

## ESG Brief

# VMware Workspace ONE: Meeting the Demand for an Intelligence-driven Workspace

**Date:** April 2018 **Author:** Mark Bowker, Senior Analyst; and Leah Matuson, Research Analyst

**Abstract:** VMware's new innovations to its Workspace ONE platform can help organizations as they transform legacy and siloed infrastructures into modern digital environments. The vendor continues to build in management and security features, which match the heterogeneous environments that IT and security professionals are managing and securing. Workspace ONE also inspires different teams (i.e., IT operations, and information security) to work together to address security concerns, while remaining focused on the end-user experience, and productivity. With the new innovations to Workspace ONE, IT can recapture control over applications and devices. VMware Workspace ONE helps them maintain a level of consistency and security, allowing them to take back control, and embrace new applications, devices, and workstyles.

## Overview

While cloud and mobile initiatives are helping businesses grow and flourish, there is a price to be paid as the security perimeter evaporates. The potential for data breaches and cyber-attacks is rising, further driving security as a key priority for businesses across industries. Siloed IT groups possess limited visibility across an organization's ecosystem due to the legacy and standalone solutions that they continue to rely on, and are unable to provide adequate protection for business-critical and personal data, devices, and applications against relentless bad actors and cyber-attacks. In fact, based on ESG's 2018 IT spending intentions research, 63% of organizations surveyed indicated that they will increase cybersecurity spending in 2018. Thirty-seven percent of respondents reported that data security was one of the areas related to cybersecurity in which they expect to make significant investments over the next 12-18 months.<sup>1</sup>

While working anywhere, anytime, on any device may be great for end-users (offering a boon to productivity), "bring your own device" initiatives can wreak havoc among IT organizations—especially when managing endpoints and securing the enterprise. But how can enterprises gain real-time visibility into their dynamic environments, ensure 24/7 protection from risk and attack, and deal with increasing operational costs and constrained IT budgets?

<sup>1</sup> Source: ESG Master Survey Results, [2018 IT Spending Intentions Survey](#), December 2017.

## VMware Workspace ONE, an Intelligence-driven, Secure Digital Workspace Platform

For two decades, VMware has been an innovator in the industry, growing into a leader in enterprise software and services. Recently, the vendor announced several intelligence-driven innovations to its Workspace ONE platform, including Workspace ONE Intelligence, Workspace ONE Trust Network, and Workspace ONE AirLift.

These new Workspace ONE innovations are designed to address the demands of the modern workforce (e.g., computing anywhere, anytime, on any device), by integrating actionable insights across devices, users, and applications, while enabling predictive and automated security across the enterprise.

Workspace ONE Intelligence, the vendor's cloud-based service, collects and correlates data from devices, users, applications, and networks, allowing organizations to leverage that data to obtain actionable recommendations and benefit from time-saving automation. This new digital Workspace ONE solution can enhance the user experience by enabling IT to detect and resolve issues before they impact user productivity, allow for employee-friendly access policies, and mitigate potential risks to security.

Workspace ONE Trust Network, another new innovation, provides organizations with predictive and automated security from a new network of VMware trusted security partner solutions.

Workspace ONE AirLift is a new Windows 10 co-management technology that can assist organizations in modernizing their PC lifecycle management, saving IT valuable time and expense.

### Highlights of Workspace ONE Intelligence include:

- **Integrated insights.** Integrated insights combine actionable information and recommendations throughout an organization's entire digital workspace across all devices, applications, and networks, presenting IT with one easy-to-understand view.
- **Automated remediation across an organization's environment.** Automated remediation is powered by a decision engine, which can help IT create and automate common tasks, including remediation for Windows 10 endpoints, with the ability to set group or individual conditional access controls to applications and services. With Workspace ONE Intelligence, IT is also able to establish automated rules to include workflows with other third-party services including ServiceNow or Slack.

**Workspace ONE Trust Network** addresses the challenges organizations experience when working with outdated and disjointed solutions and siloed IT groups. By extending Workspace ONE Intelligence and its APIs, VMware's security partners can now share and correlate threat data with Workspace ONE. This will provide shared customers with data insights and automation across their ecosystems. Carbon Black, Netskope, and Symantec are just a few of the VMware partners that will integrate their security solutions with Workspace ONE as part of the Workspace ONE Trust Network.

**Workspace ONE AirLift** is designed to help organizations make the transition from legacy Windows management models to a modern management approach. According to VMware, Workspace ONE offers the only unified endpoint management (UEM) platform with integrated intelligence, supporting all stages of the Windows 10 PC lifecycle. This innovation will enable co-management of Windows 10 PCs alongside Microsoft System Center Configuration Management (SCCM), enabling organizations to swiftly transition to the modern model without the expense of replacing SCCM PC and server upgrades.

In addition to these three key products, VMware also announced the following innovations to Workspace ONE:

- **Streamlined Mac adoption.** A new Workspace ONE client for macOS allows employees to move between OS platforms and access all applications from the macOS device, including virtual Windows applications.
- **Extended security for O365 applications.** Microsoft Graph APIs are now integrated into Workspace ONE, providing organizations with O365-specific security features comprising new data loss prevention (DLP) controls and continuous device risk monitoring.
- **VMware Boxer with intelligent workflows.** This addition allows users to perform tasks across a number of business applications (e.g., Salesforce, Jira, or Concur) without having to leave the Boxer email application.

VMware also announced a beta test for VMware virtual desktops with Azure infrastructure in partnership with Microsoft. VMware Horizon Cloud on Azure VDI will expand on VMware's support for published applications on Azure.

### Availability and Pricing

According to VMware, Workspace ONE Intelligence is now generally available, and is included in the new Workspace ONE Enterprise package. Horizon Cloud on Azure VDI is expected to be available Q2 in fiscal year 2019, in more than 40 global regions. Interested customers can contact VMware to sign up for the beta program.

### The Bigger Truth

VMware's new Workspace ONE platform innovations can help organizations as they transform legacy and siloed infrastructures into modern digital environments to keep pace with today's demanding workforce. These innovations offer organizations the ability to leverage business intelligence, gaining actionable business insights, while protecting business-critical and personal data from potential risk and cyber-attacks.

The Workspace ONE innovations come at an interesting inflection point as businesses evaluate and invest in a built-in or bolted-on security strategy. VMware continues to build in management and security features, which match the heterogeneous environment that IT and security professionals are managing and securing. Workspace ONE also inspires different teams (think IT operations and information security) to work together to address security concerns, while remaining focused on the end-user experience, and productivity.

Workspace ONE has the ability to provide the consistency businesses require as they step through a digital transformation. Applications, devices, networks, and employees will all change—but having a platform that can manage a user's identity, apply policy-based access controls, and monitor behavior will enable businesses to quickly and easily adapt to change. With the new innovations to Workspace ONE, IT will no longer have to lose control over applications and devices. VMware Workspace ONE helps them maintain a level of consistency and security, allowing them to take back control, and embrace new applications, devices, and workstyles.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



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

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

