EXECUTIVE SUMMARY

# Modernize Windows 10 Management and Security with VMware AirWatch Unified Endpoint Management

## Evolving Needs of the Modern Workplace

TODAY'S EVOLVING workforce is more mobile and self-reliant than ever before. The use of mobile devices is proliferating, and employees rely on a variety of apps, devices, and cloud-based services. They increasingly choose to perform both personal and work tasks on the same device, and expect choice, self-service, and privacy. Failure by IT to address these expectations results in the delivery of a poor user experience to disengaged employees as well as the increasing use of shadow IT.

In addition, the IT organization itself is largely siloed between the desktop and mobile management worlds. IT has addressed management of mobile devices with modern enterprise mobility management (EMM) solutions. However, the desktop devices have been managed separately until now using traditional PC lifecycle management (PCLM) tools.

This fragmented management model is falling short of IT's cost and security expectations. Since users are no longer tied to their cubicles, and traditional PCLM tools require devices to be joined to the corporate domain and network to receive IT policies and OS patch updates, there is an increased risk of noncompliance as well as a rise in potential threat attack vectors.

Responding to these modern workforce demands starts with eliminating management silos and achieving a consistent, user-centric management approach across all endpoints. According to Gartner analyst Chris Silver, "The future of endpoint management lies in consolidation of management tools that manage traditional PCs and mobile devices as a common management framework evolves across the two."

The introduction of mobile management protocols in Windows 10 provides IT with the opportunity to unite IT management teams and consolidate tools, lower costs, increase IT efficiency, and harden enterprise security. The enterprise can now streamline the management of user devices by implementing a unified endpoint management (UEM) solution for managing both desktops and mobile devices.

### LIMITATIONS OF TRADITIONAL PC MANAGEMENT APPROACH

The primary goal for IT organizations should be to create great experiences for end users that make them more effective and productive. However, the user experiences for mobile devices and PCs are in many ways polar opposites. While the process of deploying and configuring a mobile device has become self-serviceable and efficient, it can take weeks to deploy a desktop or laptop computer and countless hours to image, configure, and maintain it.

**Users are increasingly frustrated that mobile device configuration and management is streamlined while PC configuration is a slow and restrictive process.**

What needs to change?

**1 The OS**

The Windows operating system is the first thing that needs to evolve to accommodate the requirements of today's workforce. Windows 10 presents a consumer-centric OS with features that allow users choice, privacy, and mobility. More significant is the introduction of a fundamentally different approach to security and management of the OS that is more aligned with modern EMM solutions. The unified set of management protocols across Windows 10 PCs, tablets, and phones means IT can now consolidate management tools, provision devices out of the box, and push out policies and apps over the air to get users up and running quickly.

**2 The Management Tools**

Legacy PC management tools cannot efficiently address today's workforce requirements, where end users expect to be able to work anywhere, at any time, and from any device. Users expect a similar experience for accessing work apps and data across all of their devices. Meeting these expectations is becoming more complex for IT teams who continue to use traditional tools to manage PCs because they are:

- **Costly**—Legacy PC management approaches are server-heavy and labor-intensive; they require multiple software solutions and are driven by complex imaging and configuration management methods. Managing software packages and OS patches is a tedious process, and IT is faced with the need to develop and maintain internal skill sets across both desktop and mobile management silos.

- **Insecure**—Management is largely driven by Group Policy Objects (GPOs), and those are only possible for network- and domain-joined devices. With this approach, it could take weeks or even months before security policies, OS patches, and app upgrades are completed, potentially exposing the enterprise to increased security risks. As newer forms of attack vectors continue to originate daily, it is becoming even more difficult for IT to obtain proper visibility into the health and compliance of the endpoints.

- **Restrictive**—Legacy approaches frustrate users by restricting the control they have over their devices. To increase security, IT must limit device types and lock down the OS with only trusted apps and updates. This provides little room for customization, and users have little or no self-service capabilities. These restrictions result in high-touch IT demands and increased help-desk calls, even for simple tasks such as installing an application on the device.

## DAWN OF UNIFIED ENDPOINT MANAGEMENT

The introduction of mobile management APIs into Windows 10 dramatically changes how organizations will be able to manage their PC endpoints. However, unlike iOS and Android, PCs present several unique challenges, such as:

- The need to support complex scripts and GPOs
- Packaging and distribution of classic Windows (Win32) apps
- Testing OS patches before they are made available to the users
- The sheer size of these apps and updates, causing network constraints

Organizations need a unified endpoint management platform that combines the IT and end-user efficiencies seen with EMM for mobile devices, along with the granular requirements of traditional PC management.

