REVISED 5 NOVEMBER 2018

BUSINESS DRIVERS AND USE CASES

vmware®

Table of Contents

VMware Workspace ONE Cloud-Based Reference Architecture - Business Drivers and Use Cases

Business Drivers and Use Cases

An end-user-computing (EUC) solution based on VMware Workspace ONE® and VMware Horizon® Cloud Service™ on Microsoft Azure can address a wide-ranging set of business requirements and use cases. In this reference architecture, the solution targets the most common requirements and use cases seen in customer deployments to date.

Addressing Business Requirements

A technology solution should directly address the critical business requirements that justify the time and expense of putting a new set of capabilities in place. Each and every design choice should center on a specific business requirement. Business requirements could be driven by the end user or by the team deploying EUC services.

The following common key business drivers can be addressed by the Workspace ONE solution.

Mobile Access

Requirement definition: Provide greater business mobility by providing mobile access to modern and legacy applications on laptops, tablets, and smartphones.

Workspace ONE solution: Workspace ONE provides a straightforward, enterprise-secure method of accessing all types of applications that end users need from a wide variety of platforms.

- It is the first solution that brings together identity, device and application management, a unified application catalog, and mobile productivity.
- VMware Horizon® Client™ technology supports all mobile and laptop devices as well as common operating systems.

Fast Provisioning and Access

Requirement definition: Allow fast provisioning of and secure access to line-of-business applications for internal users and third-party suppliers, while reducing physical device management overhead.

Workspace ONE solution: Workspace ONE can support a wide range of device access scenarios, simplifying the onboarding of end-user devices.

- Adaptive management allows a user to download an app from a public app store and access some published applications. If a user needs to access more privileged apps or corporate data, they are prompted to enroll their device from within the app itself rather than through an agent,

such as the VMware Workspace ONE® Intelligent Hub app.

- Horizon Cloud Service on Microsoft Azure delivers feature-rich virtual desktops and applications using a purpose-built cloud platform. This makes it easy to deliver virtualized Windows desktops and applications to any device, anytime. IT can save time getting up and running with an easy deployment process, simplified management, and a flexible subscription model.

Reduced Application Management Effort

Requirement definition: Reduce application management overhead and reduce application provisioning time.

Workspace ONE solution: Workspace ONE provides end users with a single application catalog for native mobile, SaaS, and virtualized applications and improves application management.

- Workspace ONE provides a consolidated view of all applications hosted across different services with a consistent user experience across all platforms.
- With Horizon Cloud Service on Microsoft Azure, Windows-based applications are delivered centrally, either through virtual desktops or as RDSH-published applications. These can be centrally managed, allowing for access control, fast updates, and version control.
- VMware Workspace ONE® Intelligence™ gives IT administrators insights into app deployments and app engagement. Analysis of user behavior combined with automation capabilities allow for quick resolution of issues, reduced escalations, and increased employee productivity.

Centralized and Secure Data and Devices

Requirement definition: Centralize management and security of corporate data and devices to meet compliance standards.

Workspace ONE solution: All components are designed with security as a top priority.

- VMware Workspace ONE® UEM (powered by AirWatch) provides aggregation of content repositories, including SharePoint, network file shares, and cloud services. Files from these repositories can be synced to the VMware Workspace ONE® Content app for viewing and secure editing.
- Workspace ONE UEM policies can also be established to prevent distribution of corporate files, control where files can be opened and by which apps, and prevent such functions as copying and pasting into other apps, or printing.
- Horizon Cloud Service on Microsoft Azure is the platform for delivering virtual desktops or published applications where user data, applications, and desktop activity do not leave the data center. Additional Horizon Cloud and VMware User Environment Manager™ policies restrict and control user access to data.

- Workspace ONE Intelligence detects and remediates security vulnerabilities at scale. Quickly identify out-of-compliance devices and automate access control policies based on user behavior.

Comprehensive and Flexible Platform for Corporate-Owned or BYOD Strategies

Requirement definition: Allow users to access applications, especially the Microsoft Office 365 suite, and corporate data from their own devices.

