vmware® airwatch®

Redefine Windows 10 Management

Embrace True Business Mobility

DELL

Table of Contents

Introduction

Many IT organizations are still treated as cost centers with their roles squarely focused on run-the-mill operations – relentlessly supporting users, devices, apps, and operating systems (OS).

Consumerization of IT (with BYOD) and mobile-cloud initiatives are quickly becoming the norm in order for businesses to stay competitive. This is forcing organizations to think beyond basic end user productivity and collaboration, and embrace modern business mobility initiatives that require reengineering core business processes to a mobile-cloud model.

With Windows 10, Microsoft brings to market a mobile and cloud-ready OS that is poised to have a significant impact on organizations' end user computing (EUC) strategy. The modern OS offers a unified platform for building apps and extending the organization's core processes to end users anywhere and using any Windows 10-powered device. However, enterprise wide execution of this business mobility vision comes with its own set of challenges. A 2015 VMware study involving 1,000+ IT decision makers identified the following top concerns for adoption of mobility initiatives:[1]

1) Reduce the overall cost and complexity of management

2) Ensure security and control of devices at all times

3) Minimize the risk of corporate data loss

With a unified endpoint management vision, VMware is strategically positioned to address these challenges. VMware's EUC solution enables organizations to fully capitalize on their mobility initiatives and IT departments to redefine themselves as true business enablers. This whitepaper is targeted at Technology Decision Makers (TDMs) and IT Pros and highlights how VMware redefines Windows 10 deployment and management across the enterprise.

[1] VMware State of Business Mobility Report. Rep. VMware, Nov. 2015. Web. <http://www.air-watch.com/lp/vmware-state-of-business-mobility-report-2015/>.

VMware Solution

At the core of VMware's unified endpoint management vision lies the AirWatch enterprise mobility management (EMM) solution.

VMware AirWatch® offers Windows 10 management support and introduces smarter ways to deploy, control, and manage an organization's PC fleet. It reduces the total cost and complexity of management by enabling IT to consolidate on the required tools and management panes of glass, and eliminating many of the pain points of traditional PC lifecycle management tasks (e.g. need for staging and imaging; complexity of maintaining drivers; managing OS updates, firewall, antivirus, encryption policies).

Further, AirWatch enables IT to control and secure devices for end users via detailed security profiles, compliance settings, and device restrictions. The solution minimizes the risk of data loss by ensuring that only managed devices meeting company defined compliance polices get access to apps, content, and email.

The rest of the whitepaper goes through in detail, how the VMware End User Computing solution helps address an organization's concerns for adoption of business mobility initiatives, particularly as it relates to their Windows 10 deployments.

Reduce Cost and Complexity of Management

Windows 10 enables IT administrators to take full advantage of the new enterprise mobility management capabilities. AirWatch embraces the best of the traditional client management functions and brings together the industry leading EMM capabilities to simplify Windows 10 desktop and mobile device management.

Streamline Deployment

With AirWatch, IT administrators can dramatically simplify the process of device enrollment and provisioning. AirWatch provides an intuitive Windows 10 onboarding experience over any network—public (cloud domain joined) or private (non cloud domain joined)—across corporate, BYOD, and CYOD scenarios. AirWatch integrates with Microsoft Active Directory (AD) on-premises and Microsoft Azure AD in the public cloud to support either hybrid or full cloud enrollment models for joining the devices to the domain.

