VMware Workspace ONE

Consumer simple. Enterprise secure.

AT A GLANCE

VMware Workspace ONE® is an intelligence-driven digital workspace platform that simply and securely delivers and manages any app on any device by integrating access control, application management, and multiplatform endpoint management. It is available as an annual cloud subscription or a perpetual on-premises license.

Workspace ONE integrates unified endpoint management technology (formerly VMware AirWatch®) with virtual application delivery (VMware Horizon®) on a common identity framework. With Workspace ONE, organizations can now evolve siloed 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 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
- Get insights and automation capabilities across your entire digital workspace environment

Key market trend

The rapid adoption of new modern applications—such as software-as-a-service (SaaS) apps and 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. 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. To be productive whenever and wherever, employees have gone around traditional rigid and old policies. Organizations face the critical decision to either ignore these trends at the peril of unintended security breaches or embrace a new way of working, leveraging a new management framework.

What is VMware Workspace ONE?

VMware Workspace ONE is the intelligence-driven digital workspace platform that simply and securely delivers and manages any app on any device by integrating access control, application management, and multiplatform endpoint management. It begins with consumer-simple, single sign-on (SSO) 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's 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 unified endpoint management (UEM) technology. Workspace ONE automates traditional onboarding and laptop and mobile device configuration, and delivers real-time application lifecycle management that bridges legacy enterprise client-server apps to the mobile cloud era. The Workspace ONE platform is powered by intelligence and uniquely combines workspace data aggregation and correlation to deliver integrated insights and automation that help organizations manage complexity and security without compromising on user experience.

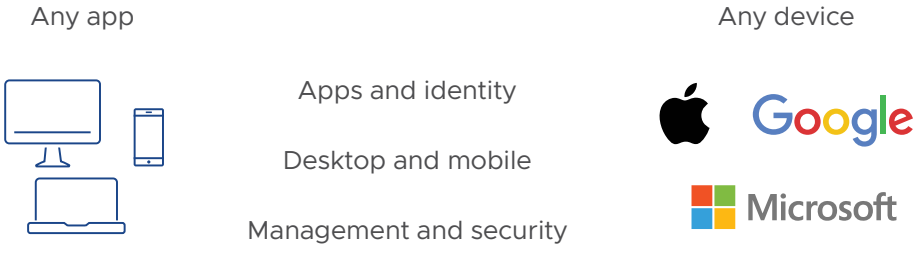


FIGURE 1: VMware Workspace ONE simply and securely delivers any app on any device.

Key capabilities

With consumer-simple access to cloud, web, mobile, Windows, and Mac apps, onboarding new apps and new employees couldn't be easier. Once authenticated through the VMware Workspace ONE Intelligent Hub app, employees can instantly access their personalized enterprise app catalog and subscribe to virtually any mobile, Windows, and Mac apps. Workspace ONE simplifies application and access management by offering SSO capabilities and support for multifactor authentication.

CAPABILITY	DESCRIPTION
Deliver any application from the latest mobile cloud apps to legacy enterprise apps	An enterprise app catalog delivers simple SSO access to the right apps to any device, including: • Internal web apps through a secured browser and seamless VPN tunnel • SaaS apps with SAML or OpenID Connect–based SSO • Native public mobile apps through brokerage of public app stores • Modern Windows apps and macOS apps • Legacy Windows apps through MSI package delivery, real-time delivery with VMware App Volumes™, and published virtually in the on-premises data center or in the public cloud • Secure sensitive systems of record apps behind a HTML5 proxy by hosting in the data center or cloud provider with VMware Horizon Cloud Service™ • Complete virtualized managed desktops in the cloud or in on-premises data centers
Unified app catalog transforms employee onboarding	Simply downloading the Workspace ONE Intelligent Hub app on iOS or Android provides employees with a complete, self-service enterprise app catalog that can be easily customized and branded for your company. The Workspace ONE Intelligent Hub app provides employees with native apps that can be installed.
SSO that federates even the most complex on-premises Active Directory topologies	Workspace ONE integrates with Active Directory, LDAP directories, its own internal directory, and third-party identity providers to simplify access to all apps across your organization for all your users.
Password-free 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 UEM to create an industry-leading, seamless user experience across desktop, web, and mobile.

