

VMware helps keep employees connected and protected virtually anywhere



Consumer grade simplicity. Enterprise grade security.

Key market trend

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

The modern apps sit outside of the traditional corporate network and some have to be supported and updated in addition to the existing portfolio of legacy/ native and web apps that still consume significant

IT resources. Furthermore, the growing proliferation of mobile apps also gives rise to inconsistencies in user experience, security posture, and support requirements that must be addressed to manage cost. In order to be productive whenever and wherever, employees have gone around the traditional rigid and old policy. Organizations are facing the critical decision to either ignore these trends at the peril of unintended security breaches or embrace the new way of work using a new management framework.

At a glance

VMware Workspace ONE™ Cloud is the enterprise platform that enables IT to deliver a digital workspace that empowers the workforce to more securely bring the technology of their choice - devices and apps - at the pace and cost the business needs.

Workspace ONE™ Cloud is built on the VMware® Unified Endpoint Management™ technology.

With Workspace ONE™ Cloud organizations can now evolve silo-ed hosted and mobile investments, enabling all employees, devices and things across the organization to accelerate their digital transformation journey with a platform-based approach.

Key benefits

Workspace ONE™ Cloud enables you to improve experiences and tasks that were previously costly, time consuming, and resource intensive. With Workspace ONE™ Cloud, IT organizations can:

- Quickly onboard a new employee with all of his or her apps and devices in under an hour without tickets and help desk calls
- Set and enforce access and data policies across all apps, devices, and locations in one place
- Complete business processes from a mobile device, similar to consumer experiences

What is Workspace ONE™ Cloud

VMware Workspace ONE™ Cloud is the enterprise platform that enables IT to deliver a digital workspace that empowers the workforce to more securely bring the technology of their choice — devices and apps — at the pace and cost the business needs. It begins with consumer simple, single-sign on access to hosted, mobile, web and Windows apps in one unified catalog and includes powerfully integrated email, calendar, and files that engage employees. Employees are put in the driver seat to choose their own devices or benefit from employer provided devices with the ability for IT to enforce fine-grained, risk-based conditional access policies that also take into account device compliance information delivered by VMware Unified Endpoint Management technology.

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

Key features

Consumer-simple access to hosted, web, mobile and Windows apps. Onboarding new apps and new employees couldn't be much easier. Once authenticated through the VMware Workspace ONE™ Cloud app, employees will quickly access their personalized enterprise app catalog where they can subscribe to virtually any mobile, web, hosted or Windows app. Workspace ONE™ Cloud simplifies application and access management by offering Single Sign-On (SSO) capabilities and support for multi-factor authentication.

| Feature | Description |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deliver virtually any application from the latest mobile hosted apps to legacy enterprise apps | An enterprise app catalog to deliver the right apps to virtually any device including: <ul style="list-style-type: none"> • Internal web apps through a highly secured browser and efficient 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 or near real-time delivery with app volumes • Helps secure sensitive systems of record apps behind a HTML5 proxy by hosting in the datacenter or hosted provider with Horizon Hosted • Deliver complete virtualized managed desktops in the hosted, or in on-premises data centers |
| Unifi app catalog transforms employee onboarding | Simply downloading the Workspace ONE™ Cloud 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 | Lightwave can be implemented and run by a hosted provider. The hosted provider's customers can then use it as a hosted-based domain controller running in active-active mode with an on-premises directory service or as a stand-alone directory service. |
| One-touch access leveraging device trust and PIN/biometric timeout settings for authentication | Many apps can be more 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™ Cloud integrates identity management and VMware Unifi Endpoint Management to create an industry leading, seamless user experience across desktop, web, and mobile. |
| Authentication brokerage leverages new and existing forms of third-party authentication | Workspace ONE™ Cloud includes an Authentication brokerage that supports third-party authentication services such as Radius, Symantec, RSA SecurID®, 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™ Cloud with adaptive management 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 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adaptive management designed to maximize adoption for even the most privacy sensitive employees | The Workspace ONE™ Cloud app enables Adaptive Management to enable employees to comfortably adopt BYOD programs by putting control in their hands to decide what level of access, and corresponding management they want to use. |
| 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 VMware Workspace ONE™ Cloud platform powered by VMware VMware Unifi Endpoint Management technology. VMware uses 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 help secure apps and devices. This also enables devices to receive patches through the OS vendor for the fastest response to vulnerabilities while leaving configuration and app management to IT. |