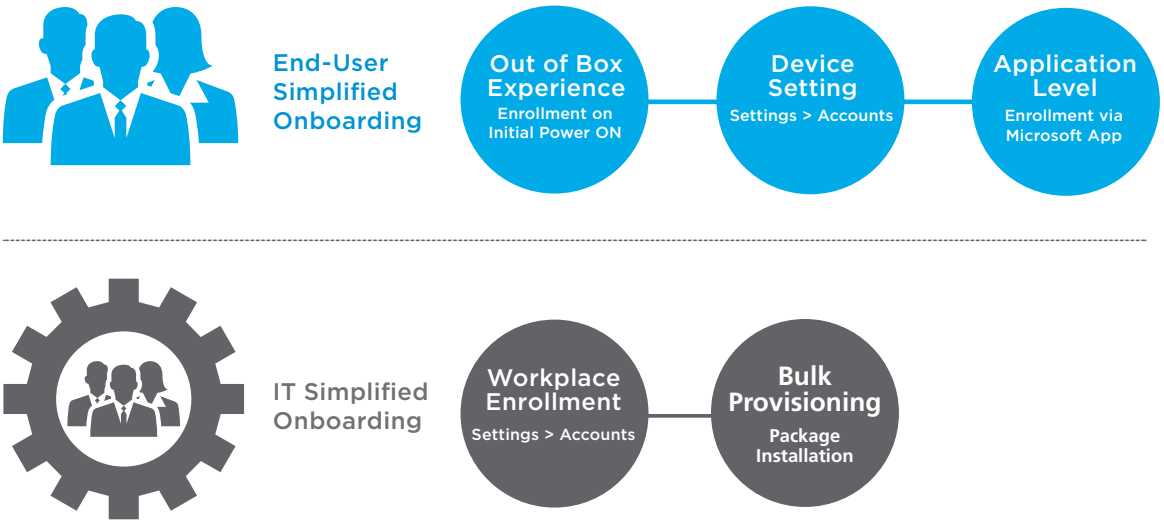

Figure 1: AirWatch Windows 10 provisioning use cases

End User Simplified Onboarding

Integration with Azure Active Directory enables organizations to support end user self-service enrollment with zero IT involvement and minimal user interaction. End users can enroll via:

- An out-of-box enrollment experience upon boot
- Adding their corporate credentials
- Signing in to organizational applications (e.g. Microsoft Office)

OpEx/IT Productivity:

End user self-service enrollment with zero IT involvement

The self-service enrollment methods using work credentials join the devices to the cloud domain; correctly configure profiles, settings, apps, compliance policies, and content; and set up the device for management by AirWatch – all in one streamlined workflow.

IT Simplified Onboarding

Traditional imaging and domain joining has always been a time consuming and complex solution for enrollment of devices. Runtime provisioning in Windows 10 when combined with AirWatch product provisioning capabilities enables IT admins more granular, policy-based approach to bulk enroll devices without the need for re-imaging for individual use.

OpEx/IT Productivity:

One click bulk enrollment via policy without the need for re-imaging

(cont. from IT Simplified Onboarding)

Using AirWatch, IT administrators can bulk import specific device serial numbers and map these to the user accounts that are receiving the device. AirWatch provides the necessary staging and provisioning service URLs (discovery, enrollment, and policy), which feeds into the Windows Imaging and Configuration Designer (ICD).

Combined with AirWatch product provisioning capabilities (see Application Management section), AirWatch enables IT to to create a single pre-configured enrollment package; where configuration settings, apps (including EXEs and MSIs), software updates, drivers, files, and commands are delivered remotely to the end user via email or a media disk, and installed with just one click. Alternatively, the package may be imported directly by the admin or the end user within Windows Work Access settings.

Applications

- Remove Bloatware
- Install MSIs
- Install EXEs
- Install DLLs
- Install Drivers
- Install Store AppsInstall Windows Updates
- Deploy Windows License Keys
- Deploy Custom Scripts

Configuration

- Certificates
- Email
- VPN
- WiFi
- Firewall
- Antivirus
- Encryptions
- Windows Update Client
- Application Restrictions
- Add Accounts
- Configure Start Menu
- Configure Wallpaper
- Printer Configuration

Figure 2: Provisioning package can include app lists and configuration settings

Simplify Management

Devices

The AirWatch admin console features the device dashboard that provides IT administrators a quick, high-level, and real-time view of the entire fleet of organization's endpoints – including Windows 10 based devices. The device dashboard is customizable, searchable, and includes filtering capabilities so admins can find specific devices based on various criteria, e.g. device platform, OS version, compliance status, ownership type, etc. The drill down capabilities make it simpler and faster to perform MDM actions and administrative functions on a particular set of devices.

