WHITE PAPER – **APRIL 2018**

FIVE IMPORTANT BUYING CRITERIA TO ENABLE A TOTALLY MOBILE WORKFORCE

vmware®

Table of Contents

Introduction

This paper provides guidance for selecting and purchasing a digital workspace solution to enable your totally mobile workforce. Five buying decision considerations that directly impact the success of your mobile workspace initiative are discussed in detail. Recommendations for the most critical specifications are given to help you define an effective digital workspace strategy for your environment.

The intended audience for this paper is enterprises seeking to empower a completely mobile workforce while enabling IT administrators to manage and secure their rapidly changing networks. IT decision-makers and line-of-business leaders alike will find the insights presented helpful for executing a mobile conversion project.

Why This Paper?

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 information presented in this paper can help.

When developing your digital workspace, it is important to keep five key considerations in mind, both on the front end and the back end of your environment. But before we get into the recommendations for creating an effective digital workspace, let us take a look at the concept in general.

A digital workspace provides access from anywhere—on any device, at any time—to the applications, services, and data that end users need, while offering administrators the ability to quickly and easily control and secure the functions they provide from a centralized location. The best digital workspace is invisible to the end user and meshes neatly with the devices they already know how to use. An essential element of a digital workspace is a self-service catalog that allows users to subscribe to the apps and services they need to do their work.

So, how do you go about creating an effective digital workspace? First, take into account these basic considerations:

- Seamless, secure end-user access to applications and files
- Easy-to-use enterprise app store
- Management security
- Fully integrated infrastructure stack
- Open platform

This paper discusses these major considerations, as well as detailed strategies, and provides recommendations for effectively addressing each one.

First, let us look at the forces that are driving countless organizations to adopt digital workspace solutions.

Why a Digital Workspace?

End-user work habits are changing dramatically. Users are increasingly working from anywhere, at any time. What's more, countless end users are relying on a multitude of personal devices to remain productive around the clock. According to Forrester's Forrsights Workforce Employee Survey, about 74 percent of information workers use two or more devices for work, and 52 percent use three or more.

In addition to device proliferation, the headache of managing a myriad of app types—the average organization owns about 2,500 apps—and machines, combined with the emergence of software-as-a-service (SaaS) applications and cloud storage, brings the need for a digital workspace into clear focus, both from the end-user and administrator perspectives.

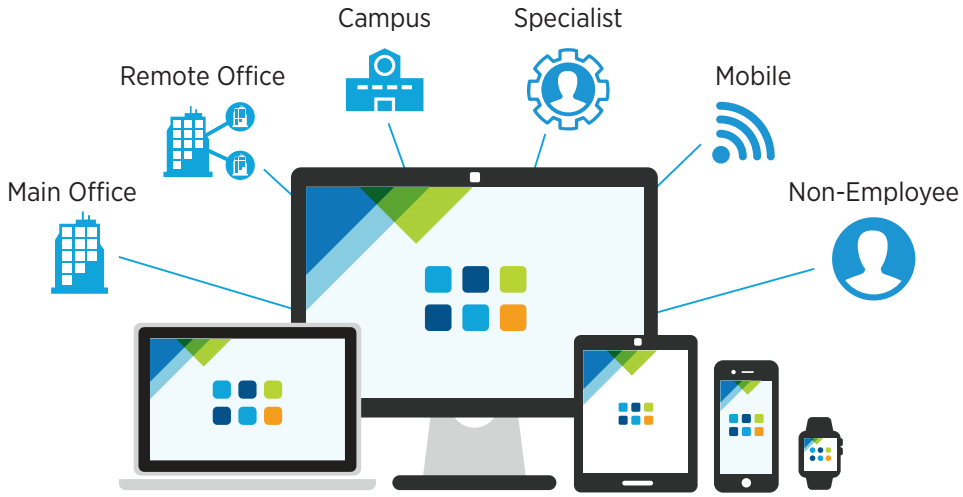

Figure 1: The Digital Workspace Boom

The forces driving the digital workspace boom create two perspectives in the mobile workforce: that of end users and IT administrators.

