VMware Workspace ONE

Consumer Simple – Enterprise Secure

AT A GLANCE

VMware Workspace™ ONE™ is the simple and secure enterprise platform that delivers and manages any app on any smartphone, tablet or laptop. By integrating identity management, real-time application delivery, and enterprise mobility management, Workspace ONE engages digital employees, reduces the threat of data leakage, and modernizes traditional IT operations for the Mobile Cloud Era.

KEY BENEFITS

- Allow organizations to securely embrace SaaS, mobile apps while supporting existing enterprise applications
- Attract and retain top talent with tools that give employees freedom to be productive while maintaining the right data security and compliance
- Accelerate the adoption of Windows 10 by using the same modern management framework designed for mobile devices
- Adaptive conditional access ensures the right level of security based on authentication strength, data sensitivity, user location, device posture

Key Market Trend

The rapid adoption of new modern applications (SaaS apps, mobile apps) coupled with the proliferation of powerful yet affordable mobile devices has introduced new challenges in the work environment.

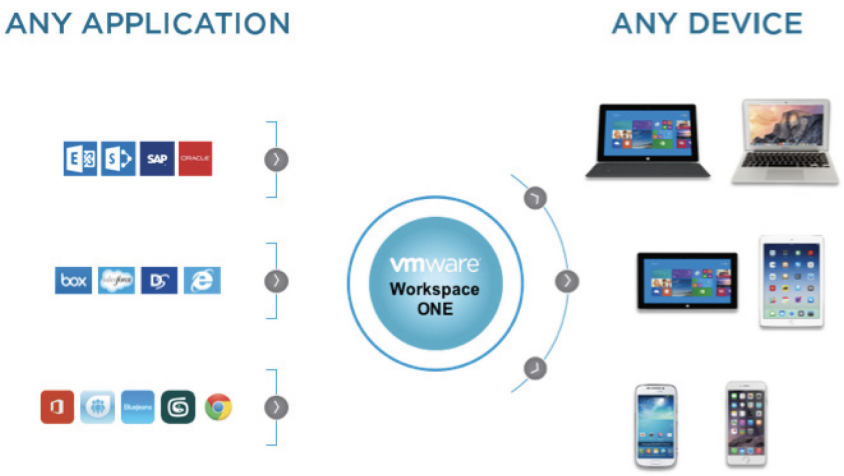
In order to be productive whenever and wherever, employees have gone around traditional rigid policies. Organizations are facing a critical inflection point to either ignore these trends at the peril of unintended security breaches or to embrace a new way of working leveraging a new management framework.

What is Workspace ONE

VMware Workspace™ ONE™ is the simple and secure enterprise platform that delivers and manages any app on any smartphone, tablet, or laptop. It begins with consumer grade self-service, single-sign on access to cloud, mobile, and Windows apps and includes powerfully integrated email, calendar, file and social collaboration tools that engage employees.

Meanwhile, employees are put in the driver's seat to choose their own devices and the weight of management necessary to drive the adoption of BYOD programs including a combination of VMware Identity Manager and AirWatch Enterprise Mobility Management to enforce fine-grained, risk-based conditional access policies.

Finally, Workspace ONE ruthlessly automates traditional onboarding, laptop and mobile device configuration, and delivers real-time application lifecycle management that bridges between legacy enterprise client-server apps to the mobile-cloud era.



Key Features

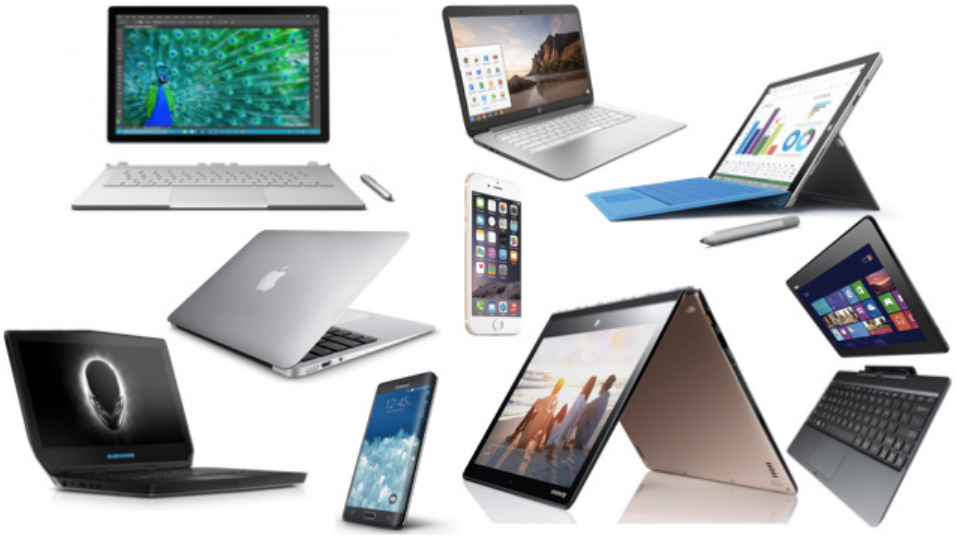
Consumer Grade Self-Service access to Cloud, Mobile, Windows apps

