tablets, phones, and other Windows devices means IT can consolidate management tools and employees can access and perform self-service install from a custom company app store.

This evolved OS is forcing organizations to rethink traditional management practices, and instead adopt EMM as the standard management tool for any device running Windows 10. The industry leading EMM suite, AirWatch delivers a comprehensive set of capabilities and a low TCO, simpler and flexible approach across Windows:

- Device and OS lifecycle management
- Application management and delivery
- End-to-end security management

GET USERS UP AND RUNNING QUICKLY WITH ENHANCED PROVISIONING AND OS LIFECYCLE MANAGEMENT CAPABILITIES

Device and OS Lifecycle Management

Provision Devices | Configure Policies | Manage OS Updates

AirWatch provides an intuitive Windows 10 onboarding experience over a public or private network across corporate, BYOD, and COPE scenarios. End users can have an out-of-box enrollment experience, with zero IT involvement, on power ON or adding their work account to an existing Microsoft Office application. On enrollment, the device can be joined to a cloud-domain; correctly configured with profiles, settings, apps, compliance policies and content; and set up for AirWatch management. AirWatch enables you to create dynamic policies around how OS updates are managed and delivered across your organization. IT can flexibly deploy and/or defer OS updates and patches based on device priority, sensitivity, and desired maintenance windows. AirWatch fully integrates with an existing Windows Server Update Services (WSUS) or the new Windows Update for Business service and supports peer-to-peer delivery of updates to eliminate caching infrastructure.

skywire

vmware® airwatch®

DELIVER A UNIFIED AND SECURE APP MANAGEMENT, DISTRIBUTION, AND ACCESS EXPERIENCE ACROSS ALL APP TYPES.

Application Management and Delivery

One-Touch Access | App Delivery | App Inventory

With AirWatch, organizations no longer need multiple app distribution tools for each app type. IT can aggregate and distribute all app types – classic or modern (e.g. MSI, MST, MSP, EXE, APPX, APPV…) via a unified company store. Integration with VMware Identity Manager™ also ensures a consistent one-touch single sign-on (SSO) user experience across all Windows apps – including native, web, and remote. AirWatch fully integrates with the Microsoft Store and the new Business Store Portal to manage application delivery, licensing, and security. AirWatch supports auto provisioning workflows and multiple software distribution methods including remote installation of apps, drivers, firmware updates, and other custom scripts. IT gets full inventory control, collection, and reporting for Windows apps, including classic desktop (legacy Win32) apps and Metro (modern) apps. Also, IT administrators can create compliance policies with custom whitelists and blacklists that allow only apps from trusted publishers and locations to be installed or run on the device.

TAKE ENDPOINT AND DATA PROTECTION TO A NEW LEVEL WITH ADVANCED SECURITY FEATURES.

End-to-End Security Management

Establish User Trust | Ensure OS Health | Prevent Data Leakage

AirWatch integrates with Microsoft Passport for Work and Windows Hello so you can enable multi-factor authentication (MFA) for user verification, including biometric gestures. AirWatch compliance engine gives IT admins real-time visibility into device's health and image integrity (Windows Health Attestation). This allows you to provision conditional access controls such that only authorized users and compliant Windows 10 devices have access to enterprise resources. With AirWatch compliance engine, IT can also define automated escalation policies to notify users and/or perform remediation actions on devices. AirWatch prevents data leakage (DLP) by activating Windows Enterprise Data Protection (EDP) to protect sensitive work data from accidental or deliberate leaks. AirWatch, automatically tags company data from the cloud, network or company apps and enforces policies on the use of the data such as copy/paste controls, drag and drop prevention between work and personal apps and even encrypts corporate data file differently so they can only be accessed from approved work applications and devices.

For more information on AirWatch support for Windows 10, visit: www.air-watch.com/solutions/windows.

vmware® airwatch®

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