Workspace ONE solution: Workspace ONE can meet the device-management challenges introduced by the flexibility demands of BYOD.

- Workspace ONE and features like adaptive management simplify end-user enrollment and empower application access in a secure fashion to drive user adoption.
- With Horizon Cloud Service on Microsoft Azure, moving to a virtual desktop and published application solution removes the need to manage client devices, applications, or images. A thin client, zero client, or employee-owned device can be used in conjunction with Horizon Client. IT now has the luxury of managing single images of virtual desktops in the data center.
- Get insights into device and application usage over time with Workspace ONE Intelligence to enable optimizing resource allocation and license renewals. The built-in automation capabilities can tag devices that have been inactive for specific periods of time or notify users when their devices need to be replaced.

Reduced Support Calls and Improved Time to Resolution

Requirement definition: Simplify and secure access to applications to speed up root-cause analysis and resolution of user issues.

Workspace ONE solution: Workspace ONE provides single-sign-on (SSO) capabilities to a wide range of platforms and applications. By leveraging SSO technology, password resets are unnecessary.

- VMware Identity Manager™ provides a self-service single point of access to all applications and, in conjunction with True SSO, provides a platform for SSO. Users no longer need to remember passwords or request applications through support calls.
- Both Workspace ONE UEM and VMware Identity Manager include dashboards and analytics to help administrators understand what a profile of application access and device deployment looks like in the enterprise. With greater knowledge of which applications users are accessing, administrators can more quickly identify issues with licensing or potential attempted malicious activities against enterprise applications.
- Workspace ONE Intelligence ensures that end users get the best mobile application experience by keeping an eye on app performance, app engagement, and user behavior. With detailed insights around devices, networks, operating systems, geolocation, connectivity state,

and current app version, LOB owners can optimize their apps for their unique audience and ensure an optimal user experience.

Use Cases

Use cases drive the design for any EUC solution and dictate which technologies are deployed to meet user requirements. Use cases can be thought of as common user scenarios. For example, a finance or marketing user might be considered a “normal office worker” use case.

Designing an environment includes building out the functional definitions for the use cases and their requirements. We define typical use cases that are also adaptable to cover most scenarios. We also define services to deliver the requirements of those use cases.

Workspace ONE Use Cases

This reference architecture includes the following common Workspace ONE use cases.

Table: Workspace ONE Common Use Cases

Use Case	Description
Mobile Task-Based Worker	Users who typically use a mobile device for a single task through a single application. - Mobile device is highly managed and used for only a small number of tasks, such as inventory control, product delivery, or retail applications. - Communications tools, such as email, might be restricted to only sending and receiving email with internal parties. - Device is typically locked down from accessing unnecessary applications. Access to public app stores is restricted or removed entirely. - Device location, full device wipe, and other features are typically used.
Mobile Knowledge Worker	Many roles fit this profile, such as a hospital clinician or an employee in finance, marketing, HR, health benefits, approvals, and travel. - These workers use their own personal device (BYOD), a corporate device they personally manage, or a managed corporate device with low restrictions. - Users are typically allowed to access email, including personal email, along with public app stores for personal apps. - Device is likely subject to information controls over corporate data, such as data loss prevention (DLP) controls, managed email, managed content, and secure browsing. - Users need access to SaaS-based applications for HR, finance, health benefits, approvals, and travel, as well as native applications where those applications are available. - Device is a great candidate for SSO because the need to access many diverse applications and passwords becomes an issue for users and the helpdesk. - Privacy is typically a concern that might prevent device enrollment, so adaptive management and clear communication regarding the data gathered and reported to the Workspace ONE UEM service is important to encourage adoption.
Contractor	Contractors might require access to specific line-of-business applications, typically from a remote or mobile location. - Users likely need access to an organization’s systems for performing specific functions and applications, but access might be for a finite time period or to a subset of resources and applications. - When the contractor is no longer affiliated with the organization, all access to systems must be terminated immediately and completely, and all corporate information must be removed from the device. - Users typically need access to published applications or VDI-based desktops, and might use multiple devices not under company control to do so. Devices include mobile devices as well as browser-based devices.

