White Paper

Integrate Office 365 with a Digital Workspace Platform to Empower Employees Securely

A modern unified endpoint management approach delivers controls for maximum productivity *and* compliance

By Mark Bowker, ESG Senior Analyst

February 2018

This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

Contents

Office 365 Everywhere Empowers the Workforce but Extends IT Complexity 3
The Influence of BYOD and Mobile Device Management 3
Mobile Application Management and the Digital Workspace 4
Productivity and Security: Better Together 4
Four Management Components Associated with Office 365 5
Critical Security and Management Considerations 6
Authentication 6
Conditional Access 6
Information Protection 6
Data Loss Prevention 7
Extending the Baseline with Workspace ONE and Office 365 Integration 7
The VMware Workspace ONE Environment 8
Authentication 8
Conditional Access 8
Information Protection and Data Loss Prevention 9
Enhanced Office 365 Management 9
The Bigger Truth 10

Office 365 Everywhere Empowers the Workforce but Extends IT Complexity

The growth of Microsoft Office 365 subscriptions is showing no sign of slowing, nor are the information sharing capabilities the company is adding to its software and services. The number of commercial seats exceeded 120 million units in 2017 and grew 30% last quarter. Driving that growth are several factors, including the workforce empowerment and productivity improvement it provides, a constant stream of new capabilities that arrive in monthly updates, and the considerably lower operational and capital costs it offers by eliminating the need to run Microsoft Exchange and SharePoint infrastructure on-premises. In many scenarios, OneDrive for Business, which has become the file and content storage repository for SharePoint Server, and Office 365 SharePoint Online can replace the need for file servers.

These benefits come with new complexities for IT, which are not trivial. Fortunately, IT can now provision and manage Office 365 licenses in concert with employees' client computing devices, smartphones, and other applications. This report covers the technical, operational, and security benefits of managing Office 365 in tandem with your organization's devices in the context of the underlying complexities.

Besides the reduced cost of owning and maintaining Exchange Server and SharePoint infrastructure, the most significant change introduced when switching to Office 365 is the number of installs available to each user. Instead of having one email, SharePoint, and Office license and client installed on a single system, users can now have multiple installs—in most cases, up to five PCs/Macs and five smartphones and tablets. In addition to running on their company-issued systems and devices, the Office 365 license allows employees to download the software onto their own personal computers, phones, and tablets. For many organizations, that can open a Pandora's box. If not managed correctly, suddenly any employee can have access to files and other information assets on their own systems. Even if IT is aware of this, administrators no longer have any control.

Like any major enterprise IT initiative, large organizations don't switch to Office 365 overnight. It's an incremental process and, depending on the number of employees, can take place over many months or multiple years. Whether your organization is considering the move or is at any stage of already doing so, it makes sense to evaluate the notion of managing all aspects of Office 365 and other SaaS apps the same way you provision PCs and provide access on employee-owned devices, software, and services. A unified approach not only provides a more secure environment for all of your data but provides flexibility to move to any number of digital workspace options, perhaps multiple topologies, depending on the type of workforce your organization employs.

The Influence of BYOD and Mobile Device Management

Now, thanks to some new technical advances, IT can manage Office 365, which is the conduit to an organization's information assets, using the same approach, policies, and tools that enabled bring-your-own-device (BYOD) policies—namely VMware AirWatch and now, VMware Workspace ONE, powered by AirWatch. The complexity of managing Office 365 has many similarities to the issues IT grappled with a decade ago when almost everyone in the workforce had a personal smartphone and tablet. Consequently, organizations saw the benefit, or need, to create BYOD policies. The flexibility that BYOD and mobility have given to employees has helped organizations become more efficient and responsive.

The enterprise mobility movement and BYOD might not have gained acceptance and accelerated at the pace and scale that occurred among enterprises had it not been for the availability of mobile device management (MDM) tools. MDM tools enabled IT to enroll devices and users, segregate personal data from business information, and remotely wipe all enterprise data from devices that were lost or had belonged to terminated employees. The absence of these tools would have made managing and securing these enterprise resources a nightmare for IT.