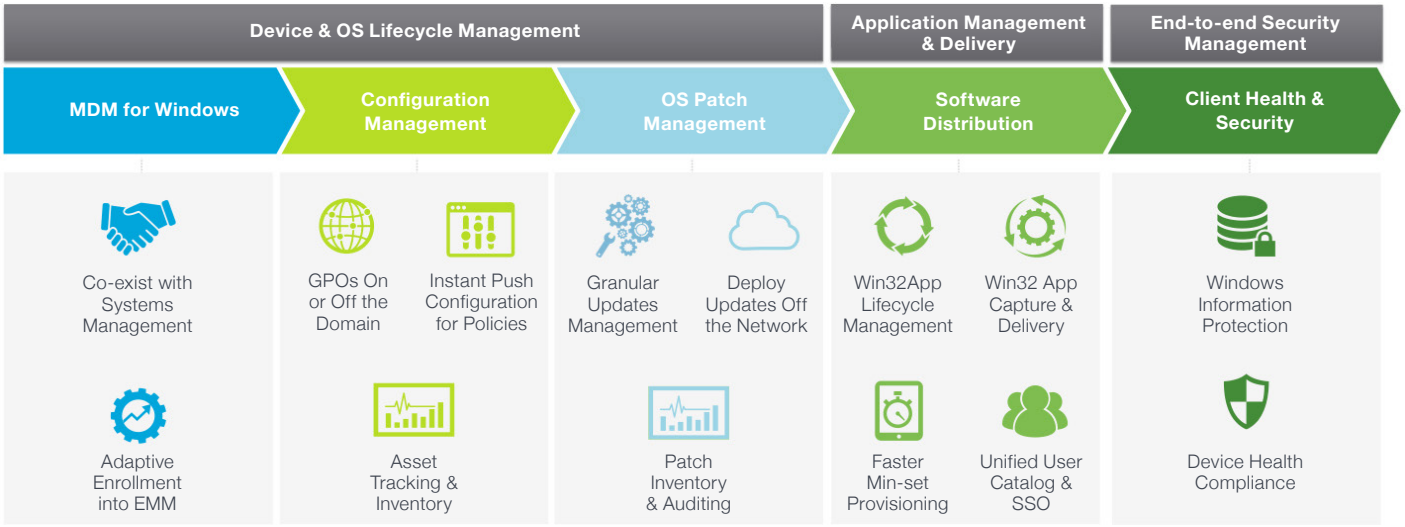
VMware AirWatch Unified Endpoint Management introduces a full set of Windows 10 capabilities enabling OS deployment, configuration, application (including Win32 apps) and update distribution, and end-to-end security. By taking a modern, cloud-first approach, it reduces the costs and burden on IT, and facilitates simpler and more secure implementation and management of Windows 10. This allows the organization to:

- Move from an expensive imaging process to a simpler deployment model
- Support OS patching and software distribution for devices off the domain and on any network
- Provision user self-service access and choice of features, devices, and apps
- Establish co-existence of personal and work data on devices
- Enable instant visibility, security, and compliance for all endpoints on or off the network

With AirWatch UEM, Windows management also scales across any use case, such as:

- Deploying Windows 10 to remote workers
- Onboarding employees' BYOD machines
- Implementing corporate deployments across branch offices
- Managing a special line of business terminal

## AirWatch UEM delivers simpler, more secure, and cost-effective device managment




## DEPLOY CLOUD-FIRST WINDOWS MANAGEMENT AND SECURITY

### MDM for Windows

AirWatch supports consistent device enrollment workflows suitable across use cases, such as company-owned or BYOD, whether domain-joined, new, or an existing device. With AirWatch, a generic OEM device can be fully transformed to a trusted state, out of the box, without the need for imaging, which saves IT time and money. In addition to the IT-enabled workflows, AirWatch also supports end users with intuitive, self-service onboarding of devices.

For BYOD users or contractors, AirWatch also enables a step-up enrollment into management based on app sensitivity and security requirements. For example, access to basic productivity apps can be granted via a customized company app catalog based on user identity and entitlement; however, access to apps that contain sensitive company data can be made available only if the device is fully managed with AirWatch.

