SELECTING A DIGITAL WORKSPACE SOLUTION

Technical Buyer's Guide

vmware®

Table of Contents

About This Guide

This paper provides technical and comparative guidance for selecting and purchasing a digital workspace solution. The intended audience for this paper is technical IT professionals seeking to understand the requirements for digital transformation and how solutions compare based on 32 key capabilities. Technical decision-makers and others will find the insights presented here helpful for selecting the most suitable digital workspace solution.

How to Be Competitive in the Era of the Digital Workspace

The landscape of enterprise IT is evolving. Traditional silos such as Telecom, Network, Desktop, and Security are combining to meet today's business needs. Typically, Telecom moves into the new era of mobility, followed by integration with Networking teams, and then the convergence of the Mobility and Desktop teams. In addressing this shifting paradigm, a holistic approach is required to support different platform types, security requirements, productivity, and ease of use that drive user adoption and privacy.

Countless organizations are deploying digital workspace solutions to meet the demands of today's mobile end users and the IT administrators that support them. The goal is to empower users to work from anywhere, on any device—mobile or laptop—at any time. However, architecting a secure, seamless, scalable digital workspace solution is not necessarily easy. The comparative information presented in this paper can help uncover which solution is the best choice for your needs.

More and more organizations are turning to technology to help them provide easier-to-use productivity tools, respond to customer inquiries faster, and save money while so doing. Everyone from the most sophisticated high-tech firm to the small business selling cupcakes relies on technology to reach their customers and enable their workforce. The digital transformation is a natural evolution of the tools and processes used to run all types of businesses all around the world. Selecting the best partner for your digital workspace becomes job number one in today's competitive economy.

The information presented here is organized into four categories:

1. **Proof-of-Concept capabilities** are required in order for solutions to qualify as unified endpoint management and digital workspace transformation.
2. **Enterprise capabilities** are required for production deployment.
3. **Line-of-Business capabilities** satisfy a broad set of use cases that support all types of users.
4. **Strategic capabilities** support expanded use cases and transform how work is accomplished by end users and administrators.

Comparing Capabilities

To compare VMware Workspace ONE™ to other providers' solutions, 32 categories of capabilities were examined. These capabilities fall into four deployment categories:

1. **Proof-of-Concept (POC) capabilities** are baseline functions required for the solutions to be evaluated as a digital workspace transformation initiative.
2. **Enterprise capabilities** are the features and functions required for production deployment. These capabilities support integrations to Enterprise infrastructure.
3. **Line-of-Business (LOB) capabilities** satisfy a broad set of use cases that support all types of users. These capabilities support the LOB use cases and the systems and apps they require.
4. **Strategic capabilities** transform how work is accomplished by end users and administrators. These capabilities support long-term platform requirements for digital transformation.

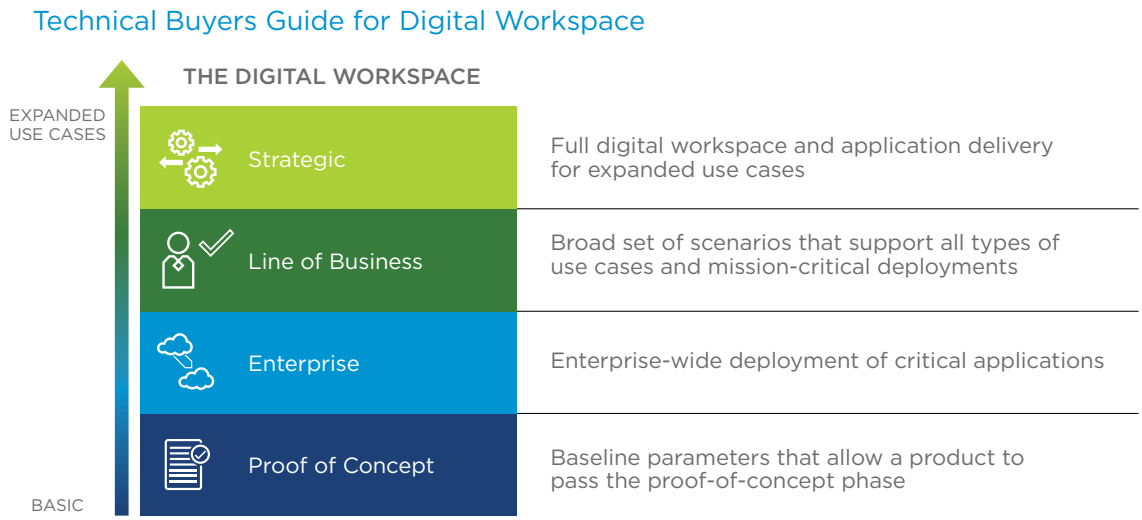

Figure 1: Digital Workspace Use Cases

The following sections discuss differentiating capabilities within the four categories of decision criteria.