- **IT perspective** – Supporting thousands of disparate apps, services, and machines is a significant challenge. A digital workspace gives administrators a simple way to manage and secure sensitive apps and data via a simplified, centralized interface.
- **End-user perspective** – Users need to access an increasing number of apps and data from anywhere at any time. A digital workspace allows them to personalize their interface with the apps and data they need, and gives them the freedom to access them from a single location.

The results:

- A significant boost in productivity for both your end users and the IT administrators that support them
- The ability to transform existing business workflows and processes with ease and efficiency

Now let us take a look at the top-five buying criteria for selecting an effective digital workspace solution.

Buying Criterion 1: Simple, Seamless End-User Interface

One of the most important aspects of an effective digital workspace is a user interface that offers

- A single point of access for productivity apps and tools
- Easy application navigation and management
- Personalization and customization
- Native-device integration
- User change isolation

Single Point of Access for Productivity Apps and Tools

Managing multiple passwords is a risky proposition, both for end users and administrators. End users have to keep track of several passwords, and, as a consequence, many are simple and hackable. Administrators worry about enforcing password policy, which resets periodically via Microsoft Active Directory (AD), while simultaneously ensuring those credentials stay safe within company walls.

With single sign-on (SSO), the user logs in once with a single set of credentials and gains access to the various systems they need without having to re-enter passwords at every turn. SSO gives users the ability to navigate through their applications, workspaces, and data freely, which, in turn, boosts their productivity. (Consider how much time you spend finding, entering, and re-entering passwords on a daily basis.) As an added bonus, SSO also reduces the amount of time IT spends ensuring password security as well as addressing help-desk calls about access privileges.

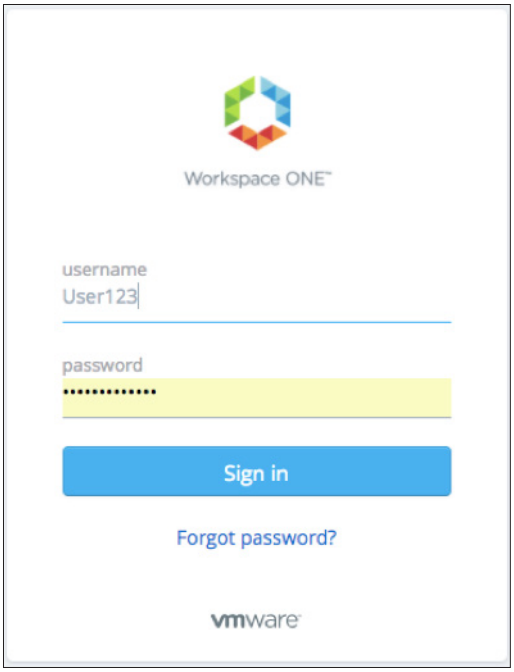

Figure 2: Typical SSO Screen

Generally, any workspace solution must have one identity source to be secure. Good workspace solutions check with AD and issue a token that allows users to seamlessly open applications and data. Depending on the policy, you can also have different authentication methods to achieve a higher level of security (or conform to organizational standards).

Easy Application Navigation and Management

The modern end user relies on a large number of applications to stay productive. With SSO, users do not have to worry about entering various passwords to access their applications and data. The next step on the road to a better digital workspace experience is to enable end users to manage their apps by adding subscriptions and creating favorites, with the additional ability to navigate between apps with ease and efficiency.