Mobile Application Management and the Digital Workspace

As a result of the need to manage access to applications and services such as Box, Dropbox, Google Drive, and OneDrive, many MDM tools have evolved to offer mobile application management (MAM). The capabilities of MDM and MAM have enabled organizations to create digital workspaces for their employees. The digital workspace gives employees an image on whatever device they're using based on their identities. Workspaces are provisioned upon successful authentication, based on employee identities, their roles, permissions, and the associate apps and data they require for everyday use. Office 365 should not only be included in the digital workspace, it's the best case yet for moving to the digital workspace platform.

There's even more justification for moving to the digital workspace model. Now that Microsoft has released its Graph APIs, IT organizations have the option of applying the data retention capabilities built into the Office 365 platform as well as the Intune management interfaces in a uniform manor. Effectively, Office 365 is MAM-enabled. While MDM and MAM solutions are now designed to manage SaaS apps, Office 365 is more than just another service. It includes Exchange Online, SharePoint Online (including OneDrive for Business), Power BI, Skype for Business, and the new Microsoft Teams chatbot platform, among others.

Productivity and Security: Better Together

As companies continue to embrace Office 365, they must factor in a variety of circumstances. The traditional IT "balancing act" between ensuring security and enabling productivity in which one is favored at the expense of the other is no longer feasible. Both productivity and security are now data center requirements, not subject to compromise. Employees and executive leadership won't accept clunky experiences or limited access to information when they need it without interruption. Yet the business can't afford loss of data or security breaches. It's vital that IT management and CISOs ensure device compliance at a time when attacks and breaches have reached epidemic proportions. As an IT professional, what do you do?

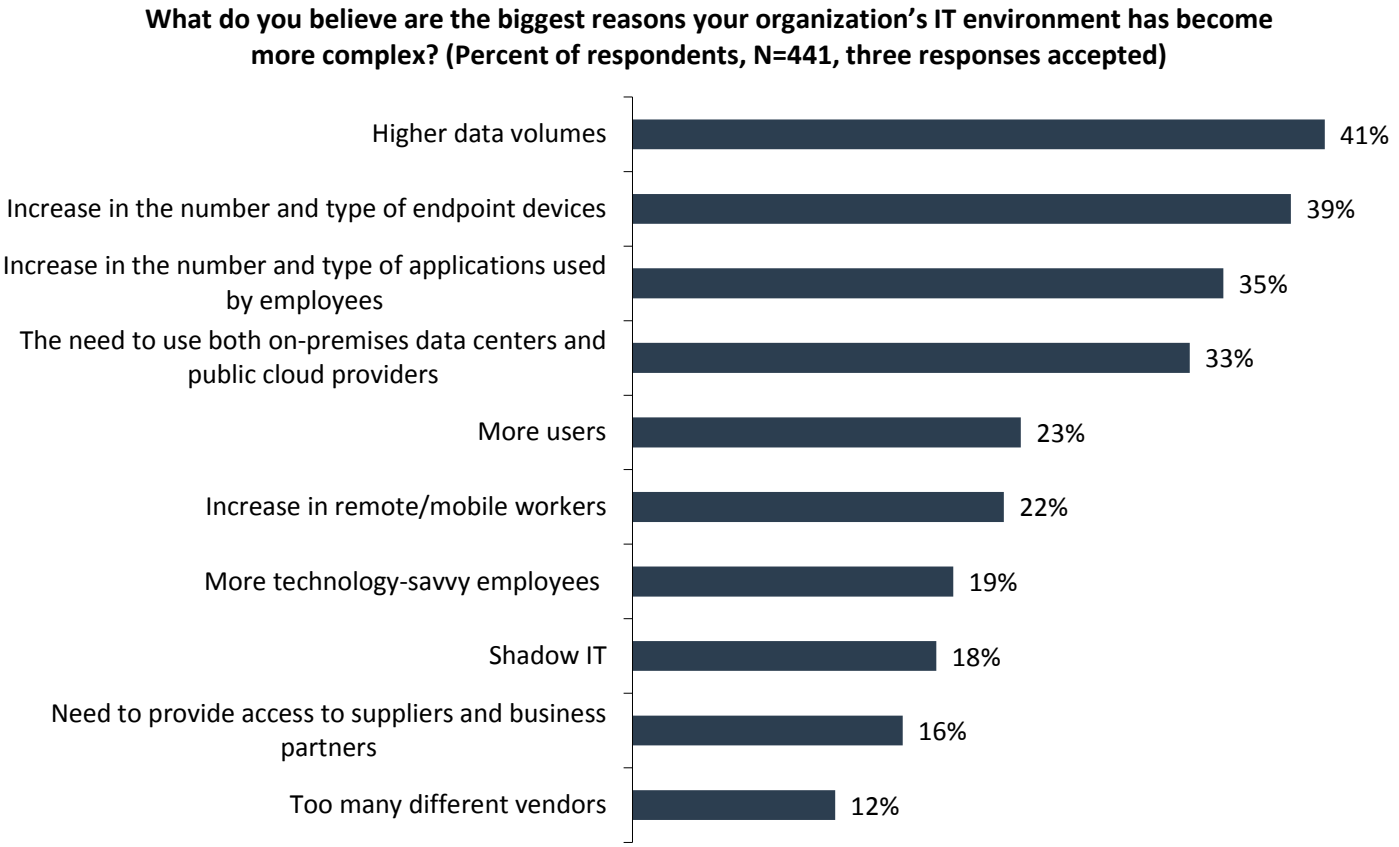
The primary goals for any organization should be to improve:

- Employee productivity.
- Security posture.
- Operational management of IT.

As companies look to achieve these goals, there are IT complexities that can't be ignored. A recent ESG research study revealed that IT organizations are feeling the squeeze of having to manage increasing amounts of data, applications, devices, and users (see Figure 1).[1] While IT decision makers have to address these and many other issues, this issue can no longer be approached as a balancing act. It's unacceptable to compromise one requirement in favor of another. Security and productivity are both vital to the success of any organization in today's economy. The ESG research shows the complexity that IT organizations must contend with in their environments. There are more data, applications, and ways of accessing them than ever. And based on the soaring growth of Office 365, which in many enterprises is evolving into the source of the core information assets and productivity platform, managing all the pieces has become a critical IT priority.

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Figure 1. Factors Influencing Increased IT Complexity



Source: Enterprise Strategy Group

Four Management Components Associated with Office 365

The percentage of organizations facing the complexities raised in this survey validates the need for a long-term strategy for Office 365 that will ensure a reliable and uniform capability to manage:

- **Applications:** At its core, Office 365 is a suite of numerous applications—many that are used daily and often together—including Word, Excel, PowerPoint, Outlook (for email, calendaring, and contact management), Teams, Skype for Business, and others.
- **Data:** The above-mentioned applications and all information traditionally stored on a client device, file server, or online using OneDrive for Business as a common data store.
- **Devices:** Until a few years ago, Office apps primarily have run on Windows devices and Macs, though with some limitations on the latter until recently. Now, Office is available as a native app on iOS, Android, and Chromebooks, and with vastly improved browser functionality. Equally significant is Microsoft's license model for Office 365 that lets an employee run the full Office Suite on multiple PCs, Macs, and mobile devices.
- **Users:** Like all other SaaS offerings today, Office 365 is licensed by the user rather than the device. And now that each user has the license rights to Office 365 on multiple devices, either enterprise-controlled or employee-owned, IT must manage all four of these components together and in context.

Critical Security and Management Considerations

In many work environments, Office 365 is one of the first services people log on to each day, whether to check email or access a file. Employees can access their Office 365 accounts using their Azure Active Directory credentials from their company-issued systems and their personal devices anywhere. But just as organizations now use MDM and MAM tools to deploy and manage mobile devices and, increasingly, Windows 10-based PCs and MACs, it makes sense to use these tools for the rollout and de-provisioning of Office 365 services, using the same user profiles and policies.

