

ESG Economic Validation

Analyzing the Economic Benefits of VMware Workspace ONE Access Cloud-hosted Option









By Aviv Kaufmann, Senior Validation Analyst
April 2020

Executive Summary

Never before has the ability to work from remote locations been so important to business continuity. Giving remote workers the freedom to work from any location, on any device, while still having access to critical and secure company assets is paramount to the success of most operations. Being physically present in the office or place of business is no longer a critical prerequisite for productivity. In fact, by eliminating commutes and long lunch breaks and minimizing the chance of unexpected proximity-based interruptions and non-business-related interactions, some might argue that working remotely at times presents the opportunity for increased levels focus and productivity. The increased accessibility can speed up task flow-related processes (like waiting for authorization on a prescription or sharing a document for a colleague) that otherwise might have taken a day or more waiting for human interaction to a few minutes. Whether workers are working remotely by choice or for reasons outside of their control, the burden falls on IT to deal with the complexity around providing secure access across a large number of devices, users, locations, and applications.

ESG validated that VMware Workspace ONE Access, deployed in the cloud and used in conjunction with other Workspace ONE components, has significantly reduced IT complexity and provided enhanced business agility while providing end-users with a secure, consistent, and simple experience for all applications. Organizations rolled out applications faster and allowed employees to focus on doing their job rather than wrestling with technology and logins.

Validated Benefits of Workspace ONE Access Deployed In the Cloud

 <p>Consistent and simplified end-user experience</p>	 <p>Improved remote worker capabilities</p>
 <p>Reduced IT operational complexity</p>	 <p>Fewer support issues and greater visibility</p>
 <p>Faster time to value</p>	 <p>Faster rollout of new applications and updates</p>
 <p>Improved business agility</p>	 <p>Accelerated path to Zero Trust security</p>

Introduction

This ESG Economic Validation focused on the benefits that organizations can expect by deploying VMware Workspace ONE Access in the cloud to deliver consistent, enterprise-wide access to applications and data from any device in any location.

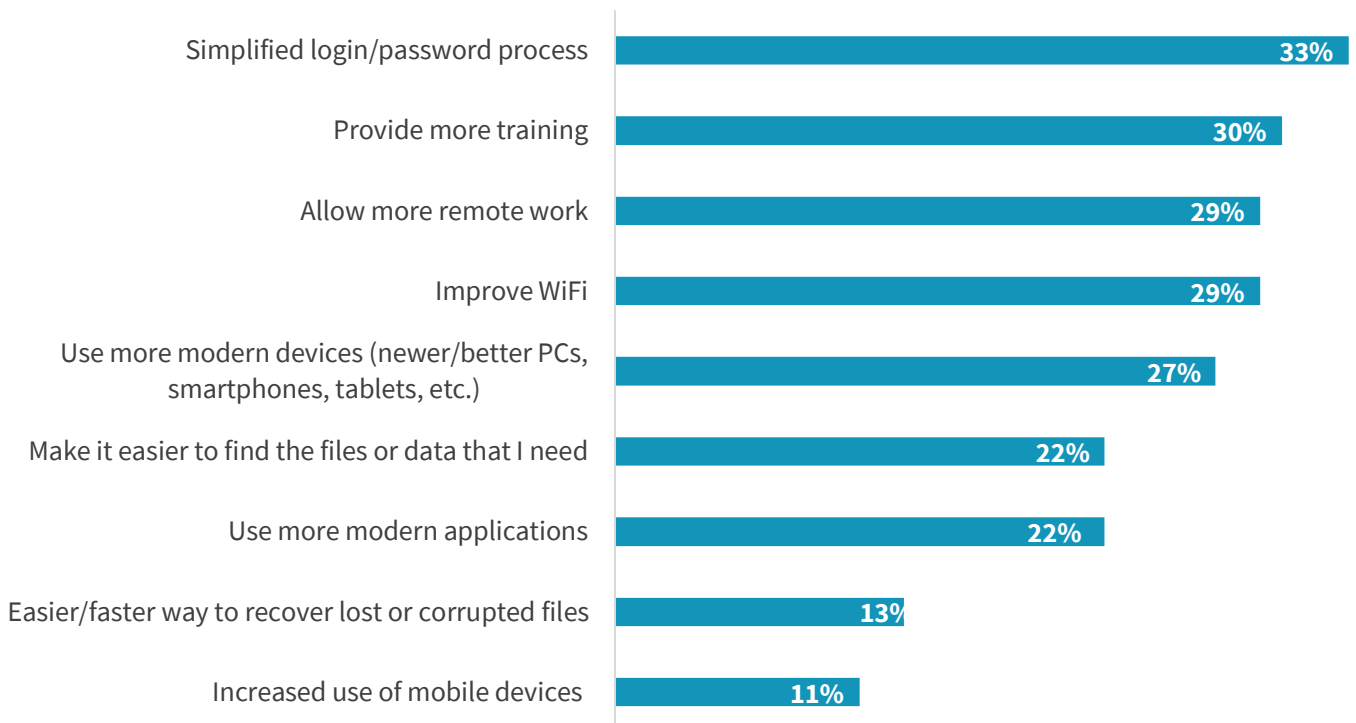
Challenges

Digital transformation initiatives have tasked IT organizations to better support an increasingly mobile workforce across a much wider range of end-user devices. ESG research reveals that 70% of all workers expect to be productive from anywhere, and 57% of all workers expect to be able to perform the majority of their job functions from any device.¹ Supporting a positive end-user experience across an increasing number of access locations, application versions, device types, and operating systems places a substantial burden on IT organizations. Unified endpoint management (UEM) solutions like VMware Workspace ONE help to relieve the management burden on IT through automation and consolidation of the management silos around supporting a variety of end-user devices.

