

COMPLETE YOUR OFFICE 365 DEPLOYMENT WITH A DIGITAL WORKSPACE PLATFORM

Table of Contents

Introduction: Consumerization is Changing the Workplace 3

Embracing Opportunity with a Digital Workspace Strategy3

Making Office 365 Part of the Digital Workspace 4

Delivering Management at Scale 4

Office 365 Extends to New Use Cases 5

Best Practice Security Made Practical with Office 365 5

Conditional Access to Managed and Compliant Devices Made Easy 6

A Superior Experience Across Applications 6

Connectivity Delivers the Big Picture 7

Multi-Tenancy Enables Scalability and Simplicity 7

Conclusion 7

Introduction: Consumerization is Changing the Workplace

The age of consumerization is unfolding everywhere. People are more comfortable than ever using new consumer apps and services, delivered on the web and over mobile devices. They're easy to purchase, simple to learn, and enjoyable to use. Consumerization is not only changing personal lives, but reshaping expectations in the workplace.

Today's workforce is looking for the same degree of convenience and accessibility at work that they find on their mobile apps and devices at home. With today's new delivery models, they can get the apps they need in seconds. If their IT teams can't offer the same level of agility, these employees will source and buy their own. In fact, studies show that over one in four business apps are brought to the company by the employees themselves¹. Professionals rely on business apps to increase their productivity and spend more time collaborating within and across teams. According to Forbes Insights, 67 percent of employees with immediate access to the applications they need cited them as "very important" to increasing collaboration². These employees also reported a 34 percent increase in productivity, and 100 percent increase in the quality of service they gave customers³. Unfortunately, if employees access such apps without cooperation from IT, compliance and security issues can be introduced, putting organizations at risk of data loss.

For businesses on the path toward an employee-centric digital workspace, Microsoft Office 365 can be a convenient starting point. When integrated into a digital workspace strategy, Office 365 supports easy access to the productivity tools users require. That's why now is the time for organizations to combine Office 365 and other vital apps into a digital workspace strategy.

Embracing Opportunity with a Digital Workspace Strategy

To offer the employee-centric experience businesses need, IT organizations are adopting a digital workspace strategy. The digital workspace is a fundamental change in the way end-user services are delivered. It lets IT securely and reliably deliver the apps and data employees need to work across any device, company-owned or personally-owned (BYO).

The digital workspace makes it easier to manage user services and access policies across all types of applications, on premises or in the cloud. It integrates endpoint management, application management, and access control, to minimize the cost of IT operations while incorporating security best practices.

A digital workspace allows organizations to implement a more collaborative, compatible approach to application access that complements Office 365.

¹ "The Impact of the Digital Workforce," Forbes Insights, 2017

² Ibid.

³ Principled Technologies, "Simplify digital workspace management for admins", September 2017

VMware Workspace ONE™ is a digital workspace platform that puts IT in the position to succeed by allowing executive, end user and IT needs to be met. The platform provides management at scale to keep pace with today's dynamic business environment. Its enterprise-class security is built around best practices, to help ensure that users, devices, and apps remain compliant.

“An admin using Workspace ONE deployed a public Windows 10 app in 29 seconds, compared to 58 seconds to deploy the same app using Microsoft Enterprise Mobility + Security⁴.”

— PRINCIPLED TECHNOLOGIES

Making Office 365 Part of the Digital Workspace

Business productivity applications like Office 365 span multiple organizations and processes across the enterprise. To deploy them successfully, it's important to consider the requirements of all stakeholders.

For executives, quickly adopting and implementing cloud strategies are paramount concerns. They're seeking quick deployments to rapidly unlock the value from their technology investment and strengthen their competitive position.

End users, however, are more concerned with improving collaboration and personal productivity. They expect a frictionless experience with intuitive, convenient access to Office 365 as well as other apps they may need—across all their devices. A well-planned deployment will provide support for single sign-on (SSO), bring-your-own-device (BYOD) initiatives, and self-service capabilities.

IT must consider both the concerns of executives and end users, while also supporting compliance, security, and compatibility requirements. To maintain the integrity of their network, resources, and business processes, IT must focus on securing all data, and ensuring it integrates smoothly with their existing environment. They must also please executive stakeholders, performing quickly and delivering Office 365 to end users to help drive productivity. And at the same time, they need to deliver a good experience for end users to minimize support calls and helpdesk tickets.

