BRING MAC TO THE ENTERPRISE WITH A MODERN APPROACH TO MANAGEMENT

Unified endpoint management brings together traditional client management with a modern enterprise mobility management framework.
Employees are used to working on whatever mobile devices they want. Even if a company provides phones and tablets, there is usually some freedom of choice for employees. But when it comes to laptops and desktops, employees typically don’t have the same freedom to choose. Windows rules in most enterprises, and employees who prefer Macs often aren’t officially supported.

However, this bias against Macs may be hurting businesses. Studies have shown that Macs can improve employee productivity and help lower costs for companies of all sizes.¹ Often, companies that let their employees choose between Macs and PCs find their Mac users are more productive. Peter Yared, while serving as CTO at CBS Interactive, told Network World that with Macs, “Employees are happier and that makes them more productive.”

The cost of ownership is less for Macs than PCs, researchers have said, because they require less IT support, don’t require imaging and have a longer shelf life. A survey by the Enterprise Desktop Alliance reported that 45% of IT managers who support both PCs and Macs say Mac has a lower total cost of ownership (TCO) than PCs and requires less troubleshooting time.² Furthermore, the survey found that employees who use Mac systems require less user training and help desk support than employees who use PCs.

Interestingly, if given the choice, many employees would opt to use Macs over PCs, according to a recent survey conducted by IDG TechPulse.¹ IT decision makers say 56% of users in their organizations would rather use Macs than PCs. The survey found that despite this, 80% of organizations are mostly using PCs.

¹ CAN PCs AND MACS COEXIST IN THE CORPORATE WORKPLACE?, IDG TechPulse Whitepaper
Mac Management Challenges

Historically in the enterprise, there have been barriers to Mac adoption that require a solution to overcome:

• Device deployment and configuration is very high touch for IT
• Remotely managing users’ devices is impossible unless they physically come on site
• Laptops must be domain-joined, leaving no flexibility for use cases beyond corporate-owned devices
• Critical apps users need to do their work may require Windows

Apple Innovations for Mac Management

In the keynote session at WWDC 2016, Apple’s Senior Vice President of Software Engineering Craig Federighi announced the new productivity features that would make macOS Sierra a big hit with enterprise users. Federighi also noted the new name for Mac OS X: macOS.

Apple has steadily rolled out features aimed squarely at the enterprise market in both iOS and macOS operating systems over the last few years. iOS is the leading platform for corporations embracing the post-PC era, with a reported 98% of companies recently surveyed currently supporting the platform. The latest Apple software updates, iOS 10 and macOS Sierra, introduce new features that simplify both enterprise use and management.

New continuity features enable users to switch freely between Apple devices. A universal clipboard for copy/paste between Apple devices as well as new auto unlock for Macs based on Apple Watch or iPhone proximity will make it easier to work between devices. And with desktop syncs between devices, users always have access to their latest work.

Device and OS convergence can also help simplify the management process for IT. Apple began aligning management profiles in Mac and iOS software years ago so that Macs could be managed alongside iOS devices with mobile device management (MDM). Each macOS update has delivered additional MDM controls, enabling IT to manage more endpoints together.

VMware AirWatch Delivers the Modern Approach to Mac Management

Following Apple’s introduction of new features, VMware AirWatch® has added enhancements to the Mac management capabilities, streamlining device management in a single console to help drive enterprise adoption. IT is beginning to see mobile devices and laptops (like Mac) as a single set of endpoints to secure, manage and enable with access to enterprise resources. This unified view of all devices will help IT departments streamline processes and prepare for the future.

AirWatch helps IT bring Mac into the enterprise with a unified endpoint management (UEM) platform that provides a holistic and user-centric approach to managing all endpoints. By bringing together traditional client management with a modern

3 Enterprise tablet adoption slowing, but Apple’s iOS still dominates corporate world http://appleinsider.com/articles/15/01/06/enterprise-tablet-adoption-slowing-but-apples-ios-still-dominates-corporate-world
enterprise mobility management (EMM) framework, AirWatch enables over-the-air configurations for quick deployment options, easy app delivery and end-to-end security.

Managing Macs like mobile devices means they can be configured without ever having to be domain-joined. This is a great benefit for global organizations, remote workers and companies who use contractors or freelancers, since it enables additional BYO use cases and device management options for contractors. Additionally, AirWatch can help IT implement a BYOD program and policies for Mac while also ensuring personal information remains private. A UEM platform provides IT with a consistent management experience for all device types and operating systems, enabling a single-pane-of-glass view of all endpoints in an enterprise.

Key AirWatch UEM Platform Features for Mac Management
As an Apple mobility partner, AirWatch is committed to supporting macOS and Apple programs for businesses and schools. As the industry leading EMM platform, AirWatch delivers a comprehensive set of capabilities for macOS management:

• Over-the-air deployment, configuration and management
• App delivery and OS updates
• Data security and compliance

By integrating real-time application delivery and AirWatch, IT can deliver any application to Mac computers, secure endpoints, and manage macOS alongside your other devices. With AirWatch, Mac notebooks can be deployed, configured and managed with zero touch from IT to eliminate imaging and staging services. Easy app delivery, OS updates and system integrations keep users productive. It enables users to deliver virtual legacy Windows apps to run on Mac. Configure settings for FileVault, Gatekeeper and more to keep devices secure. Integrate with Apple services like the Device Enrollment Program (DEP), Volume Purchase Program (VPP), Apple School Manager (ASM) and AppleCare to manage devices, apps and security.