OpEx/IT Productivity:

Unified dashboard for management and reporting for all devices, apps, and OS platforms

The AirWatch admin console also enables for a deeper assessment of any specific device. For example, admins can get detailed information on the security status of the device, e.g., whether or not the Windows 10 device is enrolled into management, if the device is compliant with the passcode and encryption policies, and whether the device posture is healthy based on the configured Health Attestation settings (see Device Posture section).

AirWatch also features an extensive set of pre-configured reports and event logging capabilities that provide administrators with actionable, result-driven statistics on their Windows 10 deployments. IT administrators can also create custom reports, define distribution lists and automate report delivery and schedules all within the centralized admin console.

Device Inventory

AirWatch features asset intelligence capabilities built into the console. IT admins are presented with various device inventory details such as devices in specific organization groups, device network connection status, devices with specific applications installed, whether the device is compromised, and many other pre-configured and detailed reports.

Figure 3: AirWatch Device Dashboard

Applications

One challenge IT admins face with PC management is the fragmented app ecosystem. With Windows 10, organizations no longer need multiple app distribution tools for each app type, and admins can enable end users to access all apps - be it an EXE or a MSI package, a web app, remote, or a universal app - from one unified app store. The new store supports apps that maintain a single code base across mobile and desktop platforms of Windows. This feature saves time for developers and enables admins to work towards unified endpoint management.

OpEx/IT Productivity:

End user self-service installation of apps

(Cont. from Applications)

AirWatch enables admins to deploy a unified app catalog so end users can access corporate approved apps from one location. Application configuration policies in AirWatch also ensure that only trusted apps run on the end users machines (see Application Groups section). Integration with VMware® Identity Manager, an Identity as a Service (IaaS) solution enables IT to control and secure access to corporate apps and provision convenient one-touch access for end users using these apps anywhere and on any device (see Single Sign On section).

The VMware AirWatch® App Catalog™ fully integrates with the Microsoft Store and enables self-service installation of apps that are assigned to the user based on platform, user group, role, and more. It enables developers and admins to view app installation statistics, collect feedback / comments, push update notifications, silently install apps on end users' devices, and create custom branding and categories for the catalog. The AirWatch App Catalog can be pushed to devices automatically during the Windows 10 enrollment workflow or on-demand as a web clip.

With the development of the Microsoft Windows Store for Business, Microsoft delivers the place for developers, IT decision makers and administrators to submit, find, acquire, manage, and distribute Windows 10 apps for organizations. AirWatch is excited to be working with Microsoft to integrate with the Windows Store for Business so that end admins can access, deploy, and use Windows 10 apps in their organization.

Product Provisioning

AirWatch enables for remote delivery of apps, files, and commands via “product profiles.” AirWatch product provisioning capabilities lets IT admins push apps, drivers, firmware updates, complex packages or scripts to keep the organization’s Windows desktops up-to-date and always ready for use. Admins can further simplify product provisioning and software distribution tasks by creating automated schedules and workflows for installation, which can also be configured to install depending on certain conditions, such as network, schedule, or power. AirWatch fully supports basic installation of MSIs, and it goes further by featuring a traditional task automation scripting engine, which provides capabilities that would typically require use of a PC Lifecycle Management (PCLM) tool. This enables IT admins to embrace the best of traditional PCLM capabilities as they transition to the new EMM based managmenet flow.

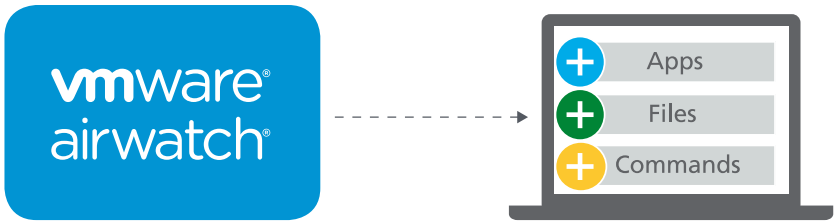

Figure 4: AirWatch product provisioning

Application Inventory

AirWatch supports full inventory control, collection, and reporting for Windows desktop (legacy) and Metro (modern) apps. IT admins can view reports on application versions and deployment status, presence of apps on selected devices, list of applications with their costs; and access many others application inventory features.