Proof of Concept

The first and most basic layer of technical requirements is represented by standard mobile device management (MDM) and mobile application management (MAM). Expanding from there, we also include the following requirements:

- Simplified email configuration and management of corporate content to enforce data loss prevention (DLP) policies
- Basic auditing and reporting for regulatory, industry, and governmental compliance
- Publishing apps via an app catalog – For public apps as well as for managing internally developed and third-party apps
- Basic certificate management – Provides better user experience with increased security in publishing certificates to devices for user authentication to apps, mail, and endpoints
- Pushing configuration and personas to devices
- Secure posture for lost, stolen, or departing employees' devices
- Management of Office 365 apps
- User management or integration to existing user management systems

POC capabilities are common among all vendors surveyed, with differences in the solutions' sophistication and the advanced features they provide. Most vendors in the mobile management industry can provide varying degrees of these capabilities. Differentiation exists for the industry leader, VMware Workspace ONE, but most solutions are optimized to pass this proof-of-concept (POC) test. Purchasing a solution based solely on these features will satisfy POC requirements, but could result in failure to meet the needs of a broader, more challenging, enterprise-wide deployment. Buyer beware of choosing the lowest priced or "free" solution that meets only these requirements. Look beyond the basics and up the sophistication ladder for a more secure and future-proof solution.

Enterprise

The next layer of requirements is where significant differentiation between vendors exists. Fundamental production capabilities comprise this layer almost exclusively. It is rare that an organization relies on a single vendor for their entire stack. Some IT departments are motivated to select best-of-breed, others are obligated to find the best value, and still others look for technology leaders and visionaries. Enterprise integration across vendors is imperative for production deployments. Other mission-critical requirements:

- Multi-tenancy – Provides a flexible, orthogonal structure to absorb the fragmentation of different infrastructure technologies, and the flexibility to maintain global control of your deployments by geography, business unit, department, use case, or any combination.
- Native App configuration – Eliminates the burden of first-time setup of site URLs, group IDs, and other application-specific configurations .
- Full lifecycle certificate management to issue, revoke, and automatically renew certificates on devices from MSCA sources and other third-party and cloud-based certificate authorities such as Symantec, Entrust, Open Trust, Verisign, RSA, Global Sign, SecureAuth, Gleas, and others.
- Ease of scalability – Applies to the number of devices under management and to the manageability and administrative burden as organizations scale to tens and hundreds of thousands of devices.
- Consumer simplicity and a consistent experience across all platforms including native apps, web apps, and remote apps on any device – Key end-user demands.
- Ability to set compliance policies that will automatically apply a list of escalating and time-based configurable actions – Protect corporate apps, accounts, data, and access.

This set of capabilities is sometimes evaluated in the vendor selection process, but many times it is missed. Then, the importance of these features is discovered during a production rollout. If the "free" solution was initially selected, it is oftentimes during this phase that a re-evaluation of the solution occurs, approximately 3–6 months after a purchasing decision has been made. Buyer's remorse is often experienced at the Fundamental capability level.

Line of Business

The third layer of capabilities satisfies unique customer requirements and specific use cases. These requirements may include integrations between a broad ecosystem of partners such as Apple, Google, Microsoft, Samsung, Lenovo, Motorola, Zebra, and others. There may be a specific use case that hasn't been implemented before that requires special attention and knowledgeable resources. Some organizations need laptop management and others need to seamlessly pass mobile devices from one shift worker to another, requiring over-the-air (OTA) (re)provisioning. In some cases, security and compliance certifications might require choosing a platform that is part of the FedRAMP package, meets NIAP MDM standards for iOS or Android, and leverages certificate pinning.

Other organizations may be developing apps and need to include MDM and MAM capabilities into all their apps using a common SDK framework or leverage app wrapping. The next generation of software distribution may be required for provisioning apps to Windows 10 because there is a desire to move away from legacy imaging by managing Windows 10 in a modern way. Rugged device management doesn't have to include a separate solution. The top providers in the market include rugged devices for a seamless management experience. Every customer has unique uses cases or requirements that fall into one of these capabilities.

Strategic

The final layer of requirements is also the most strategic layer. This is the point that encompasses all the underlying technology to complete the digital workspace transformation. This level includes:

- Insights and analytics to better understand how organizations can enable operational efficiencies and drive stronger security.
- Automated Adaptive Management – Gives end users access to apps, data, and remote services immediately without the need for any control at the app or device layer. If an end user requires access to company confidential or sensitive data such as a Human Resources app or design documentation, Adaptive Management will automatically guide the user through a quick registration of the device, providing secure access and enforcing data loss prevention (DLP), for example, with a Workspace ONE services profile. Immediate access to apps without taking control of the personal device is critical for a bring-your-own (BYO) implementation where privacy is a priority.
- The generic capability of accessing critical Win32 apps and desktops on any non-Windows device.
- Enterprise-wide capabilities integrating and providing a unified VDI experience with app layering through, for example, VMware Horizon® and VMware App Volumes™.
- Custom branding provides an important method for establishing an organization's identity with end users and guaranteeing a specific user experience.
- Universal SSO provides access to all apps, for example, Office 365, native apps, web apps, and legacy apps across multiple platforms such as Windows, iOS, Android, and Chrome. It supports different app types that have differing directories and differing authentication requirements.
- Conditional access gives IT a flexible security model that can detect who, what, where and require the appropriate level of authentication. For example, if a user is in the office on their domain-joined computer, the platform will allow access. If the same user is attempting to log in from a non-corporate-controlled site such as a coffee shop on their Android tablet, the platform should require two-factor authentication. Then, if the same user attempts to log in thousands of miles away from the first location a few minutes later (physically impossible to do), the access is blocked.