While UEM helps on the device side of operations, providing end-users with a secure and consistent application experience on their choice of device is an increasingly difficult task, especially as more organizations are tasked with supporting a mix of modern cloud-based applications and legacy on-premises applications. End-users have become accustomed to a simplified experience for their personal applications and are demanding the same seamless experience in their professional life. But each SaaS and on-premises application may require a separate set of login credentials, interrupting end-user productivity and increasing frustration and “login fatigue.” It is no surprise that respondents most often identified a simplified login/password process as an improvement that they would like to see from their company in terms of the technology experience it provides (see Figure 1).

Figure 1. Most Important Company Improvements Affecting End-user Technology Experiences

What improvements would you like to see from your company in terms of the technology experience it provides? (Percent of respondents, N=1,033, multiple responses accepted)



Source: Enterprise Strategy Group

¹ Source: ESG Research Report, [2019 Digital Work Survey](#), December 2019.

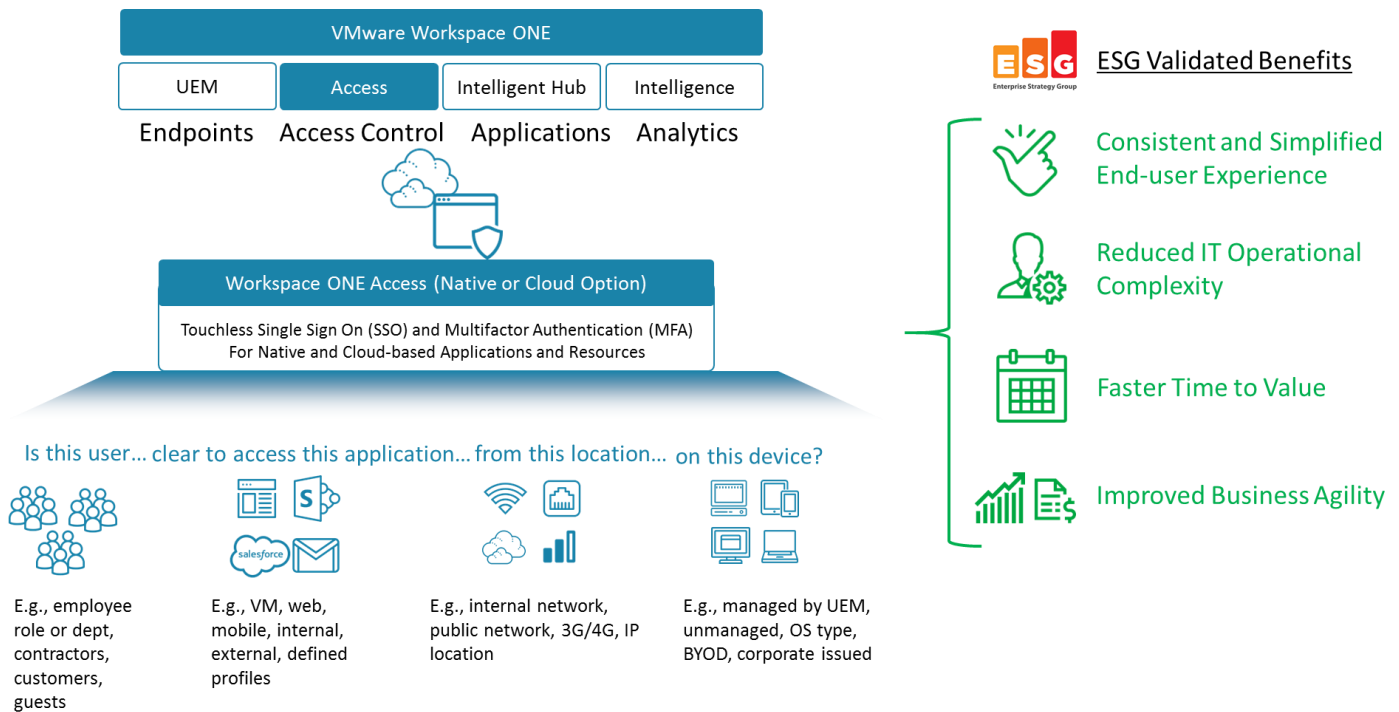
The burden once again falls on IT to provide consistent and simplified application access from any device while transparently dealing with the underlying complexities around secure application deployment and intelligent access decisions across device types, networks, and a mix of cloud-based and on-premises identity stores.

The Solution: VMware Workspace ONE Access Deployed in the Cloud

VMware Workspace ONE Access (formerly VMware Identity Manager) combines the user’s identity with factors such as device and network information to make intelligence-driven, conditional access decisions for applications delivered by Workspace ONE. This enables organizations to quickly and more securely provide a consistent application access experience from any device.

Available as a cloud-hosted service, Workspace ONE Access is an integral part of the Workspace ONE platform and supports Workspace ONE Intelligent Hub, Workspace ONE Unified Endpoint Management (UEM), and VMware Horizon. Workspace ONE Access acts as a broker to other identity stores and providers—including Active Directory (AD), Active Directory Federation Services (ADFS), