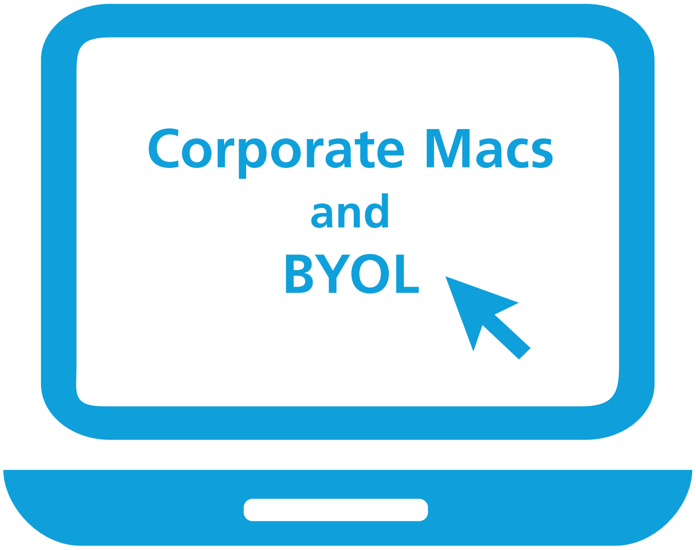
airwatch® by vmware®

Unified Laptop Management

Laptops have become an integral part of how people work, allowing users access to corporate content from any location. Traditional laptop management consisted of domain-joined management, leading to fragmentation and variations in management among different laptop platforms. Emerging new use cases such as bring your own laptop have also expanded the role of laptop management in the enterprise, changing how IT must manage these devices. The combination of multiple operating systems, management solutions and other mobile devices entering the enterprise has led to additional challenges for IT in ensuring these devices remain secure and monitored.



AirWatch® Laptop Management enables you to manage Chromebooks, Mac OS and Windows laptops alongside your smartphones and tablets in a single console. For IT, allow for quick configuration and automated software package distribution and workflows. With AirWatch, IT can view an inventory of connected laptops and provide support to end users through remote assistance and troubleshooting capabilities. For end users, AirWatch ensures that their laptops remain secure with multilayered endpoint protection. Users can enroll in AirWatch through a simplified enrollment process and gain access to AirWatch apps to enhance their productivity. End user privacy is protected with a complete separation of personal and corporate data for BYOL, and users have visibility and control of their devices with the self-service portal.

About AirWatch by VMware

AirWatch® by VMware® is the leader in enterprise mobility management, with a platform including 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

Unified Laptop Management

Configuration Management

Configure corporate resources for laptops and ensure secure connectivity to back-end systems with certificate authentication and per-app VPN. Manage configurations based on dynamic smart groups and leverage custom profile configurations to deploy managed preferences. Automatically connect end users to corporate resources such as Wi-Fi and VPN, and configure Exchange Web Services and Outlook accounts automatically.

Software Distribution

Install, update and remove software packages as well as provide scripting and file management tools. Create an automated workflow for software, apps, files, scripts and commands and configure installation during enrollment, on-demand or at a pre-defined time. With AirWatch, you can also set the package to install based on conditions, including network status or defined schedules, and deploy software updates automatically and notify the user when updates occur. Once deployed, view a log of successful installations and executions in the AirWatch console. Upload and deploy enterprise applications to laptops with defined app descriptions, images and categories for display in AirWatch® Catalog. For Macs, integrate with the Apple Volume Purchase Program for managed app distribution.

Asset Tracking

Monitor and track laptop inventory from a single console, and manage across organization groups with multitenancy and role-based controls. View detailed laptop and end user information, and record and export reports or console event logs. For Macs, integrate with AppleCare to request details like warranty status, purchase country and purchase date.

Remote Assistance

Provide support to your end users with remote assistance and troubleshooting. Send end users a push notification or lock the screen remotely. Perform a device query or remotely access file system logs to assist with troubleshooting. If a device is compromised, perform a remote device lock, enterprise wipe or full device wipe.

Endpoint Protection

Ensure security with a multi-layer approach to endpoint protection. Require a device passcode and certificates for authentication, and configure restrictions to prevent user actions on the device. Ensure protection against malicious attacks with automatic configuration of anti-virus and malware software. Full disk encryption ensures your corporate data is secure. Continuously monitor laptops for security issues with the AirWatch compliance engine.

User Enablement

Enable users with simplified self-enrollment and automatically configure laptops once they are enrolled. Provide complete separation of personal data for BYOL users. Allow users to share devices with multiuser support. Enhance productivity with AirWatch apps for laptops, including AirWatch® Agent, AirWatch Catalog, AirWatch® Content Locker, AirWatch® Inbox and AirWatch® Browser. Users can resolve common laptop issues through the AirWatch self-service portal. Users can also view details of all their enrolled devices, such as encryption status, installed profiles and apps, and compliance status.