These requirements comprise the critical enterprise criteria for a secure, easy-to-maintain digital workspace platform that will delight even the most discerning end users.

Comparing Basic Capabilities

VMware Workspace ONE has significant advantages over Microsoft EM+S in three key areas in the basic capabilities category: MDM/MAM, email management, and Office 365 management.

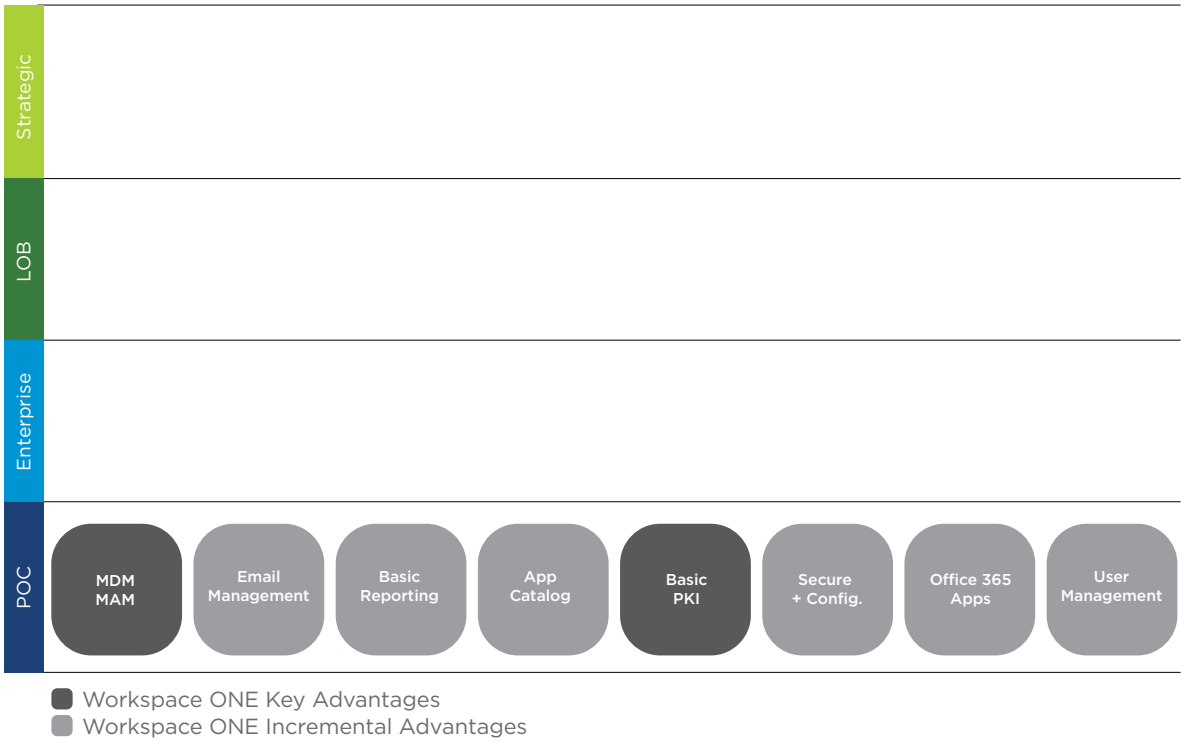

Figure 2: Workspace ONE Basic Capabilities

MDM/MAM

Mobile Device Management (MDM) and Mobile Application Management (MAM) provide the ability to administer device and application policies across all devices. Workspace ONE offers significant advantages over Microsoft EM+S for iOS and Android (including Android OEM-specific controls):

- Supports Android OEM controls
- Full support for Android Enterprise
- Supports device staging
- Full support for Apple DEP
- Supports time-based profile installation
- Real-time visibility
- Industry templates
- Granular enrollment restrictions

Organizations that serve a broad customer base will appreciate the consistent administrator and user experience across all devices and apps that VMware Workspace ONE provides. Incomplete support for legacy Android versions may present management issues in environments where managing Android devices is central to the use case.

Email Management

Email management provides the ability to restrict email access to managed and/or compliant mobile devices across iOS and Android. Workspace ONE advantages are:

- Full support for native mail client
- Support for third party Exchange ActiveSync (EAS) clients
- Realtime visibility
- Hyperlink transformation
- LDAP lookup for S/MIME
- Supports IBM Lotus Domino

Office 365

Office 365 management includes the ability to restrict email access to managed or compliant mobile devices across iOS and Android. Workspace ONE enhances and complements Office 365 in three key ways:

- Improved security
- Better administrator experience
- Greater end-user satisfaction

Workspace ONE improves the security of Office 365 through public key infrastructure (PKI) lifecycle management, secure connectivity, and an automated compliance engine. PKI lifecycle is the ability to automate the certificate lifecycle for devices under management. This includes issuance, renewal, and revocation. Secure connectivity is the ability for the platform to provide a seamless way for off-network devices and computers to securely connect to internal resources and endpoints without the need for a third-party VPN solution. An automated compliance engine enables the platform to provide an automated way to alert, notify, and enforce policies on devices that is scalable and does not require administrative overhead. The flexible rules engine provides an unlimited set of escalating actions based on the policy and infraction. When a user or device returns to a compliant state, the automated engine restores the device posture.