CAPABILITY	DESCRIPTION
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.

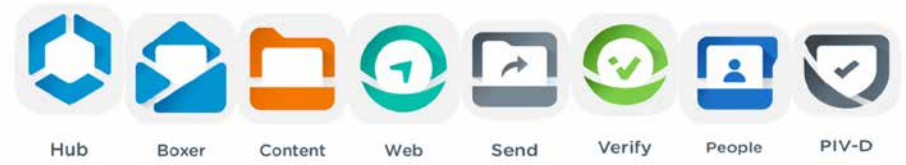
Choice to use any device: BYOD or corporate owned

The architecture you deploy today must work with devices not yet invented. From wearables to 3D graphics workstations, keeping employees productive means their apps must 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. 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 bring-your-own-device (BYOD) programs while getting IT out of the device business.

CAPABILITY	DESCRIPTION
Adaptive management designed to maximize adoption for even the most privacy-sensitive employees	The Workspace ONE Intelligent Hub app enables adaptive management, so employees can comfortably adopt BYOD programs by deciding 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 Workspace ONE–powered UEM that leverages enterprise mobile management APIs from Apple iOS and OS X, 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: Catalog, mail, calendar, contacts, docs, and more

Workspace ONE secure productivity apps include catalog, email, calendar, contacts, content, authentication access, and more. Designed for business users, Workspace ONE apps have a wealth of time-saving features employees want to use, and industry-leading, enterprise-grade security to protect sensitive corporate data. Enable users with frictionless, secure access to the apps, tools, and content they require to get work done from anywhere.



CAPABILITY	DESCRIPTION
Empower employees with an enhanced catalog and progressive value	Workspace ONE Intelligent Hub is a single destination where employees have unified onboarding, catalog, and an enhanced user experience to access optional Hub Services[1] such as People, Notifications, and Home. Core capabilities of the Workspace ONE platform are leveraged to deliver a secure, consistent, cross-platform experience. Hub Services include: • Notifications – Provides IT-administered push and in-app notifications, and custom notifications. • People – Enables users to quickly look up colleagues via an employee directory; includes organization chart with name, email, phone, and search. • Home – Gives users access to company resources by embedding an intranet or company portal.
Contextual actions and notifications on mobile	Workspace ONE mobile flows is the VMware extensibility service that allows IT to surface contextual notifications and alerts with information and actions against business systems. Workspace ONE mobile flows allows employees to be productive on the go by easily completing actions such as customer relationship management (CRM) updates, ticket management, and approvals. All of these actions can be completed without moving between multiple applications. Workspace ONE mobile flows can be enabled in Workspace ONE Intelligent Hub and Workspace ONE Boxer.
Consumer-simple, enterprise-secure email application designed for more productive employees on the go	Workspace ONE Boxer is an intuitive, all-in-one email, calendar, and contacts app stacked with features specifically for business users on the go. Workspace ONE Boxer is equipped with industry-leading, enterprise-grade security and supports Exchange, Outlook, G Suite, Yahoo, Hotmail, iCloud, Office 365, IMAP, and POP3 mail accounts. With integrations to content services such as Dropbox, Box, and Evernote, Workspace ONE Boxer makes it easy to stay organized.

CAPABILITY	DESCRIPTION
Integrated calendar and contacts with email makes it simple to manage	By integrating email, calendar, and contacts, employees no longer need to move out of the email app when checking their calendar, looking up a colleague, and more.
Advanced email attachment security reduces data leakage	Secure email and attachments through the use of the AirWatch Secure Email Gateway™, which enforces enterprise encryption, wipe, and open-in controls to keep attachments secure.
Content management app permits line of business to push and manage secure content on the device	The Workspace ONE Content application gives admins the power to distribute files directly to devices, users, groups, and more across a range of internal repositories and external cloud storage providers, ensuring the latest, most up-to-date information is at employees' fingertips.