Delivering Management at Scale

The days of an office with company-controlled PCs and laptops are long gone. Today's workplace is a cornucopia of laptops, tablets, smart phones, PCs, and field devices. They may be owned by the company or employees. Organizations that don't allow corporate data on personal devices face the risk of users seeking out ways to circumvent controls, doing work on personal devices or using unapproved apps and services. To support this growing variety of devices and their apps, organizations need a trusted, proven way to enable organizations to extend their workspace to all endpoints.

Workspace ONE delivers the robust management foundation that organizations need to effectively support Office 365 and all their other apps and services, across all device types. It helps organizations ease deployment, security, and management—not only with the services and apps they use, but on every device and its data. With Workspace ONE, it's easy for IT to deploy the resources users need at scale, while providing frictionless access users expect—without compromise to security. Workspace ONE enables IT to rapidly enable and support every endpoint and every user from a single management console, with deep enterprise security at every layer. An admin using Workspace ONE deployed a public Windows 10 app in 29 seconds, compared to 58 seconds to deploy the same app using Microsoft Enterprise Mobility + Security⁴.

Business needs are constantly shifting and evolving, and Workspace ONE was designed with scalability in mind. When requirements change, it gives organizations the ability to quickly grow into new use cases—not grow out of the solution. The built-in agility of the digital workspace delivery model makes it easier for IT and line-of-business stakeholders to collaborate and respond proactively to changing business priorities. The result is a more agile organization that can better meet expectations from executives, as well as end customers.

⁴ Principled Technologies, “Simplify digital workspace management for admins”, September 2017

Office 365 Extends to New Use Cases

A cloud-first digital workspace delivers the flexibility and scalability organizations need to keep pace with rapid business changes. For example, an organization might start its Office 365 deployment with a small proof of concept project at select sites in the U.S. Using Workspace ONE, the company could create all the necessary device policies, app and user access policies required for the pilot program. When the company expands operations to Europe, it could easily add new privacy rules to comply with European privacy regulation—without having to redesign the rest of their existing policies for North American office workers.

The flexible platform scales not only geographically, but can also accommodate new devices and use cases. When the organization expands operations to its manufacturing plants in Asia, it can easily support line workers and rugged industrial devices without requiring a complete rework of policies.

Best Practice Security Made Practical with Office 365

Security is critical in a fast-changing landscape where traditional perimeters do not apply. In some ways, it is even more essential for organizations where Office 365 is widely deployed and accessible across the organization. An enterprise-wide Office 365 deployment is packed with valuable data, and its wide availability puts customer information and intellectual property at risk.

The stakes are high, and external, malicious threats like hackers and viruses aren't the only threat to data integrity. Data and communications can also be compromised from within an organization by non-compliant devices, rogue users, and misconfigured applications—or by external attackers that can take advantage of these internal vulnerabilities.

Workspace ONE integrates with Office 365 to deliver the comprehensive data security required to safeguard company assets on premises and in the cloud. Its policy-based security approach helps ensure that only the right users, with the right app configuration, can access the network. With Workspace ONE, IT and other key stakeholders at an organization can define security levels and tailor granular access policies based on device state, device compliance with IT policies, network location, geographic location, device state or compliance, as well as other criteria.

For example, Workspace ONE supports robust access management capabilities to revoke access to Office 365 when a user's device becomes non-compliant. If a user attempts to access the app on an insecure device, access is immediately taken away, even if the user already has a session with Office 365. Security is based on the real-time state of the user's device, rather than an individual session token that can persist for days or weeks after a user or device becomes non-compliant. This continual access control is woven deep into the fabric of every business process and cannot be sidestepped, so corporate data remains secure.

To help enhance security and compliance, Workspace ONE also provides support for full lifecycle public key infrastructure (PKI). Public keys can be issued, revoked, and renewed automatically, providing a seamless, efficient access solution for end users and IT.

With a digital workspace, IT maximizes security and compliance, while ensuring a convenient, hassle-free user experience.

Conditional Access to Managed and Compliant Devices Made Easy

As the lines of device ownership blur, there's constant risk of users using personal devices, apps, or services for work, even if corporate policy discourages it. Companies that don't have a BYO or personal device policy still must think about personal devices, because one quarter of the apps used for work are personal apps. With a digital workspace, a company doesn't need to own a device in order to establish trust with it.

Workspace ONE employs conditional access, with real time authentication based on device compliance, as well as other Identity and Access Management (IAM) factors at the time of authentication. It enables IT to remove data, apps, and block access to Office 365—immediately—depending on the state of the device.