Onboarding new apps and new employees couldn't be easier. Once authenticated through the VMware Workspace ONE app, employees will instantly access their personalized enterprise app catalog where they can subscribe to virtually any Mobile, Cloud or Windows app. With the built-in VMware Identity Manager, access to applications is only a touch away as industry-first, one-touch mobile Single Sign-On is already established through the device.

FEATURE	DESCRIPTION
Deliver Any Application from the latest mobile cloud apps to legacy enterprise apps	An enterprise app catalog to deliver the right apps to any device including: • Internal web apps through a secured browser and seamless VPN tunnel • SaaS apps with SAML-based SSO and provisioning framework • Native public mobile apps through brokerage of public app stores • Modern Windows apps through the Windows Business Store • Legacy Windows apps through MSI package delivery • Secure sensitive systems of record apps behind a HTML5 proxy by hosting in the datacenter or cloud provider with Horizon Air • Deliver complete virtualized managed desktops in the cloud, or in on-premises datacenters through Horizon Air • Supports Citrix XenApp hosted applications
Self-Service App Catalog that transforms employee onboarding	Simply downloading the Workspace ONE app on Windows, iOS or Android provides employees with a complete, self-service enterprise app catalog that can be easily customized and branded for your company.
Single-Sign On that federates even the most complex on-premises Active Directory topologies	Remove the need for complex logins by establishing trust between user, device, and the enterprise for one-touch authentication. Step up to seamless biometric or other multi-factor authentication methods for more sensitive applications. Workspace ONE with Identity Manager includes an enterprise-grade Identity Provider for SAML and WS-Fed (Web Service Federation) supported apps and can also daisy chain to any existing 3rd party identity providers already in use.
Industry-first One-touch mobile SSO leverages device trust and PIN/biometric timeout settings for authentication	Many applications can be simply secured by relying on an employee unlocking a known, unique and registered device through the local PIN or biometric services. Once unlocked, employees may simply touch an app to open for as long as the authentication window is set. Workspace ONE with VMware Identity Manager and AirWatch combine to create an industry leading, seamless user experience across desktop, web, and mobile. SSO to public mobile apps is achieved using the patent pending Secure App Token System (SATS) that establishes trust between the user, device, application, and the enterprise.
Authentication brokerage leverages both new and existing forms of 3rd party authentication	Workspace ONE with Identity Manager includes an Authentication brokerage that supports 3rd party authentication services such as Radius, Symantec, RSA SecureID, Imprivata Touch and Go, and others.

Choice to use any device; BYOD or Corporate Owned

The architecture you deploy today needs to work with devices that have not yet been invented. From wearables to 3D graphics workstations, keeping employees productive means that their apps need to be available when and where they are.



While some of these devices may be corporate owned and require IT to configure and manage them through their lifecycle, many will be owned by the employees themselves. VMware Workspace ONE puts the choice in employees' hands for the level of convenience, access, security and management that makes sense for their workstyle providing friction-free adoption of BYOD programs while getting IT out of the device business.

FEATURE	DESCRIPTION
Shrink-wrapped device provisioning leverages OS management interfaces to self-configure laptops, smartphones and tablets for immediate enterprise use	Self-service, shrink-wrapped device provisioning is achieved through the VMware Workspace ONE unified management platform. AirWatch device management that leverages Enterprise Mobile Management APIs from Apple iOS and OSX, Microsoft Windows 10, Google Android, and a variety of specialty platforms for ruggedized devices to provision, configure, and secure apps and devices. This also allows devices to receive patches through the OS vendor for the fastest response to vulnerabilities while leaving configuration and app management to IT.

Secure Productivity Apps: Mail, Calendar, Docs, and Chat

Workspace ONE includes email, calendar, contacts, documents, chat, and enterprise social that employees want to use while invisible security measures protect the organization from data leakage by restricting how attachments and files can be edited and shared.

Far from a "walled garden;" team chat, enterprise discussions, Q&A, content access and other social tools that allow employees to work collaboratively in real time can be integrated into the apps and tools they already use - moving from productivity to real employee engagement.