As organizations incorporate Office 365 into their BYO initiatives, it's critical they ensure that they are implementing the strongest and most flexible security controls. The four most critical security controls for Office 365 are authentication, conditional access, information protection, and data loss prevention. It's important to look at the capabilities of those four controls.

Authentication

As a company's security perimeter expands with the adoption of cloud-based applications accessed from multiple devices, users can now run them from locations with varying degrees of security with authentication as the first point of entry. The most effective authentication will ease the burden for IT and security teams and vastly reduce the risk of unauthorized access to Office 365 accounts. Authentication to access Office 365 should include the following attributes:

- Support for standards-based authentication: SAML, OAuth, and FIDO, which support single and multifactor authentication.
- Integration APIs with application activation and provisioning platforms.
- Universal single sign-on (SSO).

Conditional Access

While strong authentication greatly reduces the risk of data loss, IT organizations can gain further assurances by only allowing access to information under certain conditions, hence the term "conditional access." The number of conditions is infinite, as are the number of policies and how they're defined. When it comes to Office 365 and protecting an organization's key information assets, conditional access should include the:

- Ability to grant access to enterprise information based on the location, network type, and device type.
- Sensitivity of the data and trust level of the user based on their role and use of authentication.
- Data loss prevention and information protection policies and other risk factors.
- Implementation of polices based on certificate-based authentication.
- Rules engine that provides real-time compliance (RTC) based on customized policies, escalation, and platform-specific rules.

Information Protection

IT is shifting more attention to protecting information as digital workspaces have made it more difficult to predict where, when, and how a user will access and share information. Effective information protection ensures data is protected through strong:

- **Data classification:** The notion that all information is accessed and shared based on an organization's security posture, user roles, and compliance requirements among other factors set in policies.
- **Rights management:** The ability to lock down access and/or sharing of data using various forms of security including encryption, based on defined policies and controls.
- **Encryption:** Ensuring effective rights management requires appropriate levels of encryption and levels of authentication.

Data Loss Prevention

Detecting potential misuse of data or breaches and blocking access to data are important as data traverses devices, networks, and data stores. There are many controls IT can set up to remove the opportunity for employees to forward or copy information. Among the capabilities IT should have to make sure adequate data loss protection is upheld include:

- **Policies**: Organizations can now protect information at the file level by implementing policies that prevent employees from copying, printing, emailing, or storing data anywhere outside of pre-defined criteria. It's important for IT to be able to implement policies that are dynamic and granular to accommodate various conditions, and to meet regulatory requirements. This will become paramount in May 2018 when the European GDPR rules take effect.
- **Detection and monitoring**: It is important that attempts to skirt these policies or other suspicious activities be monitored and detected with automated remediation.

Companies also should be aware that Office 365 and associated solutions from Microsoft provide basic built-in capabilities to address these issues. However, IT leaders need to think beyond these basic capabilities and consider how investments in a platform such as VMware Workspace ONE can help them achieve their short- and long-term goals of securing delivery of applications and data.

Extending the Baseline with Workspace ONE and Office 365 Integration

We've established that Office 365 is a good starting point for building a digital workspace built around the notion of unified endpoint management (UEM). Now, IT managers in pursuit of UEM should consider a digital workspace platform that can address the security and data protection requirements listed above, deliver as much as their organization feels is suitable and desired on a self-service model, and support every major platform, app, and service. The VMware Workspace ONE, powered by AirWatch, solution is among those that every IT team should have on its shortlist of UEM platforms to evaluate. In many independent benchmarks, critics have rated it the most secure and feature-rich digital workspace environment.

Because the MDM and MAM tooling of Workspace ONE now has the Microsoft Graph APIs built into it, organizations can extend the Intune, identity, and rights management capabilities built into Office 365. Workspace ONE can extend these capabilities with its extensive list of added security and management features, including single sign-on, with advanced authentication and conditional access as well as the ability to containerize data. While Office 365 is the start, it creates the baseline to extend UEM to other SaaS and mobile applications made available to employees. Why is this necessary?

