WINDOWS 10 SECURITY AND VMWARE AIRWATCH

Protecting your digital workspace

OVERVIEW

Anytime, anywhere access to work is now a basic need for the modern workforce. Whether remote, in the field or in the office, workers are no longer physically connected to your network or data center. Today's employees work in a digital workspace that features virtualized laptops, desktop and workstations; a variety of personal systems and smart devices that may be part of BYOD programs and a diverse app ecosystem with desktop, remote, mobile, SaaS and Universal apps. In this mobile-cloud world, new and unpredictable forms of malicious software continue to evolve. Traditional network security, perimeter protection and firewalls are no longer enough to combat these new threats to the corporate IT infrastructure and company data integrity.

Windows 10 is Microsoft's first truly mobile operating system – designed to work seamlessly across desktop, mobile and multiple other device types such as wearables and IoT devices that run on this new OS. The platform redefines how organizations manage desktops and devices and incorporates security features that are purpose-built for desktop and mobile security challenges.

VMware® AirWatch® enhances these Windows 10 security features and makes them easier to manage and deploy so you can ensure your mobile enterprise is secure and that corporate data is protected.

HOW AIRWATCH EXTENDS WINDOWS 10 SECURITY

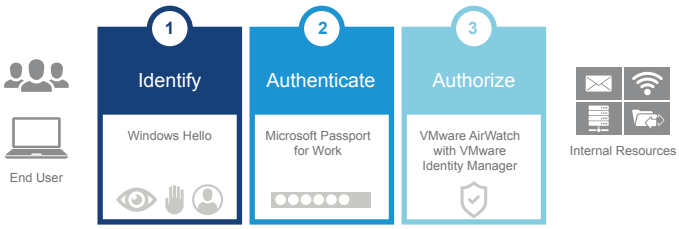
AirWatch extends Windows 10 security to users, devices, apps, data, content, email and networks. It adds protection in three key areas: identity and conditional access, OS health and threat protection, and data loss prevention.

Identity and Conditional Access

Ensuring data is accessed by authenticated users from trusted devices.

The requirements for secure user passwords and authentication have changed a lot over the years. Many enterprises struggle balancing stricter standards with user convenience and compliance. With Windows Hello and Microsoft Passport, Windows 10 offers strong multi-factor authentication (PIN and biometrics) so both IT and end-users can do their part to keep the enterprise secure.

Also, Credential Guard incorporates virtualization-based credential isolation to safeguard corporate identity even further.



AirWatch integrates with these Windows 10 features and your directory services (AD or Azure AD) to help establish well-defined authentication policies that mitigate credentials from being exploited and put an end to pass-the-hash attacks. AirWatch enables you to set Passport for Work policies, including use of Hello biometric gestures and PIN strength and complexity requirements. With AirWatch, you can also provision certificates for use with Passport for Work that identifies the enrolling user and device, and allows for a more secure and simplified multi-factor authentication use case when compared to smartcards.

AirWatch also features VMware Identity Manager™, an identity provider incorporating single sign-on and a conditional access control framework to ensure access to enterprise resources is restricted to authorized users and devices. With point solutions for identity and OS management, companies often have a weakened security posture that can be compromised. Valid users could access the network from a compromised device or a malicious user could gain access to a trusted company device and bypass the security.

However, AirWatch combined with VMware Identity Manager provides complete conditional access control and a stronger security posture. AirWatch continuously evaluates for device compliance, to control access to apps and data based on device type, app type, device management status, location and network (domain) membership among several other criteria. Devices not in compliance have their access to corporate VPN, Wi-Fi, email, content repositories, as well as on-premises and cloud apps like Office 365, revoked automatically. This access control ensures the best user experience for your Windows users, while maximizing security for untrusted and unmanaged devices.

vmware® airwatch®

ABOUT VMWARE AIRWATCH

VMware AirWatch is a comprehensive enterprise mobility platform built to manage any endpoint including smartphones, tablets, laptops, rugged, printers, wearables and IoT devices across all major operating systems in a single management console throughout the entire device lifecycle. With a mobile-cloud architecture, AirWatch is designed to scale as business initiatives evolve. AirWatch seamlessly unifies the technologies of identity, native apps and device management to remove the friction of disparate systems. With a multi-layered security approach across the user, endpoint, app, data and network, AirWatch provides complete protection of corporate data and intelligent access controls, compliance monitoring and threat detection. The AirWatch apps suite enables mobile productivity and collaboration with consumer-simple and integrated business apps that unlock mobile micro-moments and drive digital transformation.

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

OS Health and Threat Protection

Lock down devices against malware and un-trusted apps.

As numerous new and unpredictable forms of malicious software and malware continue to emerge, reactive threat protection approaches may no longer be viable. New features in Windows 10 redefine how apps are trusted from the moment a device is powered ON to when it is shut down.

Device Guard - a combination of hardware and software security features allow only trusted applications to run and prevent attackers from taking control of the Windows kernel.

Secure Boot - allows only trusted software to load when a device is turned on.

Health Attestation - checks boot state and security status to determine whether a device is compromised.

All these features increase IT's visibility into the health of managed Windows 10 devices and provide a way for IT teams to manage these security policies with AirWatch. IT admins can select specific attributes from the AirWatch console to mark the device as compromised. The AirWatch compliance engine continuously checks to see if any of these attributes failed and then performs automated actions as defined by the admin to urge users to correct the compliance issue. Compromised detection works even when the OS kernel is compromised as AirWatch pulls the health attestation information directly from the Trusted Platform Module (TPM)—an encrypted hardware component built into the device—instead of the operating system (OS).

Data Loss Prevention

Ensuring corporate data is kept separate from personal data and is encrypted when stored on devices.

Enterprise Data Protection (EDP) is integrated into Windows 10 to protect data at the file-system level, while providing a seamless experience for end users that are increasingly accessing both personal and work data on the same device. EDP makes it easier to detect and differentiate between company and personal data on a device by classifying data, domains, cloud services and apps as "corporate" and setting appropriate policy levels for handling data coming from corporate sources.

AirWatch administers these policies and allows admins to designate trusted desktops or modern apps with permission to open encrypted work data. Admins can configure enterprise-protected boundaries—IP ranges, domain names or proxy servers—where data originating from these sources is automatically tagged as corporate data and is protected by the OS. Flexible enforcement levels in AirWatch can either enable or disallow certain user groups from data moving and sharing through actions such as copy / paste or drag.

Windows 10 also enhances many existing EMM security features from previous Windows versions, including BitLocker encryption. AirWatch allows 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 console and the end user Self-Service Portal (SSP).

vmware® airwatch®

VMware, Inc. 1155 Perimeter Center West Suite 100 Atlanta, GA 30338 United States | t: +1 404 478 7500 | f: +1 404 478 7530 | sales@air-watch.com | air-watch.com

6/28