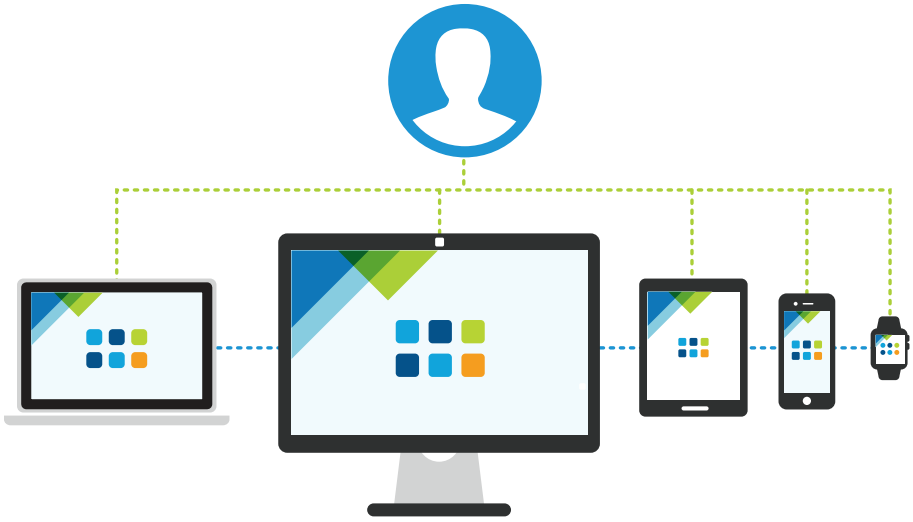

Figure 3: Users Access Apps Easily on Any Device

Therefore, it is important that end users have a single location from which they can open their apps with the click of a button. Additionally, end users should be able to add subscriptions to new apps and organize their existing catalog to best suit their needs, all without having to consult an IT administrator.

By allowing users to add subscriptions and favorites independent of IT, you enable them to personalize their experience and boost their productivity. For IT, less time is spent on managing a particular end user's personal workspace and more time on addressing higher-level concerns.

Personalization and Customization

End users have come to expect a lot from the apps and services they use at home. Unfortunately, they have come to painfully accept the opposite from the apps and services they use at work.

By *consumerizing* their enterprise-app experience, that is, by providing the same fluidity and efficiency that users get from their personal apps at work, you enable them to work more quickly and confidently on the tasks that matter most.

"Consumerization is the reorientation of product and service designs around the individual end user. The emergence of the individual consumer as the primary driver of product and service design originated from and is most commonly seen as a major IT industry shift, as large business and government organizations dominated the early decades of computer usage and development."

– WIKIPEDIA

Offering users the ability to personalize their digital workspace by dragging and dropping apps where they want them, much like people personalize their smartphone interface, streamlines their experience, increases workflow, and produces a happier, more productive end user.

Moreover, by giving end users the freedom to customize their interface, you free IT from the burden of helping individual users create a solution that makes them more comfortable and more productive.

Native-Device Integration

A good user experience is embedded natively into a desktop or device. Users should be able to open their Start menus, or catalog of apps and files for non-Windows systems, to access their workspace apps and files just like they would with the apps and files that live on their actual device.

User Change Isolation

From an administrator's perspective, giving users the freedom to customize their workspace poses a significant managerial problem. It is important that user-initiated changes remain independent from the core infrastructure—any change a user makes to their workspace affects nothing on the back end.

By preserving all user workspaces independently of the back end, you also give IT the ability to easily deprovision or provision end users. Isolation bolsters the security of the workspace platform and reduces the time it takes IT to provision and decommission a particular user's digital workspace.

Buying Criterion 2: Enterprise App Store

To enable end users to personalize their workspace experience—and achieve a higher level of fluidity and productivity—you need one key feature: an enterprise app store. An enterprise app store gives users the ability to personalize their app catalog by adding apps and services independent of IT and to access any app from a single console, regardless of app or machine type.

Figure 4: Users Navigate to an Enterprise App Store That Is Context-Specific to the Device They Are Using

According to ZDNet's Joe McKendrick, enterprise app stores are "meant as centralized directories for services, applications, and APIs that are available for integration or consumption, and can be downloaded or reviewed in a single click or two."