Horizon Cloud Service on Microsoft Azure Use Cases

This reference architecture includes the following Horizon Cloud Service on Microsoft Azure use cases.

Table: Horizon Cloud Service on Microsoft Azure Common Use Cases

Use Case	Description
Static Task Worker	These workers are typically fixed to a specific location with no remote access requirement. Some examples include call center worker, administration worker, and retail user. A static task worker: - Uses a small number of Microsoft Windows applications. They do not install their own applications and do not require SaaS application access. - Might require location-aware printing.
Multimedia Designer / Engineer	These users might require GPU-accelerated applications, which have intensive CPU or memory workloads, or both. Examples are CAD/CAM designers, architects, video editors and reviewers, graphic artists, and game designers. A multimedia designer: - Has a GPU requirement with API support for DirectX 10+, video playback, and Flash content. - Mainly uses applications from a corporate location but might access applications from mobile locations. - Might require two-factor authentication when accessing applications remotely.
Mobile Knowledge Worker	This worker could be a hospital clinician, a company employee, or have a finance or marketing role. This is a catch-all corporate use case. A mobile knowledge worker: - Mainly uses applications from a corporate location but might access applications from mobile locations. - Uses a large number of core and departmental applications but does not install their own applications. Requires SaaS application access. - Requires access to USB devices. - Might require location-aware printing. - Might require two-factor authentication when accessing applications remotely.
Contractor	External contractors usually require access to specific line-of-business applications, typically from a remote or mobile location. A contractor: - Mainly uses applications from a corporate location but might access applications from mobile locations. - Uses a subset of core and departmental applications based on the project they are working on. Might require SaaS application access. - Has restricted access to clipboard, USB devices, and so on. - Requires two-factor authentication when accessing applications remotely.

Recovery Use Case Requirements

When disaster recovery is being considered, the main emphasis falls on the availability and recoverability requirements of the differing types of users. For each of the previously defined use cases and their requirements, we can define the recovery requirements.

With cloud-based services, such as Workspace ONE UEM, VMware Identity Manager, and Workspace ONE Intelligence, availability is delivered as part of the overall service SLA. For VMware

Horizon–based services, the availability portion of the solution might have dependencies on applications, personalization, and user data to deliver a full experience to the user in a recovery site. Consider carefully what type of experience will be offered in a recovery scenario and how that matches the business and user requirements.

This reference architecture discusses two common disaster recovery classifications: active/active and active/passive. When choosing between these recovery classifications, which are described in the following table, be sure to view the scenario from the user's perspective.

Table: Disaster Recovery Classifications

Use Case and Recoverability Objective	Description
Active/Passive RTO = Medium RPO = Medium	- Users normally work in a single office location. - Service consumed is pinned to a single data center. - Failover of the service to the second data center ensures business continuity.
Active/Active RTO = Low RPO = Low	- Users require the lowest possible recovery time for the service (for example, health worker). - Mobile users might roam from continent to continent. - Users need to get served from the nearest geographical data center per continent. - Service consumed is available in both primary and secondary data centers without manual intervention.

With a VMware Horizon–based service, the recovery service should aim to offer an equivalent experience to the user. Usually the service at the secondary site is constructed from the same or similar parts and components as the primary site service. Consideration must be given to data replication and the speed and frequency at which data from the primary site can be replicated to the recovery site. This can influence which type of recovery service is offered, how quickly a recovery service can become available to users, and how complete that recovery service might be.

The RTO (recovery time objective) is defined as the time it takes to recover a given service. RPO (recovery point objective) is the maximum period in which data might be lost. Low targets are defined as 30- to 60-second estimates. Medium targets are estimated at 45–60 minutes. These targets depend on the environment and the components included in the recovery service.

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