Zero-trust 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.

CAPABILITY	DESCRIPTION
Combines access management and mobility management	Workspace ONE controls access to mobile, web, SaaS, Windows, Mac, Chrome, and virtual apps on a per-application basis. Workspace ONE examines authentication context such as authentication method, user group, target app, network location, and device state to automate access decisions and keep corporate data safe.
Device management and compliance powered by UEM technology	Only the right devices get access to data with real-time, continuous device compliance checks. Workspace ONE uses UEM technology to ensure that devices comply with IT policies on rooted or jailbroken devices, whitelisted and blacklisted apps, open-in app restrictions, and other policies enforced through the AirWatch policy engine.
Intelligence-driven insights and automation to increase the level of security hygiene and compliance across the entire environment	With deep insights into the entire digital workspace environment and automation capabilities, Workspace ONE can help raise the level of security hygiene across your organization. Quickly identify out-of-compliance devices, apply the latest security patches, and automate access control policies based on user behavior.

1. Hub Services requires version compatibility and may have a dependency on VMware Identity Manager™. Experience may vary depending on the capabilities enabled.

CAPABILITY	DESCRIPTION
Integrated insights for your entire digital workspace	Workspace ONE powered by intelligence aggregates and correlates device, application, and user data together in one place to give you a complete view of your entire digital workspace environment. Keep an eye on the data that matters to you most with preset dashboards that can be customized to meet your unique needs. Visualize the evolution of your environment's security risks, app deployments, device management, app engagement, and patch rollouts.
Comprehensive and predictive security based on a common framework of trust	Available as an added capability, VMware NSX® with Workspace ONE Tunnel further segregates traffic from applications to specific workloads in the data center. This substantially reduces the attack vector of malware and viruses that could do significant harm to the organization.

Real-time app delivery and automation

Workspace ONE takes full advantage of new Windows capabilities and leverages industry-leading 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.

Workspace ONE eases the transition to Windows 10 modern management with co-management capabilities for Microsoft System Center Configuration Manager (SCCM).

CAPABILITY	DESCRIPTION
Remote configuration management enables employees to provision new, shrink-wrapped devices from anywhere	Workspace ONE UEM 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 back-end systems with advanced options for certificate authentication and per-app VPN.
Windows software distribution automates software lifecycle management	Workspace ONE 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.

LEARN MORE

Find out more about VMware Workspace ONE by visiting *vmware.com/products/workspace-one.html*.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller.

CAPABILITY	DESCRIPTION
Fast and easy transition to Windows 10 modern management with Workspace ONE AirLift	With the ability to co-manage Windows 10 devices, the Workspace ONE AirLift server-side connector to Microsoft SCCM eases the transition efforts to modern management. Workspace ONE AirLift allows customers to migrate high-pain PC lifecycle management (PCLM) workloads—such as onboarding, patching, software distribution, and remote user support—to a more cost-efficient and secure cloud-based modern management model. Workspace ONE AirLift makes the transition from SCCM to modern management seamless and non-disruptive, and helps customers get to lower Windows PC total cost of ownership quickly. By easing the journey to Windows 10 with co-management, Workspace ONE AirLift meets customers wherever they are on their Windows 10 modern management journey.
Virtual apps and desktops by Horizon deliver 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 they are using, providing them with the flexibility to be productive.
App analytics and automation	With the ability to monitor app performance, app adoption, and user behavior across the organization, Workspace ONE provides IT with capabilities to quickly resolve app-related issues, reduce escalations, and improve user experience. Easily analyze and quantify how app performance affects app adoption, and quickly discover the most used apps to quantify ROI of app deployments. The intelligence-driven Workspace ONE comes with automation capabilities that help IT manage the entire digital workspace more efficiently by creating rules that take actions based on a rich set of parameters. Easily automate the deployment of applications, OS patches, and software updates, and create rules to quickly bring apps back to a stable state if they don't perform as expected.
Asset tracking provides a single view of corporate-managed devices, wherever they are	Workspace ONE 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 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.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 241264aq-ds-workspace-one-uslet 5/19