Office 365 Support

For organizations using Microsoft Office 365, AirWatch and VMware Identity Manager make the process of provisioning access to the various Office 365 apps simple and automated by sycing with existing directory services (LDAP) user groups. The integration ensures a common identity for authentication and conditional access to the apps so only authorized users, on managed devices, and with purchased licenses are able to access the various Office 365 services.

Email

AirWatch delivers comprehensive email management functionality for Windows 10 to support and secure an organization's corporate email infrastructure by enabling only compliant users and devices get access to email. AirWatch supports email access on the native mail client (Microsoft Outlook) or using the AirWatch Inbox application; and deploying multiple email management configurations2 within the same organization, including Exchange Online and Office 365. This enables IT admins to centralize management of different email environments across branches or user groups, and support upgrade or migration scenarios where a portion of the end points may be on a different environment.

OpEx/IT Productivity:

Support and centralize management of multiple email infrastructures

Content

AirWatch content management solution helps organizations securely deliver and access content across Windows desktop and mobile devices. IT admins can configure and upload managed content in the admin console, sync corporate file servers (e.g. Microsoft SharePoint, Microsoft OneDrive, network shares, etc.), and also enable personal content space for end users. End users can access and share data in a secure manner using VMware AirWatch® Content Locker™.

Traditional Client Functions

Traditional Windows PC management methods are largely dependent on Group Policy Objects. With GPOs, it is necessary that devices be connected to corporate network and have to reboot in order to get policies. Also, organizations would often require a separate EMM-based management infrastructure to secure and manage their mobile and non-Windows endpoints.

CapEx/Infrastructure:

Consolidate or eliminate licenses for traditional PC management tools

With Windows 10 however, there is a fundamental transition from GPOs to EMM-based management of the platform. Powered by AirWatch, the Windows 10 devices can now be configured with real-time updates over the air, on any public or private network. AirWatch also supports native OS settings for encryption, antivirus, malware, and firewall eliminating the need to purchase and support third party software and agents. AirWatch enables co-existence of traditional GPO-based management alongside the new EMM-based approach so admins are not forced into choosing either approach. By bringing together the best of traditional PC lifecycle management (PCLM) and EMM, the AirWatch apporach aims towards elevating IT productivity, reducing costs, and improving endpoint security.

Updates

Windows 10 features a new update service that is designed with mobility and cloud in mind. It changes the notion of the OS upgrade from a wipe and replace model to one where periodic OS and feature updates are pushed over the air. The new Windows update as a service also features servicing plans or Update Branches that enables admins to control the deployment schedule based on the organization's preferred approach or sensitivity to feature and security updates. These changes mean that organizations now require a cloud-based managmenet tool to stay on top of the new update capabilities.

(Cont. from Updates)

AirWatch provides granular control on how Windows updates are managed and delivered across the organization. IT administrator can choose whether users have access to control OS updates on their own, or can choose to enforce the device updates via subscription to the Windows update sources. AirWatch integrates with the new Microsoft Update Service, and also supports an organization's existing Corporate Windows Server Update Services (WSUS).

OpEx/IT Productivity:

Remove complexity of managing updates, patches, drivers, and other traditional PC lifecycle tasks

Admins can set policies on how the updates are delivered to the device, such as automatically or user authorized and define maintenance windows, such as the preferred day and time for installation, so updates don't interfere with user productivity. AirWatch also provides options to select if updates for other Microsoft and third party products may be installed simultaneous to Windows updates, and whether or not Windows Insider Builds should be pushed to the end users. AirWatch also supports new Windows 10 updates delivery optimization feature for peer-to-peer delivery, so users receive updates and apps more quickly.