From the end-user perspective, an enterprise app store includes two important features:

- Self-service model that allows users to select the apps they want from the app store without having to ask IT for help
- Ability to download any approved app, regardless of type, and access that app from any machine, regardless of make or model

From the administrator's perspective, there are five key considerations:

- Automated provisioning that allows IT to standardize a set of apps that every user is automatically given access to
- Ability to set policies for how long a user can stay logged in to an app and which level of authentication is required
- Automated auditing and reporting to keep track of which apps are in high demand and which are not
- Workflows for assigning licenses to particular apps and enabling and disabling users' access to the workspace
- Infrastructure service portal for granting end users self-service access to commonly used services without the need for IT to respond to every request

Self-Service Model

The most important benefit of an enterprise app store is the ability to enable users to access the apps and services they need on their own without having to turn to IT for help. Providing end users with the ability to self-serve their own apps and services from a consolidated catalog allows administrators to focus on other tasks and stay productive.

IT departments in organizations adopting a self-service model have been able to reduce call volumes by up to 90 percent.

Categorizing App Types

With an enterprise app store, you can consolidate all apps, regardless of type, into one easy-to-access location. From here, you can categorize your apps based on versions or device compatibility, allowing end users to quickly pinpoint which apps are compatible with which devices and operating system versions. The result is a reduced burden on IT and a more streamlined approach to app management and usage for the end user.

Automated Provisioning

With all apps, services, and data provided via a single app store, IT can quickly provision new users with a suite of essential apps as well as enable users to pick and choose the items they want in their digital workspace.

Controlling Access with Policies

An enterprise app store enables IT to set policies for apps and services from a single location. Administrators can control how apps and services are used and set various levels of authentication for particular apps.

For instance, an administrator can set a time limit for how long a user can stay logged in to an app or assign users particular levels of authentication to limit access to sensitive apps.

Auditing and Reporting

Another important benefit of an enterprise app store is the ability to gather intelligence on app, service, and data usage from a single location. Consolidating all resources into an enterprise app store gives IT administrators a single window into usage, thereby enabling them to collect big data without spreading themselves too thin.

For instance, IT can use a digital workspace to track entitlement (number of users assigned the app) versus activation (number of users using the app) and gain insight into who is using which apps, and how people are using them. Administrators can also go a step further and assign costs to apps and measure utilization, thereby understanding the value that a particular app is providing to the organization.

Using Workflows to Increase Efficiency

To further curtail unnecessary app expenditure, you can assign licenses to certain costly apps. The goal is to require an end user to obtain approval before they can use a particular app. When a user requests approval, a workflow is initiated in the system in which you have chosen to manage licenses. When approval is granted, the digital workspace is then notified and grants permission to the user.

This concept also applies to the employee life cycle. With workflows in place, you can easily grant new employees access to apps and, in turn, terminate their access when they leave the organization.

Self-Service Portals

More and more organizations are turning to self-service portals that empower employees to access preapproved services and make requests from IT, as well as provide additional capabilities. Portals save time for both end users and IT. When designing your digital workspace, it is important to take into account the various mechanisms already in place for web access to services and applications.