FEATURE	DESCRIPTION
Consumer-simple Email app delights consumers but is designed for business	A faster, smarter, secure email app that supports your Gmail, Exchange, Outlook, Yahoo, Hotmail, iCloud, Office 365, IMAP & POP3 mail accounts. With integrations to your favorite services like Dropbox, Box and Evernote, it's easier than ever to stay organized.
Integrated Calendar with email makes it simple to set meetings	By integrating email and calendar you no longer have to move out of the email app when you received a meeting invitation. With a few clicks, you can review, respond to the meeting or suggest a new time based on your availability without having to navigate between apps.
Advanced email attachment security reduces data leakage	Secure email and attachments through the use of the AirWatch Secure Email Gateway that can enforce enterprise encryption, wipe, and "open in" controls keeping attachments secure.
Content Management App permits line of business to push and manage secure content on the device	AirWatch Content Locker mobile app permits IT to deliver files directly to devices across a range of internal repositories and external cloud storage providers to ensure the latest, most up-to-date information is at employees fingertips.
Enterprise Chat that increases employee engagement	Secure enterprise chat platform bridges systems of record by integrating into existing enterprise applications while providing a customizable mobile-first chat and notification experience.

Data Security and Endpoint Compliance with Conditional Access

To protect the most sensitive information, Workspace ONE combines identity and device management to enforce access decisions based on a range of conditions from strength of authentication, network, location, and device compliance.

FEATURE	DESCRIPTION
ComplianceCheck Conditional Access policy enforcement that combines identity and mobility management	Conditional Access policy enforcement to mobile, web, and Windows apps on a per-application basis is configured through Identity Manager to enforce authentication strength and restrict access by network scope or through any device restriction imposed by AirWatch (rooted devices, app blacklist, geolocation and others).
Device Management and Compliance powered by AirWatch	Automate device compliance for advanced data leakage protection including protection against rooted or jailbroken devices, whitelist and blacklist apps, open-in app restrictions, cut/copy/paste restrictions, geofencing, network configuration and a range of advanced restrictions and policies enforced through the AirWatch policy engine.
App and Device Analytics provide real time visibility	Record application, device and console events to capture detailed information for system monitoring, and view logs in the console or export pre-defined reports.
Intelligent Network with integration with VMware NSX	Available as an added capability, VMware NSX with AirWatch tunnel further segregate traffic from applications to specific workloads in the datacenter. This substantially reduces attack vectors of malware / viruses that could do significant harm to the organization.

Real-time App Delivery and Automation

Workspace ONE takes full advantage the new capabilities of Windows 10 and leverages the industry leading AirWatch mobile management system to allow desktop administrators to automate application distribution and updates on the fly. Combined with award-winning Horizon virtualization technology, automating the application delivery process enables better security and compliance.

FEATURE	DESCRIPTION
Remote configuration management allows employees to provision new, shrink wrapped devices from anywhere	Workspace ONE with AirWatch configuration eliminates the need for laptop imaging and provides a seamless out-of-the-box experience for employees. Manage configurations based on dynamic smart groups, which consider device information and user attributes, and update automatically as those change.
Windows Software Distribution by AirWatch automates software lifecycle management	AirWatch software distribution allows enterprises to automatically install, update and remove software packages, and also provides scripting and file management tools. Create an automated workflow for software, applications, files, scripts and commands to install on laptops, and configure installation during enrollment or on-demand. 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.
Virtual Apps and Desktops by Horizon delivers secure hosted desktops and apps	Horizon provides secure hosted virtual apps and desktops allowing users to work on highly sensitive and confidential information without compromising corporate data. Users can access their virtual apps and desktops regardless of where they are or the device types that they are using; allowing them the flexibility to be productive wherever they are.
Asset Tracking provides a single view of corporate managed devices, wherever they are	Workspace ONE with AirWatch allows administrators to remotely monitor and manage all devices connected to your enterprise. Because AirWatch is multi-tenant, you can manage devices across geographies, business units or other segmentations in a single console and then define and delegate management with role-based access controls.
Remote Assistance makes it simple to support employees	Workspace ONE with AirWatch Remote Assistance provides support to your end users with remote assistance and troubleshooting. To gather information on a device, perform a device query to collect the latest profile list, device info, installed applications and certificates. To assist with troubleshooting, remotely access file system logs and configuration files for diagnosing an issue. Remote view commands enable IT administrators to request a user to share a device screen.

Learn More

Find out more about VMware Workspace ONE by visiting http://www.vmware.com/products/workspace-one/.
To purchase VMware Workspace ONE or any VMware Business Mobility solutions, call 877-4-VMWARE

(outside North America, +1-650-427-5000), visit http://www.vmware.com/products, or search online for an authorized reseller.

For detailed product specifications and system requirements, refer to the product documentation.

vmware®

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