Antivirus and Malware

Administrators can also manage policies for the native Windows Defender antivirus and build compliance policies from within AirWatch. IT admins can enable real-time monitoring, set definition update and scan windows, add exclusions, choose automatic actions across different threat levels, and set various other advanced monitoring and scan policies.

In addition to native Windows Defender policies, admins can configure compliance rules for third-party antivirus solutions to ensure that monitoring is enabled and the the virus definitons and signature files are up to date.

Firewall

Firewall policies across private and public networks are yet another traditional client management functions that can now be managed more efficiently via the AirWatch admin console.

Encryption

AirWatch enables configuration of BitLocker Encryption policies so organizations can silently encrypt a full disk or just the OS partition. Admins can escrow the BitLocker recovery key within the AirWatch admin console and also the end user Self-Service Portal (SSP) – as part of enabling a new self-service model that reduces the burden on IT.

Enable End User Self-Service

AirWatch also enables for a number of end user self-service capabilities, which further reduces the burden on IT in supporting end users and clients, and instead enables them to focus on more value enablement tasks.

Self-Service Portal (SSP)

In addition to end user self-service device enrollment and installation of apps and updates, AirWatch enables admins to set up the Self-Service Portal (SSP) that alleviates IT support and helpdesk tickets by empowering end users to remotely monitor and manage their own devices. End users can enterprise wipe their devices, view the BitLocker personal recovery key, send messages and perform many other device management tasks on their own via the Self-Service Portal. A list of SSP supported tasks for Windows desktops and mobile devices is provided in the table below:

OpEx/IT Productivity:

End user self service management reduces help desk calls and burden on IT

Actions	Delete Device	Device Query	Device Wipe	Enterprise Wipe	Lock Device / Screen	Locate Device	Send Message	Download Agent	Recover BitLocker Key	Delete Registration	View Enrollment Message	Resend Enrollment Message	Generate App Token	Revoke App Token	Manage Email	Review Terms of Use	Upload S / MIME Certificate
Windows Desktop	X	X		X	X		X	X	X	X	X	X	X	X	X	X	X
Windows Mobile	X			X	X	X	X			X	X	X	X	X	X	X	X

Table 1: AirWatch Self-Service Portal (SSP) capabilities for Windows 10 devices

Secure and Control Windows 10 Devices

Securing Windows 10 desktops and mobile devices starts with enrolling the endpoints under management by EMM. This ensures that only managed endpoints have access to corporate apps, resources, and repositories. Once enrolled, AirWatch enables configuration of security profiles, compliance policies, and device restrictions that ensures greater control and security by making sure that devices are not tampered with.

Device Profiles

Device profiles are the primary means for managing and securing devices using AirWatch and contain the payloads (i.e., settings, configurations, and restrictions) that organizations want to enforce on the Windows 10 devices. The payloads help admins set polices that mitigate the key problems associated with ensuring identity/access (e.g. passcode, credentials, Passport for Work), data (e.g. Data Protection, encryption), and threat protection (e.g. anti-virus, firewall) for the Windows 10 users and devices.

With AirWatch, admins can build both Windows 10 desktop and mobile device profiles and assign these to specific smart groups – admin defined customizable groups that determine which platforms, devices and end users receive an application, compliance policy, and device profile. Table 2 identitifies the Windows device profile payloads that are supported in AirWatch.