Highly secure productivity apps: mail, calendar, docs

Workspace ONE™ Cloud includes email, calendar, contacts, and documents that employees want to use while invisible security measures help protect the organization from data leakage by restricting how attachments and files can be edited and shared. Far from a “walled garden,” enterprise discussions, Q&A, content access and other tools allow employees to work collaboratively in near real-time and can be integrated into the apps and tools they already use — moving from productivity to real employee engagement.

| Feature | Description |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Consumer-simple, enterprise-grade secure email app delights consumers, but is designed for business | VMware Boxer® is a faster, smarter, more 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 based on your availability without having to navigate between apps. |
| Advanced email attachment security reduces data leakage | Better secure email and attachments through the use of the VMware Secure Email Gateway that can enforce enterprise encryption, wipe, and “open in” controls keeping attachments more secure |
| Content management app permits line of business to push and manage highly secure content on the device | VMware Content Locker ⁰ mobile app permits IT to deliver files directly to devices across a range of internal repositories and external hosted storage providers to enable the latest, most up-to-date information is at employees' fingertips. |

Data security and endpoint compliance with conditional access

To protect the most sensitive information, Workspace ONE™ Cloud 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 |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 VMware Unified Endpoint Management (rooted devices, app blacklist, geolocation and others). |
| Device management and compliance powered by VMware unified endpoint management technology | 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 VMware policy engine. |
| App and device analytics provide near 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. |

Near real-time app delivery and automation

Workspace ONE™ Cloud takes full advantage of the new capabilities of Windows and uses the industry leading VMware UEM technology to enable desktop administrators to automate application distribution and updates on the fly.

| Feature | Description |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote configuration management enables employees to provision new, shrink-wrapped devices from virtually anywhere | Workspace ONE™ Cloud with VMware configuration eliminates the need for laptop imaging and provides an efficient 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. Automatically connect end users to corporate resources such as Wi-Fi and VPN, and enable highly secure connectivity to backend systems with advanced options for certificate authentication and per-app VPN. |
| Windows software distribution automates software lifecycle management | VMware software distribution enables enterprises to automatically install, update and remove software packages, and also provide 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. 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. |
| Asset tracking provides a single view of corporate-managed devices, wherever they are | Workspace ONE™ Cloud with VMware enables administrators to remotely monitor and manage all devices connected to your enterprise. Because VMware is multitenant, you can manage devices across geographies, business units or other segmentations in a single console and then define, delegate and manage with role-based access controls. |
| Remote assistance makes it simple to support employees | Workspace ONE™ Cloud with VMware 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. |

AT&T professional services

(optional but required for ASD support)

Basic installation and training*

(does not include VMware identity mgr)

AT&T will provide implementation services in a VMware hosted environment with optional integration supported by an VMware Connector in the Customer's data centers and initial deployment of an initial pilot set of devices.

Basic plus installation and training *

(does not include VMware identity mgr)

Basic Plus offer includes all of the features of Basic Installation and Training plus the configuration of the VMware Launcher feature for the setup of shared Android devices.

Premium installation and training services for EMM software

AT&T will provide implementation services that include installation of the VMware Console, an optional Connector and either a Secure Email Gateway or PowerShell Integration for email management and an initial pilot set of devices.

Premium plus installation and training for use of EMM software

Premium Plus Installation and Training Services include all the features of Premium Installation and Training, as well as installation of a Mobile Access Gateway for content management or highly secure browsing, and installation, and configuration.

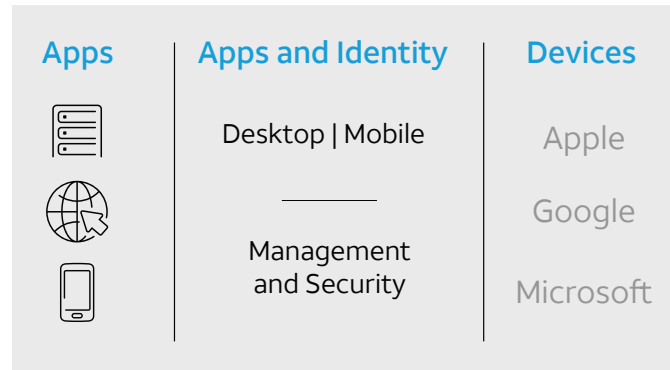
Application Service Desk (ASD)**

(AT&T professional services required)

Application Service Desk Support Plans are provided by the AT&T Global Mobility Applications and Security ("GMAS") ASD organization and are available to Customers that have not previously purchased an EMM Solution from AT&T. The components of these ASD Plans include the following:

- Technical Support
- MACD (moves, adds, changes, disconnects) Administration
- Service Optimization

Monthly recurring charge ("MRC") subscriptions to all VMware Workspace ONE™ Cloud editions include a license plus ASD Support.