Workspace ONE provides a better administrator experience that includes multi-tenancy and unified endpoint management (UEM). Multi-tenancy is the ability to serve multiple tenants on a single instance. Each tenant can be divided infinitely, making the framework easy to scale and manage. Other solutions don't provide this hierarchical management structure and ease of scalability. UEM extends to every endpoint such as smartphones, tablets, laptops, rugged devices, wearables, peripherals, and IoT devices across the organization. A UEM solution manages the full lifecycle for all endpoints, from onboarding to retirement, and even manages macOS and Windows desktop and laptop devices right alongside mobile devices using a modern approach. Provisioning and securing Office 365 using Workspace ONE is a breeze with the wizard-driven interface requiring only a few mouse clicks.

For higher end-user satisfaction, Workspace ONE provides mobile single sign-on (SSO), the ability to handle seamless access to Microsoft and non-Microsoft applications across iOS and Android devices. The unified app catalog securely delivers native, web, Office, legacy Windows, mobile, SaaS, and virtual apps through a single, easy-to-use catalog.

Comparing Fundamental Capabilities

Fundamental capabilities are features and functions required by the majority of organizations to manage their digital workspace. Unlike VMware Workspace ONE, many solutions lack native app configuration and advanced app and device management. Workspace ONE has significant advantages in the areas of enterprise integration, multi-tenancy, PKI full lifecycle management, privacy protection, secure connect, and an automatic compliance engine. Some of the vendors claiming to offer a free solution have only basic and binary compliance policies that they call out as "good enough."

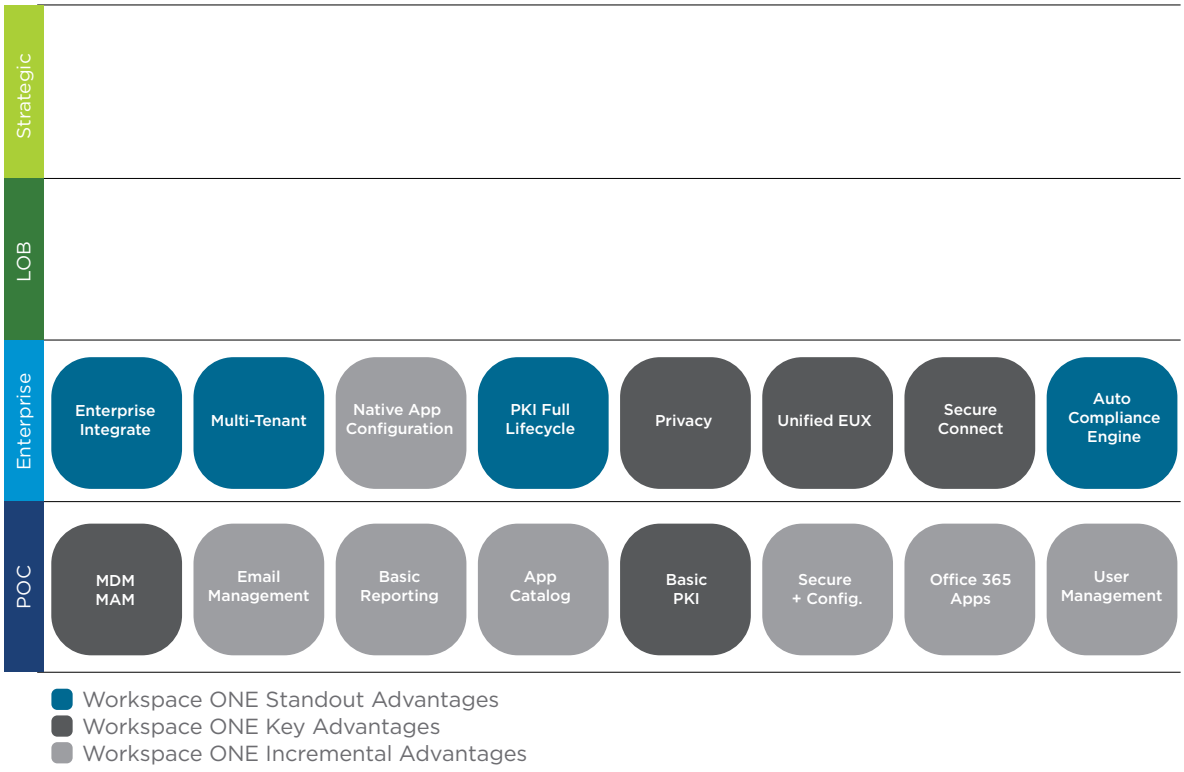

Figure 3: Workspace ONE Fundamental Capabilities

Enterprise Integration

Enterprise integration brings the ability to integrate with the best-of-breed technology and backend enterprise services to solve for various IT-driven use cases. Workspace ONE includes integrations to third-party vendors such as the companies listed below, whereas Intune lacks full support for integration with some popular identity management products such as Ping and Okta, which could make some capabilities more challenging to implement for both managed and unmanaged devices.