AirWatch can manage onboarded Windows devices leveraging this modern, mobile-cloud framework, and configure policies instantly and over the air. With every Windows 10 upgrade, Microsoft is constantly expanding the common set of management protocols available to EMM vendors. This is making management more similar to the user profiles and settings we see today for mobile devices. For example, enforcing passcodes, setting up email, enabling corporate Wi-Fi and VPN access, and enforcing device and app restrictions are all aimed at simplifying the OS configuration and enhancing security.

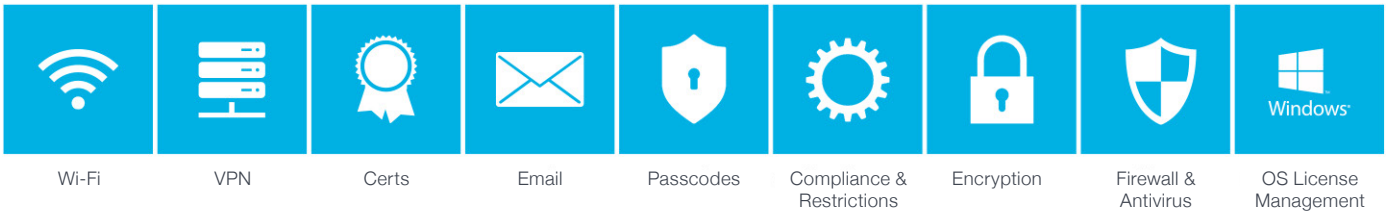
### Configuration Management

When managing Windows PCs, IT will often have complex automation requirements where they are pushing out complex scripts, GPO policies, and other traditional PC-management settings. For example, companies may want to brand their desktops with a custom wallpaper, remove bloatware, and define firewall and antivirus policies. Configuration management capabilities in AirWatch allow IT to create “products” that include these files, apps, or custom settings. These products can then be delivered to the devices instantly over any network; they can also be associated to a more complex sequence of tasks and installation conditions.

### OS Patch Management

With Windows update as a service, Microsoft is pushing cumulative updates of the OS over the air. Updates that have gone through a broad testing cycle are shipped as a business-ready servicing branch. Although there are advantages to this cloud-delivery and servicing model, IT is still fearful of losing control over:

- Which updates are distributed
- Potentially breaking the OS without having thoroughly tested the updates internally
- Network constraints, given that these updates now run several gigabytes in size




**AirWatch simplifies over-the-air device configuration and management.**

AirWatch allows IT to deploy and/or defer OS updates and patches based on device priority and desired maintenance windows. It permits IT to auto-approve or disallow certain update groups, such as application, developer, security, etc., based on users' sensitivity to feature and security updates. By leveraging peer-to-peer caching, AirWatch enables delivery optimization of updates and avoids network congestion. IT can receive detailed inventory and perform compliance auditing of individual Windows updates, and can overcome the challenges associated with off-network patching.

## Software Distribution

With Universal Windows Platform (UWP), Microsoft has unified the app experience across all devices running Windows 10. Public UWP apps can now be delivered via the Windows Store (similar to the store experience on other mobile OS platforms) or via an internal business store that is customized for an organization. AirWatch integrates with both Windows Store and the Windows Store for Business to streamline delivery of these modern apps.

However, most the Windows enterprise software still consists of classic Win32 applications that are large and can be complex to package, deploy, and maintain. This makes software distribution one of the greatest challenges when managing Windows with EMM solutions. AirWatch addresses this challenge by closing the gaps between the UWP and Win32 app lifecycle management.

With AirWatch, IT can consolidate mobile application management and the traditional Win32 software deployment experience into a single admin console. Admins can manage third-party application patches, push out dependencies, and even define conditions or contingencies for app install.