Advanced remote administration service plan (optional)

The Advanced Remote Administration Service Plan is a comprehensive program available that is designed for organizations that have limited internal support resources and mobile expertise. AT&T will provide the staff needed to administer Customer's EMM platform and provide an EMM consultant to assist Customer.

The advanced remote administration service includes:

- Device management
- User and group management
- Policy management and compliance
- Application and content management
- Active directory integration
- Certificate management
- Support for EMM integration with email**
- Complex network architecture support
- EMM advanced features support

* Available for existing VMware AirWatch customers only

**AT&T will not provide technical support to end users and will not provide technical support for the applications and/or content that Customer chooses to distribute and which are not included in the Solution's feature list.

Enterprise Mobility Management VMware Workspace ONE™ Cloud



VMware Workspace ONE™ Cloud Product Brief Important Information

General: Workspace ONE™ Cloud as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement"). The Solution is subject to (a) the terms and conditions found at https://www.vmware.com/download/eula/universal_eula.html ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. For government customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms. Except for government customers, Customer must accept the Additional Product Terms on behalf of its end users. Any service discounts, equipment discounts, and/or other discounts set forth in the Qualified Agreement do not apply to the Solution. The Solution may not be available for purchase in all sales channels or in all areas. Additional hardware, software, service and/or network connection may be required to access the Solution. Availability, security, speed, timeliness, accuracy and reliability of service are not guaranteed by AT&T.

Requirements; Technical Information: The Solution is available for use with multiple network service providers and its functionality is limited to certain mobile devices and operating systems. A list of the compatible devices and operating systems is available by contacting an AT&T Account Executive or visit www.att.com/mdm. * With respect to users subscribed to AT&T wireless service, activation of an eligible AT&T data plan with short message service ("SMS") capabilities is required. With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, customer is responsible for ensuring that its applicable end users and the Solution complies with all applicable terms of service of such other wireless carrier(s). All associated voice, messaging and data usage will be subject to the applicable rates and terms of such other wireless carrier(s). Refer to applicable wireless carrier(s) for such rates, terms and conditions. The Solution's administrative interface is accessed via a Web portal and requires a browser with Internet connection. AT&T will not provide technical support to end users. AT&T reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause. All fees paid for the Solution are non-refundable. A minimum of 20 Solution licenses is required for an initial order. Users may download licensed software onto one (1) device per license. If the license is sold on a per user basis, up to five (5) users may use one license.

Reservations: AT&T reserves the right to perform work at a remote location or use, in AT&T's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution. Any warranties related to the Solution that can be passed through under law will be passed through to Customer by AT&T. For government customers, the following applies to the extent not in conflict with the Qualified Agreement: (i) ALL SOFTWARE IS PROVIDED BY AT&T TO CUSTOMER ON AN "AS IS" BASIS; (ii) AT&T disclaims all remedies for claims of infringement by a third party based upon or arising out of customer's or end users' use of the Solution, and (iii) Customer's sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service. For all other customers: (i) VMware, not AT&T, is responsible for any such warranty terms and commitments; (ii) ALL SOFTWARE IS PROVIDED BY AT&T TO CUSTOMER ON AN "AS IS" BASIS; (iii) AT&T disclaims all remedies for claims of infringement by a third party based upon or arising out of customer's or end users' use of the Solution; and (iv) Customer's sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service.

Use of Solution Outside the U.S.: For government customers, see your account representative for additional information regarding use of the Solution outside the US. For other customers, see the Country Specific Provisions in the Solution Service Guide located at http://serviceguidenew.att.com/sg_customPreviewPDFPage?testid=068C0000001fyNEIAY.

Data Privacy: Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world; (ii) third parties who act on AT&T's or AT&T's supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt customer Personal Data in a manner compatible with the Solution. As used herein, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify customer or its end users. Customer is responsible for providing end users with clear notice of AT&T's and Customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the product brief or other sales information that describes the Solution and to AT&T's Privacy Policy at <http://www.att.com/gen/privacy-policy?pid=2506>.

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

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No. 43851vmw-ds-id-mgr-dglt-wkspc1-digital-en-us 7/17

Find out more about VMware Workspace ONE™ Cloud by
visiting: www.att.com/security.

Share this with
your peers