- SIEM
- PKI
- Mobile Security Alliance
- Print servers
- Wearables
- Content delivery networks (CDN)

Figure 4: Workspace ONE Enterprise Integration

Multi-Tenancy

Multi-tenancy is the ability to serve multiple tenants on a single instance. Each tenant can be divided infinitely using an orthogonal structure to group or segregate devices, users, regions, languages, administration, and more. Workspace ONE multi-tenancy has the following advantages:

- Provide the same UI, but limited to a specific tenant
- Hierarchical view as a Global Administrator
- Support for enterprise integration on a per-tenant level (for example, AD, PKI, Syslog)
- Hierarchical policy flow-down with inheritance and override capabilities
- Support for Smartgroups defined dynamically by Console Admins
- Ability to assign both device and app policies by smart groups
- Ability to define tenant types

Workspace ONE powerful multi-tenancy capabilities allow organizations to grow, change, and scale with complete ease.

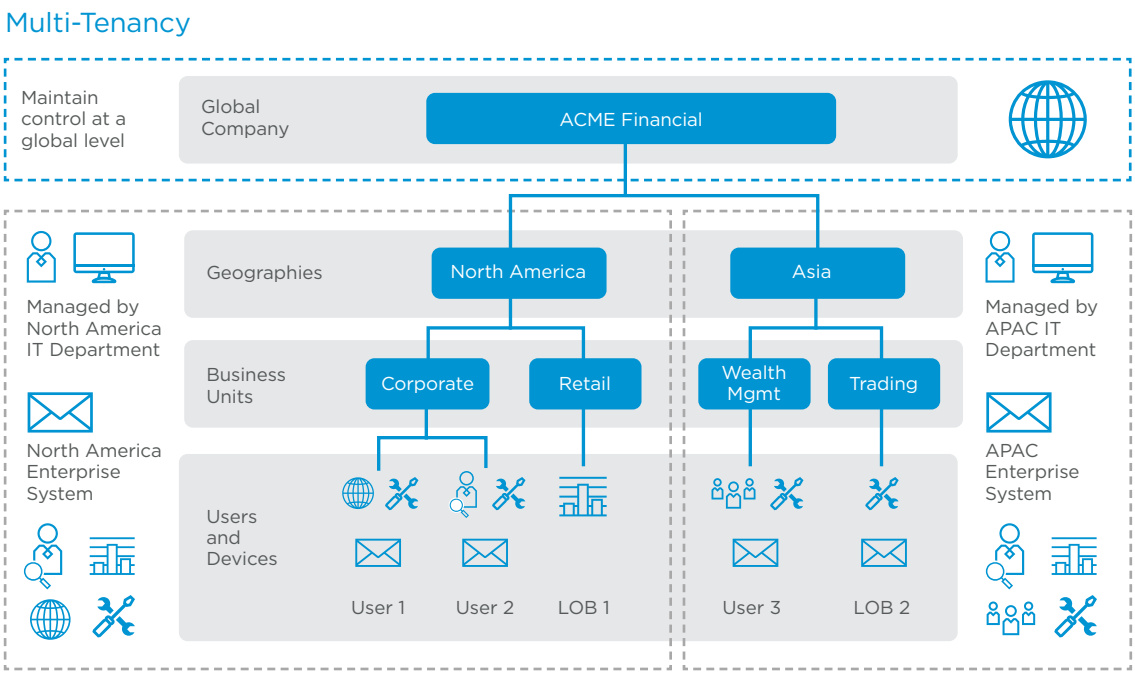

Figure 5: Create Hierarchical Management Structures That Can Grow and Scale Easily

Full PKI Lifecycle Management

Full public key infrastructure (PKI) lifecycle management is the ability to automate the certificate lifecycle for devices under management. This includes issuance, renewal, and revocation. Workspace ONE PKI management includes advanced capabilities such as: full lifecycle management for Microsoft certification authorities in DCOM mode; SCEP proxy support and force key pair generation on devices for DCOM for scalability, device, and SDK profiles; and certificate view and reporting. Workspace ONE leads Microsoft EM+S in virtually every category of full PKI lifecycle management:

- Support for defining certification authority templates in admin console
- Allow admin to upload P12s on behalf of users
- Allow users to upload S/MIME certificates and key history through SSP
- Automatically fetch user key history for various certification authorities
- Support for force key pair generation
- Support for revocation beyond NDES
- Centralized certificate list in admin console
- Certificate troubleshooting in admin console
- Distribute user certificates on Windows 10
- Unable to push or leverage certificates deployed directly to apps (BYO)
- Distribute certificates to peripherals (i.e., printers)
- Support for derived credentials

Privacy

Privacy protection is a required framework included in any workspace platform for defining the type of information collected, stored, and viewed by permission, in addition to educating the end user about the type of information being collected and stored. Workspace ONE has important advantages over Microsoft EM+S in the following areas:

- Dynamic end-user privacy awareness
- Privacy officer role in admin console
- Overarching privacy framework
- Role-based access to prevent any device manipulation

Secure Connect

Secure connect is the ability for the platform to provide a seamless method with which off-network devices and computers can securely connect to internal resources and endpoints without the need for a third-party VPN solution. IT takes the hassle out of allowing remote users to securely access corporate resources. Workspace ONE offers the following advantages over Microsoft EM+S:

- Offer a built-in, per-app VPN solution
- Provide real-time compliance access and denial
- Integration with cloud-based proxy
- Define network access rules in a single console
- Direct integration with VMware NSX®
- VPN certificate lifecycle management
- Provide secure connectivity without MDM (SDK)