Current desktop, application, and security management tools will become cumbersome to maintain across a variety of devices, cloud consumption models, and application types, and are candidates ripe for a unified approach. IT leaders are well advised to consider a modern unified management approach for desktops, applications, mobile devices, and security to achieve the goals of enhanced employee productivity while protecting (securing) the expanded perimeter among different IT silos.

The VMware Workspace ONE Environment

Beyond the basic proof of concept stage, VMware Workspace ONE has incorporated numerous capabilities into its feature set to help deploy and manage digital workspaces with success.

Authentication

End-users should be able to easily access the information they need with the strongest and most extensible authentication possible. IT and business executives are coming to terms with the fact that this means that multifactor authentication should no longer be an option but a mandate. The SSO capabilities of Workspace ONE provided with VMware Identity Manager enable end-to-end authentication from Workspace ONE to VMware Horizon virtual desktops and apps for a secure and simple user experience. Users aren't prompted for multiple logins once they've authenticated into the Workspace ONE portal or native app. Workspace ONE supports the key authentication standards including SAML, OAuth, and FIDO, which enable single and multifactor authentication, as well as single sign-on.

Given that many organizations have multiple platforms for supporting authentication to various silos and business units, the Workspace ONE console provides access and app activation for key authentication and single sign-on platforms such as Active Directory Federation Services, Okta, Ping Identity, and others, which are common conduits to Office 365, as well as Azure Active Directory. In regulated environments such as financial services, health care, and law enforcement, where multifactor authentication is already a long-established norm, Workspace ONE addresses those mandated directives, with support for standards such as the Federal Information Processing Standard Publication 201 (FIPS 201), the U.S. government standard that specifies Personal Identity Verification (PIV) requirements for federal employees and contractors for smart cards, or common access cards (CAC) for access to physical, logical, and network resources.

VMware Workspace ONE also supports the more modern PIV-D standards for managing credentials when using mobile devices to access physical, logical, and network resources. VMware PIV-D Manager uses derived credentials with native apps and profiles to access VMware apps and third-party apps easily embedded with the Workspace ONE SDK. PIV-D Manager also integrates with other derived credentials solution providers. Workspace ONE now supports the Revoke Azure Refresh Token, which means Workspace ONE can actively reach out to O365 and revoke the refresh token before it has expired—killing all access and forcing users to re-authenticate.

Conditional Access

As previously noted, implementing the most suitable authentication requirements is critical, but equally important, with today's mobile and multi-device workforce, is conditional access. VMware Workspace ONE offers several approaches to providing conditional access. Smart Policies are available in VMware Horizon 7 and VMware Horizon Cloud for IT to provide end-users with a truly contextual user experience. For example, policies dynamically change depending on the device used or the location services being accessed from.

Client policies such as enabling or disabling clipboard redirection, USB, printing, and more can be set by IT using Smart Policies. Horizon is certified to meet FIPS 140-2 and Common Criteria requirements using the secure procedures powered by Smart Policies.

Workspace ONE integration with the VMware Horizon desktop and VMware NSX network switch also provides conditional access to applications on mobile devices and data center resources using tunneling and micro-segmentation for an extra layer of security. This lets IT operations and InfoSec teams secure east-west traffic within the data center, preventing malware from spreading across the data center if a virtual desktop is compromised. That's possible because each desktop is effectively isolated from other desktops. IT can quickly and easily administer networking and security policies that dynamically follow end-users' virtual desktops and apps across infrastructure, devices, and locations. Each app creates its

own VPN session, which connects to a virtual switch that determines compliance, then authenticates through any of the identity providers including Office 365.

The latest announcements from VMware introduce the concept of intelligent security. As usage data and device health data is reported to the Workspace ONE Intelligence service, that data may be correlated to both produce management insights about usage optimization, and, more importantly, allow VMware and third-party security partners to apply algorithms that can predictively determine risk. The Workspace ONE Intelligence service can then automate the response to mitigate those risks in near real time. Intelligence simply means IT can see more, react faster, and protect the user. Eliminating blind spots and tapping into third-party security partners helps protect the security perimeter and defend against cybersecurity risks.

