VMWARE WORKSPACE ONE

Consumer Simple. Enterprise Secure.

AT A GLANCE

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

Workspace ONE is built on the VMware AirWatch® Unified Endpoint Management™ technology and integrates with virtual application delivery (VMware Horizon®) on a common identity framework. With Workspace ONE organizations can now evolve silo-ed cloud 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 enables you to drastically improve experiences and tasks that were previously costly, time consuming, and resource intensive. With Workspace ONE, IT organizations can:

- 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
- Provision a new corporate laptop out of the box, anywhere in the world, from the cloud within minutes

Key Market Trend

The rapid adoption of new 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 they 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 leveraging a new management framework.

What is Workspace ONE

VMware Workspace ONE is the enterprise platform that enables IT to deliver a digital workspace that empowers the workforce to 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 cloud, mobile, web and Windows apps in one unified catalog and includes powerfully integrated email, calendar, file and social collaboration tools 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 AirWatch Unified Endpoint Management technology. Finally, Workspace ONE automates traditional onboarding and 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-simple access to cloud, web, mobile and 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, web, cloud or Windows app. Workspace ONE simplifies application and access management by offering Single Sign-On (SSO) capabilities and support for multi-factor authentication.

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 or real-time delivery with app volumes • Secure sensitive systems of record apps behind a HTML5 proxy by hosting in the datacenter or cloud provider with Horizon Cloud • Deliver complete virtualized managed desktops in the cloud, or in on-premises data centers
Unified App Catalog 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	Lightwave can be implemented and run by a cloud provider. The cloud provider's customers can then use it as a cloud-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 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 integrates identity management and AirWatch Unified 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 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 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 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 platform powered by VMware AirWatch Unified Endpoint Management technology. AirWatch 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 enables 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 Social

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 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.


Boxer


Content Locker


Socialcast

FEATURE	DESCRIPTION
Consumer-simple, Enterprise-secure Email App Delights Consumers but is Designed for Business	VMware Boxer® is 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 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	VMware Content Locker™ mobile app permits IT to deliver files directly to devices across a range of internal repositories and external cloud storage providers to enable the latest, most up-to-date information is at employees fingertips.
Enterprise Chat and Social 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 through Socialcast® by VMware.

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
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 Unified Endpoint Management (rooted devices, app blacklist, geolocation and others).
Device Management and Compliance Powered by AirWatch 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 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 VMware AirWatch® Tunnel™ further segregate traffic from application to specific workloads in the datacenter. This substantially reduces attack vector of malware/ viruses that could do significant harm to the organization.

Real-time App Delivery and Automation

Workspace ONE takes full advantage of the new capabilities of Windows and leverages the industry leading AirWatch UEM technology to enable 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.

LEARN MORE

Find out more about VMware Workspace ONE by visiting: 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), or

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.

FEATURE	DESCRIPTION
Remote Configuration Management Enables 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. Automatically connect end users to corporate resources such as Wi-Fi and VPN, and enable secure connectivity to backend systems with advanced options for certificate authentication and per-app VPN.
Windows Software Distribution Automates Software Lifecycle Management	AirWatch 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.
Virtual Apps and Desktops by Horizon Delivers Secure Hosted Desktops and Apps	Horizon provides secure hosted virtual apps and desktops enabling 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; enabling them the flexibility to be productive wherever they need to.
Asset Tracking Provides a Single View of Corporate-managed Devices, Wherever They Are	Workspace ONE with AirWatch enables administrators to remotely monitor and manage all devices connected to your enterprise. Because AirWatch 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 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.

vmware®

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