Streamlined Deployments
Corporate-owned
Through integration with the Apple Device Enrollment Program (DEP), users can turn on a newly purchased Mac and have it enrolled automatically—eliminating any manual work for IT. Security policies and configurations are installed automatically over-the-air, based on configurations the administrator has previously set. IT doesn’t need to touch every Mac to setup the devices—everything is pre-configured using AirWatch, by group, device type, user or job function. AirWatch can silently add a hidden admin account in addition to the user account during setup, preserving admin rights for IT.
And with a feature called Await Configuration, AirWatch can hold the laptop in Setup Assistant until everything has been pushed and installed, enabling a user to access the device only when completely configured to the standard defined by IT.

BYOD
AirWatch also streamlines enrollment for Mac BYOD deployments where using the Device Enrollment Program isn’t possible. With web-based enrollment, users access a unique URL specific to their organization that will take them directly to an enrollment screen in Safari. Users will also need to know their ‘Group ID’ (which should be communicated by IT when sending out the URL) or corporate email address, and their
corporate credentials. The webpage can be customized with branding specific to
the organization so users will know they are in the right place. This enables users
to enroll any device at any time without interaction from their IT department.
Administrators can treat macOS devices just like they would mobile devices,
managing only corporate data and leaving end user privacy intact. Unlike
traditional domain-joined management systems, IT can ensure that no personal
information is collected.

Over-the-Air Configuration
Configuration management (or provisioning) enables IT to build a specific delivery
and installation flow that can include multiple files, apps and scripts. AirWatch
enables enterprises to provision custom products to distribute apps, create and
modify files, run scripts and perform commands—all delivered to Mac notebooks
together. Administrators can configure software update source, and execute
remote scripts and complex packages. Products can be configured to deploy
dynamically during enrollment or on demand. With a “set it and forget it
approach” for admins, the same configuration can be deployed in bulk to all
devices, with dynamic configurations based on directory service and domain
memberships. Administrators can also deliver software updates and security updates on
a defined schedule through relay servers so networks aren't overloaded, and take
advantage of day one support for the latest OS releases so users can access the
latest innovations immediately.

Real Time Application Delivery
Administrators can upload and deploy enterprise applications (native, web, SaaS,
App Store, purchased through VPP, internal, remote, virtualized) to laptops
through a central app catalog. IT can even deliver virtual legacy Windows apps to
Macs that perform like a natively installed application, allowing users to work from
a Mac and still access an app that may require Windows XP or a particular version
of Internet Explorer. Integration with the Volume Purchase Program (VPP) enables
IT to assign and distribute apps in bulk to user. Apps can be distributed using
dynamic smart groups and access can be instantly removed if a user unenrolls
their device—automating both delivery and removal for IT.

Consumer Simple User Experience
In order to drive adoption, IT must deliver a consumer-grade user experience on
work devices. With simple enrollment for both corporate-owned and BYOD, users
can setup devices by simply following a few prompts. Everything users need is
auto-installed, including branding or customization based on ownership type. To
access additional applications, users can use VMware Workspace ONE™ with
single sign on capabilities, so entering credentials repeatedly when working
between apps is eliminated. If users ever need to troubleshoot or request support,
the self-service portal gives them basic administration rights over their enrolled
devices and a way to contact IT for additional assistance. For users, the native
experience is protected, even though IT is able to secure and manage the
corporate data on the device.
End-to-End Security
In addition to simple protections like requiring a device passcode, administrators can define settings for FileVault to ensure devices are encrypted, setup Gatekeeper to protect devices from apps downloaded from unknown sources, and configure certificate authentication on Macs for an added layer of security. AirWatch directly integrates with certificate authorities and automatically distributes certificates to devices without user interaction. From the AirWatch certificate management dashboard, administrators can see installed, expiring and revoked certificates to make sure users aren't losing access. Administrators can also configure restrictions to prevent user actions on the device—including access to applications, system preferences and the App Store. IT can also maintain control of the admin account on devices and utilize Firmware passwords to prevent users from changing critical security settings and policies, ensuring their policies aren't tampered with. Finally, the AirWatch compliance engine continuously monitors for non-compliance and triggers escalating actions that have been pre-set by an administrator if non-compliance is detected, automating monitoring and resolutions so IT isn't dealing with compliance issues on a case-by-case basis.

Remote Management and Troubleshooting
Managing macOS devices from the cloud enables for the devices to be treated truly as mobile devices, helping free IT from the old desktop management model. With a UEM platform IT can be consistent, regardless of the endpoint, and maintain a single-pane-of-glass view of all devices, whether they are running macOS, iOS or another operating system. And, when users need assistance, it can be done remotely, without a trip to the IT department. Push notifications, remote screen lock, device query, remote access to file system logs and configuration files, remote device lock, remote device wipe and even remote view helps IT deliver remote support to users.

Conclusion
Using a mobile paradigm for management of all devices will help enterprises prepare for the post-PC era, in which computing will be increasingly defined by mobile devices. Adopting a device-agnostic and OS-agnostic solution will ensure your enterprise is prepared to secure and manage other devices and operating systems, should the need arise, and can scale to meet the increasingly mobile needs of today's modern enterprise. With a single solution, IT is efficient and focused on one solution, and there is no need to purchase additional point solutions. A unified endpoint management platform helps administrators prepare for a future that includes not only mobile and desktop operating systems, but also wearables and connected objects.