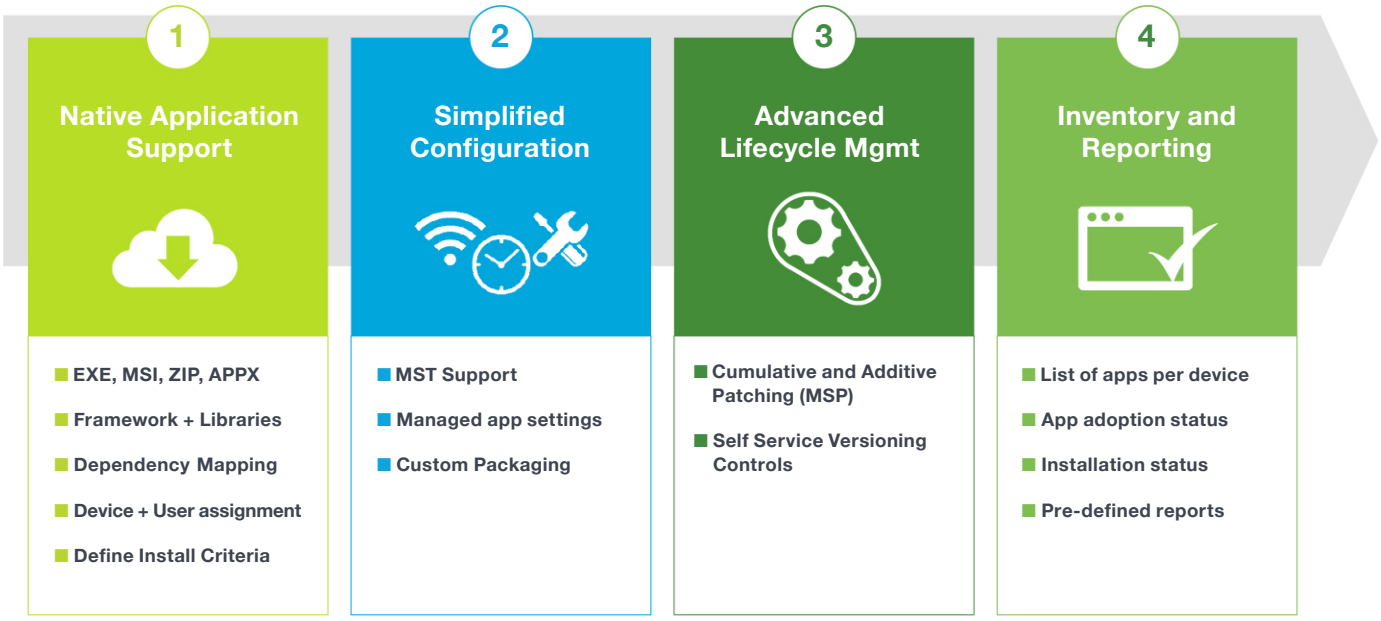
IT can also deploy Win32 apps faster across any Windows device, just as reliably and easily as deploying a mobile app. For the end user, AirWatch delivers a self-service catalog and a consistent, single sign-on (SSO) experience across all Windows apps—including native, SaaS, and remote apps.

## Client Health and Security

Today's new age of cybersecurity challenges also requires end-to-end security. AirWatch establishes user trust, hardens the OS defense against new threats, and provides work and personal data separation to protect company data at rest, in use, and in transit.

- **User trust**—Even the most secure passwords are vulnerable and can be stolen in one of many ways, such as phishing, keystroke logging, and malware. AirWatch integrates with Windows 10 identity features to set policies

## Win32 Application Management Capabilities




for password-less authentication using gestures or a PIN. Organizations can enable multifactor authentication (MFA) out of the box and help protect organizations from pass-the-hash style attacks.

**OS hardening**—AirWatch enables IT to take proactive security measures by preventing untrusted or unapproved apps from downloading or running. AirWatch checks for device integrity and compliance in real time, and automatically blocks access to company apps and services for any noncompliant devices.

**Data protection**—Data loss prevention has become a top priority today as devices grow more mobile, increasing their chances of being lost or stolen. Users are also frequently performing work and personal tasks on the same machines. AirWatch sets policies for encrypting data, allows admins and end users to remotely wipe the device if lost or stolen, and ensures separation of work and personal data by leveraging the native containerization features of the Windows OS.

AirWatch UEM helps the enterprise cost-effectively enforce end-to-end security management.

### SECURE ANY ENDPOINT FROM A SINGLE PLATFORM

By design, UEM must be platform-independent, providing a single solution for managing every device and every operating system across any organizational use case. This ensures that end users have a consistent experience regardless of the device they use to access the corporate environment.

AirWatch UEM provides a holistic, user-centric approach to manage and secure any endpoint from a single platform. It supports global deployment across divisions, regions, and departments within a single console with a multitenant architecture. AirWatch UEM integrates with enterprise systems to make the most of existing infrastructure investments and extend those services to all endpoints.

With VMware AirWatch UEM, IT can automate processes through dynamic and intelligent policy engines to Windows 10 platforms. This alleviates manual IT tasks and enables self-service capabilities, thus reducing support costs.

Are you ready to rethink how you manage endpoints? We invite you to enroll as many as 100 devices in a free, 30-day trial. To learn more, visit the website.