Payloads	Passcode	Wi-Fi	VPN	Credentials	Restrictions	Data Protection	Passport for Work	Firewall	Single App Mode	Anti-Virus	Encryption	Windows Updates	Web Clips	EAS	SCEP	Application Control	Exchange Web Service	Email	Assigned Access	Custom Settings
Windows Desktop	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
Windows Mobile	X	X	X	X	X	X	X		X		X	X		X	X	X		X		X

Table 2: AirWatch device payloads for Windows 10 devices

Device Restrictions

The Windows 10 desktop and mobile profiles in AirWatch also includes options for enabling many device-level restrictions for greater MDM control. IT administrators can now set restrictions around:

Secure/Control:

Granular controls for device- and app-level restrictions

- Device administration: e.g. enable users to un-enroll their device or reset device
- Security and privacy: e.g. enable use of location services or telemetry data
- Device settings: e.g. enable users to change date and time or language settings
- Device functionality: e.g. enable use of camera, Bluetooth, Cortana
- Applications: e.g. enable use of only trusted apps, auto updates
- Network: e.g. enable cellular data on roaming, auto connect to Wi-Fi configurations
- Browser: e.g. enable auto fill of browser forms, cookies, pop-ups

Application Groups

AirWatch supports application control3 profiles for Windows 10 enabling admins to create application whitelist and blacklist rules and prevent users from downloading and installing unapproved apps from the public app store. AppLocker policies can be provisioned to block usage of other previously installed apps that that are restricted as defined by the application control configuration.

Compliance Engine

AirWatch features a real-time compliance engine that ensures all devices abide by the management and control policies that were defined by the IT administrator. These security polices are platform specific and can cover a range of compliance criteria; e.g. device profiles (e.g. passcode, antivirus, encryption), application list (e.g. whitelist, blacklist, required), compromised status (Health Attestation), and others as identified in the table below. Admins can also configure automated escalation rules that perform specific actions (e.g. notify user, block access to apps) and enable grace periods when a device is determined to be out of compliance. Automated escalation rules reduce the burden on IT to periodically monitor their entire device fleet for compliance, and also increases the overall security posture by ensuring only compliant devices have access to corporate apps and data.

Secure/Control:

Real-time compliance engine with automated escalation policies

Compliance Policies:	Antivirus Status	Compromised Status	Device Last Seen	Encryption	Firewall Status	Terms of Use Acceptance	Model	OS Version	Passcode	Roaming	SIM Card Change	Windows Automatic Update Status
Windows Desktop	X	X	X	X	X	X		X	X	X		X
Windows Mobile			X	X		X	X	X	X		X	

Table 3: AirWatch compliance policies for Windows 10 devices

Device Posture

Health Attestation in Windows 10 checks for boot state (e.g. Secure Boot, Boot Manager version) and security status (e.g. BitLocker, Device Guard) to help identify whether the device is compromised. AirWatch admin console enables administrators to choose specific Health Attestation attributes to mark the device as being compromised. The compliance engine checks to see if any of these attributes failed, and takes necessary actions as defined by the administrator. Since AirWatch pulls the health attestation information directly from the Trusted Platform Module (TPM) – an encrypted hardware component built into the device – instead of the OS, the compromised detection works even if the OS kernel is compromised.

Secure/Control:

Combination of hardware and software controls for checking device posture

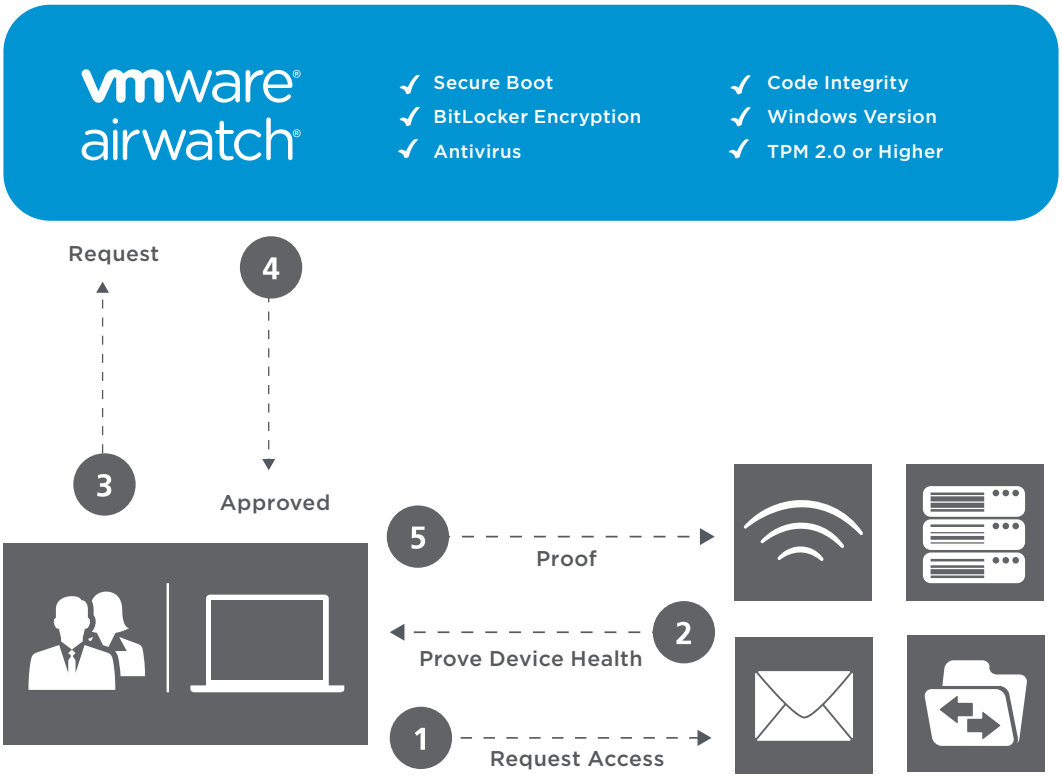

Figure 5: Heath Attestation for Windows 10

Authentication

Usernames and passwords can be forgotten, shared, or exploited (e.g. pass-the-hash-attacks) putting corporate data at risk. Windows 10 brings together a combination of strong authenticators and hardware and virtualization-based (Credential Guard) security. With AirWatch, admins can establish well-defined authentication policies for Windows 10 that mitigates credentials from being exploited and puts an end to the pass-the-hash attacks.

Multi-Factor Authentication (MFA)

Windows 10 introduces Microsoft Passport—a multi-factor authentication (MFA) built into the OS and a more secure, enterprise-grade replacements for passwords. AirWatch integrates with Windows 10 new security features Windows Hello (biometric-based authentication) and Passport PIN. With AirWatch, you can set policies for user verification gestures, configure PIN strength and complexity requirements and provision certificates to identify users.

Secure/Control:

Support MFA and SSO for greater authentication security

Single Sign-On (SSO)

SSO ensures users sign in once on their device to access all of the organization's available recommended apps without the need to sign in each time. VMware Identity Manager, a cloud-based solution, provides directory services integration for local on-premises directory services (LDAP) and uses SAML assertions to federate identity to the cloud. Federated identity enables for SSO across all of the Windows 10 apps – including SaaS, Office 365, Outlook, and mobile. Besides lowering help desk calls for "forgotten passwords," the SSO capability provides increased security as users no longer store/write down passwords at places where it can be compromised, and access to all apps can be easily turned off to prevent data leakage in the event of employee separation.

Minimize Risk of Data Loss

Security is key to every aspect of the AirWatch mobility management and data loss prevention strategy. Securing data on the Windows 10 endpoint starts with securing access to the application servers themselves so only managed apps and authorized users are able to access those servers. With AirWatch, IT administrators can define advanced data loss prevention policies on Windows 10 devices to contain and protect company data, while managing privacy concerns over employees' personal data. VMware Identity Manager integrates with AirWatch enterprise mobility management capabilities to create further value to the enterprise. The integrated solution minimizes the risk of data loss by ensuring that only managed devices meeting company defined compliance polices get access to apps, content, and email.

Per-App VPN

Organizations may employ VPN gateways to ensure secure connections from endpoints. However, device level VPNs cannot distinguish between work, personal, and rogue apps on an endpoint; and will enable traffic flow between the device and datacenter as long as the VPN connection is active.