Automated Compliance Engine

An automated compliance engine provides an automated way to alert, notify, and enforce policies on devices. The most desirable automated compliance engines are highly scalable and do not require administrative overhead. The rules engine should be flexible, and provide an unlimited set of escalating actions based on the policy and infraction. When a user or device comes back into a compliant state, the automated engine should be intelligent enough to restore the device posture. Workspace ONE provides all of these mission-critical capabilities and more. When compared to Microsoft EM+S, it has several critical advantages:

- Escalating time-based actions
- Platform and device-ownership aware
- Compliance enforcement for non-managed devices
- Install compliance profiles
- Support for SMS and push notifications
- Ability to support application list, cell usage, comp status, ibeacon, encryption, certificate expiry, last compromised scan, TOU acceptance, model, version, passcode, roaming, and SIM card change
- Support actions for application, notify, command, and profile
- Support for smart group assignment
- Support for conditional access for non-Azure Active Directory scenarios

Comparing Advanced Capabilities

Advanced capabilities address the unique customer requirements and specific use cases that can vary greatly from one organization to another, and within differing Lines of Business or departments. This category includes integration and support for third-party apps and existing enterprise investments in Microsoft and non-Microsoft infrastructure including PKI, cloud security services, and the Mobile Security Alliance (MSA) and newly announced Trust Network. Workspace ONE is the most successful offering that abstracts the operating system from the apps, access, and data, which provides unified endpoint management for any app on any platform.

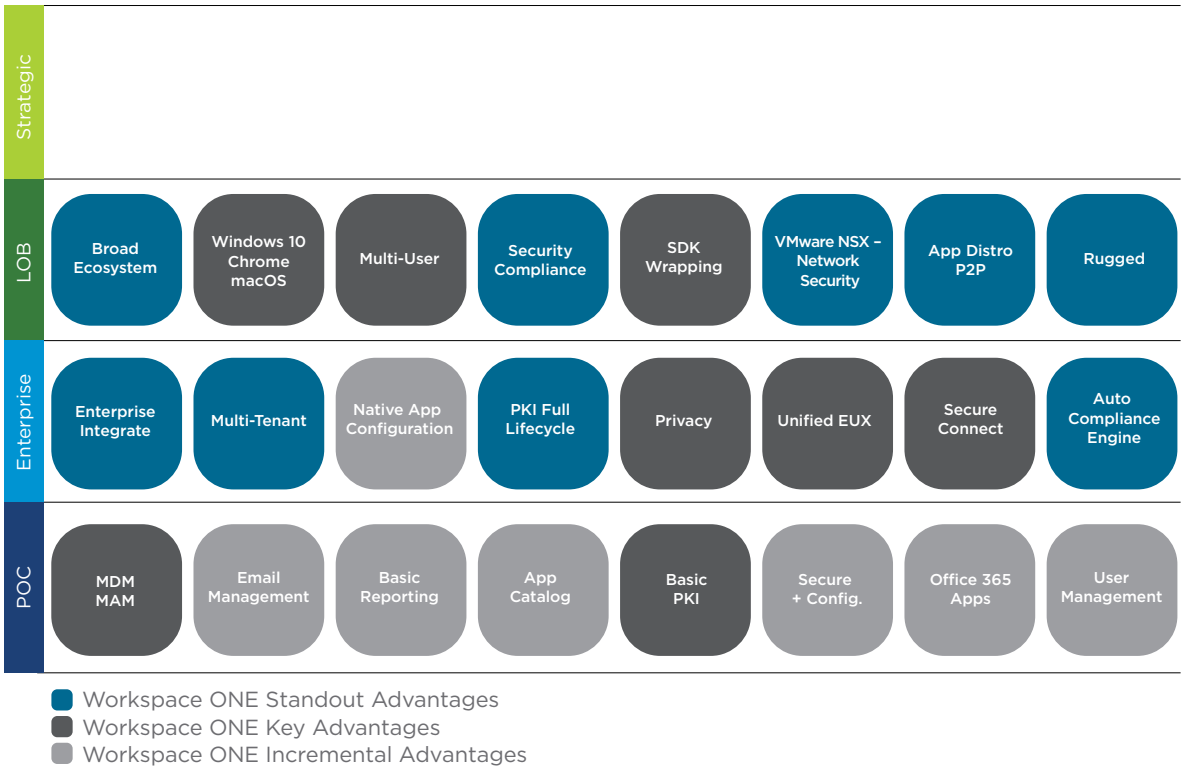

Figure 6: Workspace ONE Advanced Capabilities

Workspace ONE has standout advantages over Microsoft EM+S including broad ecosystem integration, security and compliance, network micro-segmentation and peer-to-peer app distribution, and rugged device support. Workspace ONE also has significant advantages in multi-OS support and SDK wrapping.