Workspace ONE also supports more policies for each device compared to traditional Windows management tools. Admins using Workspace ONE can have a wide selection of policies to apply to user's device regardless of OS. Policies that restrict users, such as disabling iTunes on iOS or Game Center on macOS, can allow admins to enforce corporate culture while ensuring device security⁵.

Connectivity Delivers the Big Picture

People don't work with business apps in isolation. They rely on supplementary data from cloud-based sales apps, ERP tools, project management apps, and specialized tools that are tuned for specific line of business processes. These resources enhance and add value to emails, spreadsheets, and other productivity documents by providing essential context. VMware Workspace ONE powers those inter-app synergies with smooth, intuitive connectivity.

For example, the SSO capabilities of Workspace ONE provide seamless connectivity between VMware productivity apps that are used to access Office 365; Microsoft productivity apps; and every other app that the organization employs. This secure yet frictionless connectivity lets business users easily move between apps to share data, analyze more effectively, and build insights.

Multi-Tenancy Enables Scalability and Simplicity

An effective digital workspace solution should support multi-tenancy, for common access and simplified app administration. Under a multi-tenant architecture, a single instance of the software can support multiple organizations (tenants) within a large organization.

Workspace ONE supports a flexible hierarchy of users, use cases, and geographies within the larger organization. As organizations scale and expand their digital workspace, they can inherit the settings that make sense and change only the settings that are different for each user group, use case, or geography. This lets organizations scale their digital workspace on a linear basis to all their use cases, without increasing the work that IT requires to manage the solution. It also provides an additional layer of security, configuration, customization and access control.

A Superior Experience Across Applications

Once they have enjoyed the freedom of choice and self-service flexibility of the consumer world, employees have high expectations for workplace tech. Many organizations view these consumerized employees as a risk, because they are willing to

⁵ Principled Technologies, "Simplify digital workspace management for admins", September 2017

sidestep IT and move forward with their own technology initiatives. However, rather than fearing the risk of shadow IT, organizations can empower users to do their best work, without compromising security and compliance. A digital workspace delivers the convenient access users crave, and empowers them to be more collaborative, productive, and make better, faster decisions. According to Forbes Insights, employees working in digital workspace environment report a significantly greater impact on personal productivity (63%) than on accomplishing more in a typical workday (38%), with the help of business apps⁶.

For a smooth, frictionless experience, Workspace ONE uses mobile SSO to guide users through their Office 365 experience throughout their employment lifecycle—from their first day, through their work days, to their last day.

For organizations using Office 365, Workspace ONE improves the experience by offering:

- Easy, self service enrollment of devices
- Intuitive access to apps through a centralized catalog enabling users to sign in across different apps and ecosystems in a way that's both secure and convenient
- Authentication and federated identity management that integrates with Microsoft Active Directory or any LDAP service
- Built-in, mobile-push, multi-factor authentication (MFA)
- Support for third-party strong authentication, including an identity provider for SAML and Web Service Federation-supported (WS Federation) apps
- Brokering for third-party authentication services such as Radium, Symantec, and RSA SecureID, and compatibility with existing identity providers
- Connections to other applications and services users need to add context and value to Office 365

At the end of the user's time with the company, Workspace ONE makes it easy to remove all their data to minimize risk for the user and the company.

Conclusion

To establish an employee-centric workplace, it becomes vital for organizations to remain agile and competitive. Enterprise apps play an important role in enabling business professionals to be more productive and collaborative. But to make the most of that potential, organizations need a strategy and platform that enables them to securely and reliably deliver the apps and data employees need to work—across any device.

Adopting Office 365 and VMware Workspace ONE puts the digital workspace in reach, providing a simple, secure platform solution to meet today's challenges and expectations. Microsoft Office 365 can be an integral part of the digital workspace, but to make the most of it, organizations need to support it with a strategic foundation. Workspace ONE provides a variety of rich capabilities that are not available in Office 365 and its associated management tools. From basic MAM/MDM features to advanced management and low-cost management, Workspace ONE enables organizations to support a production deployment and beyond, including specific use cases and customized workflows.

GET STARTED TODAY

To learn more about how a digital workspace can help your organization, visit www.vmware.com/go/digitalworkspace.

⁶ "The Impact of the Digital Workforce," Forbes Insights, 2017



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: Untitled-1