Information Protection and Data Loss Prevention

Aside from native OS-provided DLP controls for managed apps on iOS/macOS and/or the Samsung KNOX/AfW containers on Android, Workspace ONE provides additional DLP controls via the Workspace ONE SDK that are very useful for unmanaged/BYO devices and personal cloud services.

The Workspace ONE SDK provides a comprehensive data loss prevention (DLP) solution that enables administrators to tightly control and restrict users' ability to leak content outside of corporate control. It provides the ability to encrypt data; provide authentication for application access; block copy/paste functionality; restrict network access; provide time-based access control; enable geofencing to access content; control open-with functionality; and block export, printing, back up, copying of company information onto external SD cards or remote cloud backup solutions, and capturing of screenshots.

Enhanced Office 365 Management

VMware Workspace ONE can also secure and manage Office 365 in other ways beyond the tools offered by Microsoft using the enhanced data loss prevention and rights management services built-in and several other components recently added by VMware. Among them are:

VMware Boxer

If you prefer Outlook, that's fine, but Boxer offers a user experience that's more flexible and intuitive. It provides more advanced, customizable, and predictive capabilities for managing email, schedules, and contacts. Boxer also provides IT and SecOps more granular controls with data at-rest and in-transit 256-bit encryption, and support for advanced data loss protection that can encrypt critical information and prevent sharing, thereby providing built-in compliance and container options. Boxer also supports:

- Reading and enforcing as well as composing information rights management (IRM) secured emails.
- S/MIME with PKI.
- Email classifications that interoperate with Exchange transport rules and third-party DLP solutions like Titus, JanusNET, and Boldon James.

VMware Content Locker

Organizations can also provide centralized and secure access to Office 365 documents with VMware Content Locker, a file and sync platform that provides access to OneDrive, Google, Box, Dropbox, and more than 30 other content service repositories. Among other features, it provides:

- Reading and enforcing RMS of protected documents.

- Document expiration.
- Document watermarking.
- Controlled open-in.
- The ability to disable printing.
- The ability to disable offline viewing.
- The ability to disable access while roaming.
- Restriction of transfer method to Wi-Fi only.

Secure Email Gateway

VMware Workspace ONE Secure Email Gateway (SEG) filters every communication request from a device, relays traffic from approved devices, and protects the corporate email server by not allowing any devices to directly communicate with it. This ensures email attachments and hyperlinks can be opened only through VMware Content Locker and VMware Browser to protect enterprise information. The gateway also:

- Provides content transformations to prevent sensitive information (i.e., PII) from syncing down to a mobile email client.
- Verifies device compliance before allowing access to synchronize.
- Provides attachment encryption.

The Bigger Truth

For companies seeking to leverage existing security investments or augment VMware deployments with an enhanced level of security, VMware Workspace ONE has integrated with an ecosystem of mobile security vendors in the VMware Mobile Security Alliance. Workspace ONE integrates with technologies from the Mobile Threat Defense partners, Cloud Access Security Brokers, partners, and others to further enable comprehensive cybersecurity across mobile devices, apps, networks, and cloud services.

Office 365 is a popular option to modernize how information is created, gathered, and shared but it unleashes a whole set of risks if not managed and secured properly. A digital workspace environment with robust controls and flexible options such as Workspace ONE lends itself well to ensuring that enterprise information assets are controlled throughout the lifecycle of the information and only available to those authorized to access them. As strategic as Office 365 is, there are many other apps, SaaS services, device types, and usage environments that IT must manage and protect. It's important to remember that most companies will require capabilities beyond the basics to manage and secure Office 365. They'll need a solution that is applicable across a variety of applications, data sources, devices, locations, employees, contractors, and business partners and that has a large ecosystem of security, software, and IT service providers.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188