Windows 10 Management

Workspace ONE has the following advantages over Microsoft EM+S in a Windows 10 environment:

- Enrollment via runtime packages and limited onboarding methods for all platforms
- Support for Windows 10 advanced computer-type management (not available in Intune)
- Advanced Windows desktop app deployment and lifecycle management
- Full support for BitLocker encryption key management
- Peer-to-peer app distribution
- Full support for granular patch management within the efficient, flexible, and reliable EMM framework for Windows 10

Multi-OS

Workspace ONE has the following advantages over Microsoft EM+S in a multi-OS environment:

- Full support for advanced Android Enterprise
- Manage Windows 7 devices
- Manage Chrome OS devices
- Manage rugged devices
- Includes Mac management (Microsoft requires a third-party solution)

Security and Regulatory Compliance

Security and regulatory compliance is the ability to handle seamless single sign-on across Microsoft and non-Microsoft applications, across iOS and Android. Workspace ONE has the following advantages over Microsoft EM+S:

- Workspace ONE SDK uses a FIPS 140-2 validated crypto across iOS and Android.
- Achieved NIAP Common Criteria MDM protection profiles for iOS or Android.
- Supports events, actions, and audit logging capabilities.
- Implemented SSL pinning for console communications.
- Listed in Gartner Critical Capabilities for High-Security Mobility Management.

SDK Wrapping

SDK wrapping provides app developers with a software library that they can integrate into their apps while they are developing them. The code includes the information necessary for the developers to integrate with the MAM platform. Workspace ONE has the following advantages over Microsoft EM+S:

- Provides a common framework for developing internal apps with MDM/MAM capabilities
- Provides ability to deploy DLP-enabled apps on managed or unmanaged devices
- Provides ability to wrap apps without re-development effort
- Provides ability to support non-Microsoft apps for SDK and wrapping
- Supports custom branding

Comparing Enterprise Capabilities

Enterprise capabilities include all the strategic capabilities for creating, deploying, and managing a secure digital workspace. This includes application delivery (virtual, published, and real-time delivery), virtual desktop infrastructure, custom branding, universal SSO, adaptive management, and conditional access. Workspace ONE is the only solution that provides adaptive management and direct registration (enrollment). Workspace ONE leads Microsoft by providing market-leading products in the VMware Horizon product line (VMware Horizon Apps, Desktop, App Volumes, and VMware ThinApp®). Microsoft simply does not have comparable solutions in these areas.

Further, Workspace ONE provides leading conditional access capabilities that include: support for all apps (including Office 365); a comprehensive set of compliance policies to secure apps, devices, and users without SDKs; notifications; and escalations to an administrator if certain conditions are met. Microsoft can only enforce conditional access policies for Office apps and apps that support Intune SDK, and it cannot detect jailbreak or device compromise without device enrollment. Additionally, Workspace ONE provides more advanced capabilities for Universal SSO.

