Workspace ONE Combined with Microsoft E3

How does Workspace ONE add value to Microsoft E3?

Q. What operating systems are supported by Workspace ONE UEM?

A. VMware Workspace ONE® supports many operating systems for both configuration and application lifecycle management including but not limited to Windows 10, iOS, macOS, Android, and ChromeOS. Workspace ONE UEM has broad support for Android rugged devices with deep API integration with vendors such as Zebra, Samsung, and Honeywell. Workspace ONE UEM provides support for Android for Enterprise devices including fully managed corporate devices.

Q. I want my end users to be productive. How does Workspace ONE improve end-user experience?

A. From an end-user perspective, Workspace ONE has been meticulously designed to offer parity across all supported operating systems. From an IT perspective, you can take advantage of all the different "Out of Box" experiences offered by the operating system vendors to distribute new devices directly to the end user. VMware Workspace ONE® Intelligent Hub becomes your single application to consume corporate data, regardless of the device type or operating system.

Q. How does Workspace ONE enable best-in-class Data Loss Prevention (DLP)?

A. Workspace ONE delivers the best-in-class DLP capability by integrating Intune App Protection with the DLP controls of the operating system. This ensures that whether the application is part of the Microsoft Office suite or a third-party application, you can build coherent DLP policies across your entire suite of apps, for example, native email attachments opened into the Office applications.

Q. Does Workspace ONE add conditional access and device health capability?

A. Workspace ONE provides feature-rich conditional access controls to ensure that only healthy devices, that are known, patched to the right OS version, and used in the right locations, can consume application data. Workspace ONE understands the context of the device, the identity of the user, and the management level, for example, BYOD vs. corporate.

Q. How can I ensure that BYOD devices can only consume application data based on the management posture of the device?

A. Workspace ONE uses adaptive management to seamlessly enhance the security and management of a device based on the type of data the end user wants to consume. For instance, you can allow a device to consume email data with zero or light management; for security-critical data, the device will automatically prompt the user to elevate the management rights and thus ensure that the data is secure.

Q. Can Workspace ONE accelerate Windows 10 UEM (modern) management?

A. Workspace ONE UEM accelerates Windows 10 management by removing the complexity of having to audit and evaluate all your existing GPO policies, application distribution, and client configuration. By providing complete support for GPO, modern management CSPs, and near parity for application distribution with SCCM, you can migrate to Workspace ONE UEM silently without end-user interruption deploying your existing policies and configuration. Workspace ONE will also ensure that you can encrypt the hard disk using BitLocker and escrow the recovery keys for future use.

Q. What features does Workspace ONE add to my security infrastructure?

A. VMware understands that security is typically not solvable by a single vendor. Workspace ONE Intelligence implements a Trust Network of partners that ingests data from third parties to create a single infrastructure layer that provides client health reporting, automation, and proactive security. From an administrator perspective, Workspace ONE Intelligence alerts you when a security event is detected, automatically quarantines unhealthy devices, and reports in real time the devices that are affected.

Q. We distribute applications with SCCM. Can Workspace ONE integrate with SCCM and is it officially supported?

A. Workspace ONE UEM integrates with SCCM to silently synchronize applications into UEM management. By using VMware Workspace ONE® AirLift, you don't need to add your applications to two separate consoles. Simply map your SCCM collections to your Workspace ONE Smart Groups and you can start distributing applications from Workspace ONE UEM to Windows 10.

Q. We're migrating AD to Azure Active Directory (AAD). Can Workspace ONE integrate with AAD?

A. Workspace ONE integrates with AAD for both net-new users and users synchronized from Active Directory. Workspace ONE conditional access prevents unhealthy devices from connecting to AAD prior to authentication. Workspace ONE has direct integration with AAD conditional access controls for the Office 365 applications for unmanaged devices.

Q. Can Workspace ONE integrate with Azure Information Protection (AIP) and Azure Rights Management (RMS)?

A. Workspace ONE Integrates with AIP and RMS to ensure that your corporate data is protected and can only be viewed by authorized recipients. Both AIP and RMS are supported in the VMware productivity suite, including VMware Workspace ONE® Content and VMware Workspace ONE® Boxer.

Q. Our chosen multi-factor (MFA) solution is not Microsoft Authenticator. What MFA solutions does Workspace ONE integrate with?

A. Workspace ONE can leverage any RADIUS- or SAML-based multi-factor authentication solution. You can extend your MFA investment by using the capability of Workspace ONE Conditional Access to add additional security checkpoints before a device can consume corporate data.

Q. What reporting capability does Workspace ONE deliver?

A. Workspace ONE Intelligence supports iOS, macOS, Windows 10, Android, and ChromeOS. You can build your own custom dashboards and reports based on the information you need to perform your role. For instance, if you are interested in the patch level of your devices, you can build a report that illustrates the different versions of an operating system in your infrastructure and the associated upgrade history. If you are distributing applications, Workspace ONE Intelligence will highlight any potential app compatibility issues.

Q. How does Workspace ONE Intelligence differ from the security capabilities included in Microsoft EM+S E5?

A. Workspace ONE Intelligence has been designed to understand all the supported operating systems of UEM management, tightly integrated with conditional access. It can ingest data from the Trust Network of partners to automate the prevention of unhealthy devices from connecting to all corporate applications. For instance, if NIST releases a CVE that affects your Windows 10 devices, Intelligence automation instantly alerts the admin, provides quarantine controls for the affected devices, and generates appropriate service desk tickets. Microsoft focuses on its own technology disregarding macOS, iOS, and Android. Workspace ONE Intelligence is any device type we support.

Learn more about how VMware Workspace ONE enhances Microsoft E3 at www.vmware.com/products/workspace-one.html.