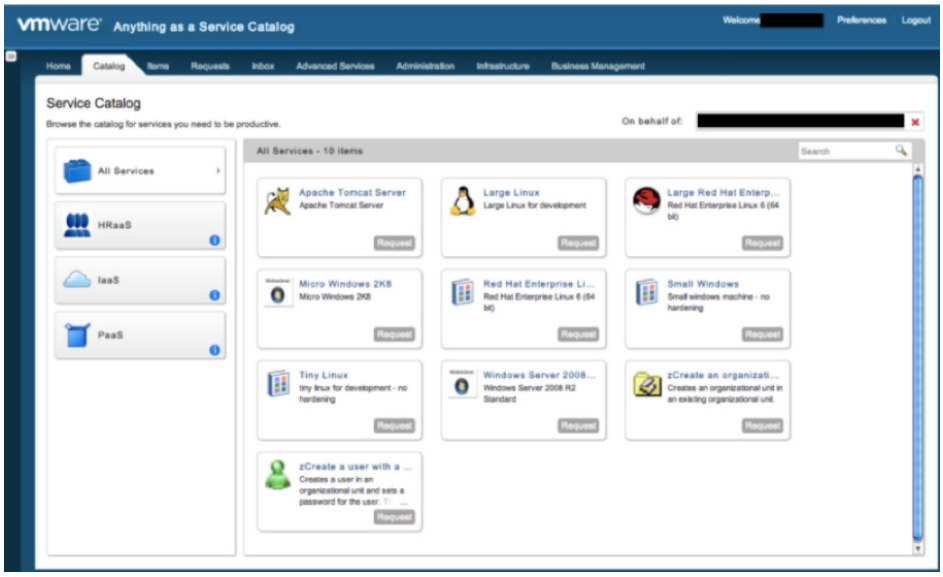

Figure 5: VMware vCloud® Automation Center™ Self-Service Portal

Regardless of which service portal your organization uses for managing workflows, make sure that the digital workspace you choose can integrate with it. The best scenario is if your workspace platform provides APIs that allow you to integrate it with your workflow of choice. Organizations typically standardize on a management platform and build up from there. Ensure that your digital workspace can integrate with existing and future-planned management and portal software.

Buying Criterion 3: Ensuring Secure Access

With so many apps, services, files, and machines to keep track of, security is a major concern for IT departments everywhere. The fact that end users are becoming increasingly mobile and accessing potentially sensitive information from anywhere, at any time, and from any machine, combined with the ever-present hacker threat, is troublesome for IT.

However, with a digital workspace solution in place, IT can manage security from a single location and across apps and machine types without spreading themselves thin across several different management platforms.

Nearly all devices trying to access corporate information will eventually be enrolled with certificate-based security profiles. From Windows 10, to the latest macOS, Android, and iOS, it is unanimous that the OS vendor will provide the integration points necessary to enforce corporate policies on both corporate-owned and BYO devices. However, it requires a robust policy engine to allow enterprises to design and implement pragmatic rules while maintaining user privacy.

With the advent of network virtualization and micro-segmentation, it is now possible to isolate individual services from each other within the firewall, rather than simply protecting the edge.

When it comes to digital workspace security, consider these four basic concerns:

- Access from any device
- Access from any location
- Multifactor authentication
- Policy attributes for better management

Figure 6: Secure Access from Any Device and Any Location

Access from Any Device

Today, with the average end user using three to four devices to access the apps, services, and data they need, IT's job is a lot more difficult. But with all apps, services, and data living under one roof—the digital workspace—you can manage security for any device from a single location. Whether your users are accessing an app from a personal tablet, thin client, or a desktop at a public library, you are able to secure any connection made to the digital workspace.

To facilitate security in a mobile device community, more and more organizations are turning to Enterprise Mobility Management (EMM). Using EMM, your end users enroll a device to bring it under IT management. The best EMM solutions allow for customizable settings of device control and access, because one size doesn't fit all. Look for EMM solutions that allow you to customize the amount of control you have over the device and the types of access you can grant your end users. Consider especially these capabilities in an EMM solution:

- Lock a device in the event that it is lost or stolen
- Locate a device in times of uncertainty
- Implement conditional compliance policies based on location or device
- Remote selective wipe devices to prevent unauthorized access to corporate information
- Enforce passcodes on devices
- Obtain information about devices such as OS version, last update, location, and more

EMM provides a centralized way for you to manage devices on all major operating systems—Windows, Mac, and Linux.

Access from Any Location

Mobile access has forever changed IT responsibilities. Now users can access the apps and data they need from almost anywhere in the world, complicating security. But with a digital workspace, you can manage access and maintain secure connections because all requests are routed to the same location—your digital workspace infrastructure.

Multifactor Authentiation

As discussed earlier, SSO is an extremely important element of an effective digital workspace. However, SSO does not mean that multiple authentication levels cannot exist behind the scenes. In addition to SSO, a secure digital workspace should offer multiple levels of authentication that are invisible to the user and easily configurable by IT administrators.

In addition to traditional multifactor authentication and conditional access designed to be less obtrusive, other authentication mechanisms exist. Many applications may simply trust that a pin or password from an enrolled, trusted device can be an effective authentication mechanism for applications. The enrollment process creates a chain of trust from the device manufacturer, to the user, to the enterprise. When using secure pin or password device-lock policies, Mobile Device Management (MDM)–enrolled devices present an interesting, user-friendly option for strong authentication.