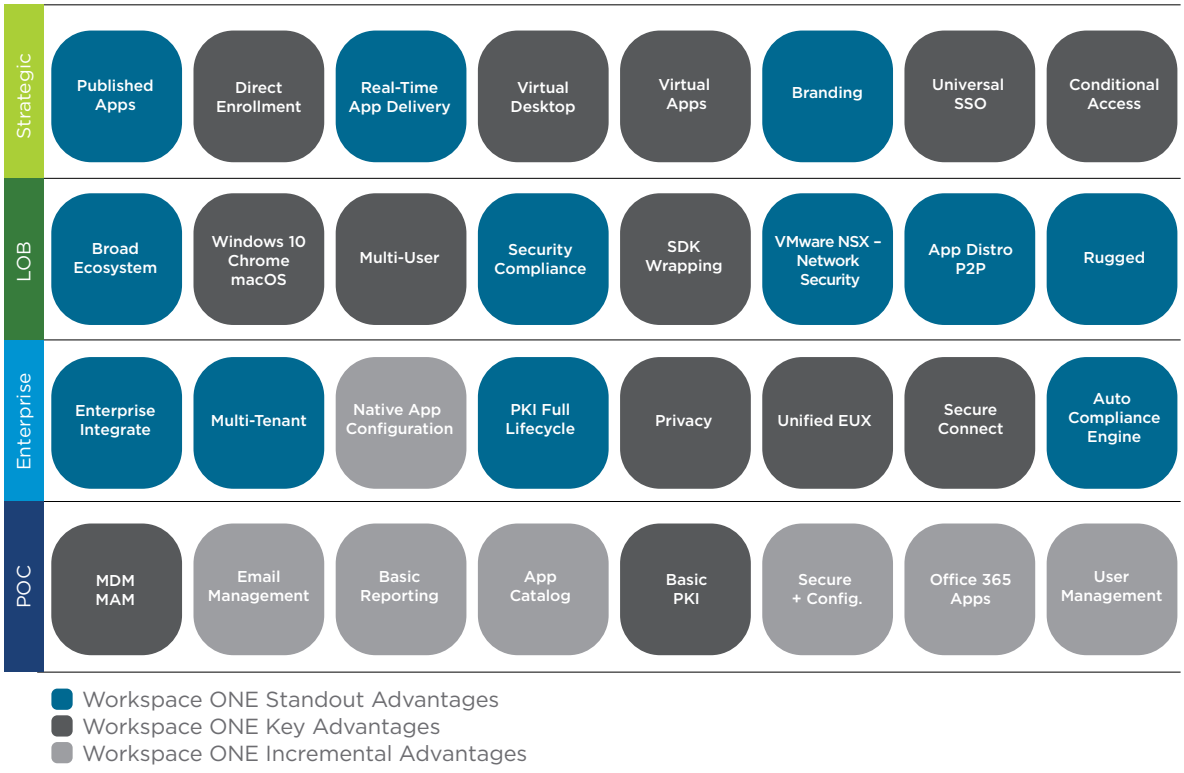

Figure 7: Workspace ONE Enterprise Capabilities

Conditional Access

Conditional access is the ability to allow or prevent access to resources based on customer-defined criteria during authentication and synchronization. Even trusted employees can unknowingly put security at risk by careless use of their device. The Workspace ONE conditional access feature allows IT to define the desired risk profile and deny access to devices that are out of compliance, protecting organizations from jailbroken devices, rogue Dropbox installations, giving access to unauthorized users, and more. Workspace ONE has the following advantages over Microsoft EM+S:

- Integration with third party IDPs and CASBs
- Conditional access from non-Microsoft apps, resources, and content
- Time-based conditional access across multiple platforms and app types

Adaptive Management

Adaptive management provides a secure method for organizations to allow both internally built and public applications to access corporate resources residing in your secure internal network on a per-app basis. It leverages device enrollment for managed timeouts and PIN strength for stronger authentication than passwords alone can provide. IT can control and enforce policy:

1. On the device
2. At the gateway talking to the internal network
3. From the identity management layer or Windows layer

Traditionally, there are different tools for managing the risks and enforcing policy across these control points. Workspace ONE is built with these integrations, allowing IT the ability to design comprehensive policies that leverage each of these control points. For instance, with Workspace ONE, IT can set up a secured dark tunnel from device to data center. With intelligent networking, IT can identify which application and which user are accessing the network, and re-route the traffic to a specific server or virtual machine to avoid attacks by malware. IT has access to a dashboard that collects data from different servers. Based on the information collected, IT administrators can quickly make changes to specific policies if necessary. They can block access to more sensitive data and unblock access to less sensitive data.

The VMware Workspace ONE platform puts policy enforcement back into the hands of IT, while giving users choice and flexibility over the level of convenience, services, and privacy they want, without the need to remember logins or use a company-provided machine. This mix of policy control and flexibility is enabled by the SDDC and the hybrid cloud, which provide the foundation for the key features of the Workspace ONE platform.

Conclusion

To be competitive in the digital workspace era, organizations need to be selective about who they choose as their partner. Vendor lock-in is an ever-present danger that will prevent you from providing an exceptional customer experience and an exceptional workplace for your employees. Workspace ONE provides mission-critical capabilities beyond what Microsoft EM+S provides. Customers have noted frustration that Microsoft offers a single price point and license for Intune, whether they are using the basic app-level controls or deploying the tool as their primary endpoint management. Addressing the many layers of an organization's unique requirements for a seamless digital workspace transformation, Workspace ONE meets or beats Microsoft on all levels.

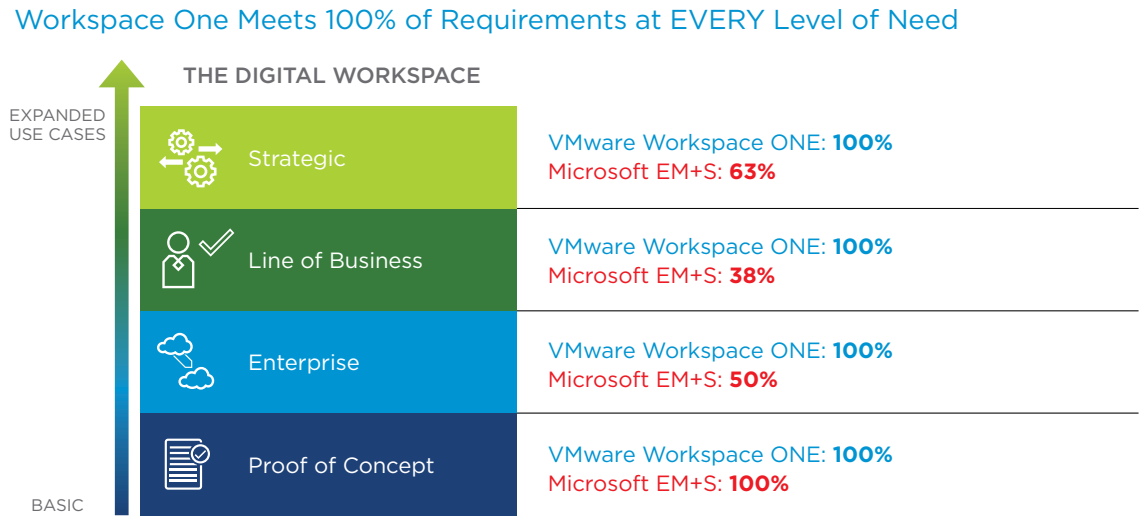

Figure 8: Workspace ONE Meets 100 Percent of Requirements at Every Level

In order to truly be successful with a digital transformation journey, a platform that supports all your IT initiatives is imperative. A "good enough" point solution will not be able to drive success past the POC stage and into your future. Choose wisely. Evaluate VMware Workspace ONE today.

Contact Us

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),
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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2018 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. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 5343-VMW-TBG-SELECTDIGWKSPSOL-USLTR-20180813-WEB
08/18