CapEx/Infrastructure:

Eliminate need for third-party VPN service and licenses

Per-app VPN capability in AirWatch enables app-level security with microsegmentation on the client side so only entitled users, with validated devices, using authorized apps are accessing the datacenter connection at any time. Using the Windows 10 VPN profile, admins can pick specific apps that are enabled access to corporate resources, which can be IP addresses, ports or intranet locations such as SharePoint. The per-app VPN capabilities prevent access to company data via any other unsecured or untrusted apps. The embedded VPN service - VMware AirWatch® Tunnel™ - eliminates the need for a third-party service and the added licensing fee, ensuring that the VPN service is delivered at a lower TCO. Besides supporting a native VPN service, AirWatch also integrates with organizations' existing VPN services.

Figure 6: AirWatch App Tunneling and per-App VPN

Conditional Access

Integration with VMware Identity Manager enables IT admins to grant conditional access to enterprise resources based on whether or not the device is managed and the compliance requirements are met. The AirWatch compliance engine continuously evaluates for device compliance, based on robust compliance profile assignment criteria (as identified in Table 3) to control access to to any app (e.g. mobile, desktop, SaaS, universal); multiple data repositories (via AirWatch Content Locker), multiple email deployments, and any device type.

When access to corporate resource is requested by the end user, VMware Identity Manager validates whether the device is managed and compliant as reported by the compliance engine. Adaptive access controls support claim based authentication that can be dependent on users or groups, device type, app type, device management, and network (domain). The conditional access policies also extend to Exchange Online or EAS configurations where admins can create whitelist or blacklist policies to restrict access and delivery of emails to unmanaged, non-compliant devices.

Data Loss Prevention

IT admins can enforce advanced data loss prevention capabilities that prevents users from copy/paste and opening of corporate attachments or files outside of the secure container (AirWatch Content Locker). AirWatch content management solution enables document level encryption, enables whitelisting and blacklisting based on file types, and protects data in transit and at rest using AES 256-bit encryption. Further, AirWatch email management capabilities prevent data leakage from corporate email by ensuring that email attachments and hyperlinks only open inside of a secure container, managed browser, or the managed mailbox.

Secure/Control:

Better end-to-end security posture with client-side microsegmentation, conditional access, and data leakage prevention

Enterprise Data Protection (EDP)

Besides native data loss prevention features, AirWatch is excited to partner with Microsoft in supporting enterprise data protection (EDP) capabilities for organizations participating in Microsoft TAP program and certain Windows Insiders.

Summary

Business mobility is rapidly evolving into a digital workspace that empowers workers with the right toolset – devices they are most comfortable with, transformative business processes, and access to data and resources – to do their jobs well. By moving from a legacy PC-centric to a modern device-agnostic OS, Windows 10 presents opportunities for organizations to embrace true business mobility scenarios that supports IT administrators, developers, and end users alike:

- By embracing enterprise mobility management as the de-facto management tool, Windows 10 enables IT administrators to efficiently support multiple device types and ownership use cases.

- The universal app platform enables developers to build or reengineer organization's core business processes using a single code base and deploy to end user devices through a unified interface.

- The OS is designed to work seamlessly across the unified desktop and mobile devices' platform, delivering a consistent productivity experience to end users anywhere and on-the-go.

As enterprise look into the future of business mobility, their leaders must adopt a cohesive, purpose-built solution that delivers a "consumer simple, enterprise secure" experience for all stakeholders involved. VMware's end user computing solutions are purpose built to address the most common challenges for adoption of mobility initiatives. Featuring VMware AirWatch® Enterprise Mobility Management™ and VMware Identity Manager, the unified endpoint management solution reduces the cost and complexity of managing organization's Windows 10 fleet, provides granular control for ensuring control and security of endpoints, and enables advanced data loss prevention capabilities.

Additional Resources

For more information, visit **www.dell.com/datasecurity**
or contact us at **DataSecurity@Dell.com**.

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

Item No: 7881_Dell Launch_Win10 Mgmt Whitepaper