Multi-factor authentication (MFA) is a method of computer access control that a user can pass by successfully presenting authentication factors from at least two of the three categories:

- Knowledge factors (things only the user knows), such as passwords
- Possession factors (things only the user has), such as ATM cards
- Inherence factors (things only the user is), such as biometrics

Requiring more than one independent factor increases the difficulty of providing false credentials.

– WIKIPEDIA

Policy Attributes for Better Management

Policies are the gatekeeper of any organization. IT relies on the effectiveness and flexibility of policies to enforce access rules. The more granularity in your access policies, the more you can be assured that the right information is getting to the right people and, more importantly, that none of your organization's intellectual property is falling into the wrong hands.

A basic policy management system includes the ability to set policies on a per-app basis, and even set per-app and per-user access rights. More secure systems might even require an RSA SecurID, and still others might have a five-minute timeout. Ideally, you want your policy system to be flexible in this way. Here are some considerations for settable policy attributes:

- Session length
- Device type
- Geographic location
- Application type
- Authentication type
- User-group membership

The more robust policy management systems can handle the complexity of a changing organization as well as the implications this has on AD, with mergers, acquisitions, and other changes in employee status. Your policy management system needs to sync data from on premises to the cloud.

Your unique environment determines the priority of the attributes needed in your digital workspace to provide both flexibility and control.

Buying Criterion 4: Open Platform

Have you ever purchased an open management or infrastructure system only to learn that by "open," the vendor meant you could freely integrate with its other systems? Many refer to this conundrum as vendor lock-in, and it is an all-too-common tale these days. Protect yourself and your investment by selecting a digital workspace platform that does not lock you in to a single vendor or standard.

Authentication Support

One way to ensure the platform you select is truly open is to ask the vendor for a list of the user authentication standards that they support. Here are a few of the most common user authentication standards that should be supported right out of the box:

- Microsoft Active Directory
- Kerberos
- RSA SecurID
- RSA Adaptive Authentication
- Certificate User Authentication Methods

Some organizations require their own custom user authentication process. Others might use lesser-known authentication products. In these cases, be sure to ask how the vendor will support custom methods. Many digital workspace vendors avoid this question. The best choice is a vendor that provides a mechanism for writing plug-ins that integrate with custom processes and other vendors.

Network Gateway Support

Another important aspect of an open platform is the ability to deploy it anywhere and have it work with any gateway. The major gateway vendors that most organizations want supported are

- F5
- Citrix NetScaler

The platform you choose is one of the most important decisions you make in your journey toward a totally mobile workforce, so be sure to select an open platform that provides robustness, openness, and security.

Buying Criterion 5: Data Center Virtualization and Flexible Cloud Infrastructure

It is nothing new: End users are demanding new applications and services daily, making it difficult for IT departments to keep up. In some organizations, end users have even gone outside the corporate firewall without IT's knowledge to access the services they want and need. This phenomenon of using IT systems without the enterprise's IT approval is commonly referred to as "Shadow IT."

Through advances like virtualization, organizations have managed to increase their ability to meet the varied and instantaneous needs of Shadow IT with the resources at hand. However, mobile workforce requirements are now outpacing what standard IT practices can deliver. A new approach is needed.

Data Center Virtualization brings together server, network, storage, and end-user computing into one common framework that can be deployed in the data center, the cloud, or a combination of the two (a hybrid). Leading-edge IT organizations are setting up hybrid cloud environments that span multiple instances while deploying network-virtualization software that simplifies data center management. These organizations are able to abstract the management of networks in much the same way as they abstracted the management of physical servers with server virtualization. And for storage virtualization, they are using a data plane through which virtual storage systems can be more easily shared across multiple instances.

There is a lot of talk about services these days: SaaS, platform-as-a-service, and IT-as-a-service. But why would IT want IT-as-a-service (ITaaS)? The answer has to do with the difficulty that IT departments face today compared to 10 to 20 years ago. Today, IT departments are being asked to do more than ever, yet budgets have remained fairly flat or have even declined.

Finding a platform that provides the flexibility for an ITaaS approach and that allows you to standardize on a set of technologies and manage a hybrid cloud environment is one of the most critical decisions of this process.

Figure 7: Data Center Virtualization and Flexible Cloud Infrastructure Future Proof Your Organization

Architectural Considerations

One architectural approach used by some organizations involves making their infrastructure more agile and adaptable through software orchestration, policy-based management, and self-service. This method enables end users in an organization to provision new services and resources when they need them rather than going through a cumbersome approval process.

Recommendations for an effective virtualization strategy are

- Integration of all platform components from the desktop through the data center to the cloud
- Hybrid cloud capabilities – Deploy on premises or in the cloud
- Policy-controlled users, resources, and endpoints
- Easy point-and-click policy management
- Unification of end users in Active Directory
- Support of objects that are aware of each other via an Internet of Things
- Single administration console
- Open services architecture
- Stateless machines – If one machine goes down, users can be moved to another

Of course, you still need the baseline expectations for your data center and cloud infrastructure:

- Scalable
- High-performance
- Robust
- Secure
- Reliable

Conclusion

The need to enable a totally mobile workforce with a digital workspace environment is driving IT departments to think out of the box and adopt new ways of doing work. Addressing the requirement for users to work from everywhere is a driving force in the shift to the digital workspace. Unfortunately, architecting a secure, seamless, scalable digital workspace can be challenging, but, if you have gotten this far, you are off to a great start.

If you are interested in going mobile, check out VMware Workspace ONE™ or talk to a VMware representative today.

For more information about VMware products, call 1-877-4VMWARE (outside North America dial +1-650-427- 5000), or visit www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and system requirements, please refer to VMware product documentation.

Appendix: Mobile Digital Workspace Buying Criteria Checklist

The following checklist is based upon the digital-workspace buying criteria covered in this paper. When creating an effective digital workspace, be sure to include most (if not all) of the following requirements.

Note: Realistically, each requirement benefits both the end user and the IT administrator; however, some requirements benefit one more than the other. Therefore, we have categorized the following requirements into two groups: those that benefit end users and those that benefit IT admins.

CHECKLIST	CAPABILITY	END-USER BENEFIT	IT ADMIN BENEFIT
☐	Simple, seamless user interface	●	●
☐	Single point of access for productivity apps and tools	●	●
☐	Easy application navigation and management	●	
☐	Personalization and customization	●	
☐	Native-device integration	●	
☐	Isolating user changes to individual workspaces		●
☐	Enterprise app store	●	●
☐	Self-service enterprise app store	●	●
☐	Categorizing apps based on type, version, and compatibility	●	●
☐	Automated provisioning		●
☐	Controlling access with policies		●
☐	Auditing and reporting		●
☐	Using workflows to increase efficiency		●
☐	Self-service service portals	●	●

CHECKLIST	CAPABILITY	END-USER BENEFIT	IT ADMIN BENEFIT
☐	Secure access to the Digital Workspace	●	●
☐	Access from any device	●	
☐	Access from any location	●	
☐	Multifactor authentication		●
☐	Policy management that syncs data to the cloud		●
☐	Settable policy attributes		●
☐	Open platform		●
☐	Supports most common user authentication standards		●
☐	Custom user authentication processes		●
☐	Supports major gateways (F5, NetScaler)		●
☐	Data center virtualization		●
☐	Deploy on premises and/or in the cloud		●
☐	Easy point-and-click policy management		●
☐	Unification of end users in Active Directory		●
☐	Support of objects that are aware of each other via an Internet of Things		●
☐	Single administration console		●
☐	Stateless machines – If one machine goes down, users can be moved to another		●
☐	Flexible cloud Infrastructure		●

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
 Item No: VMW-WP-FIVEIMPCRITERIA-USLTR-20180409-WEB
4/18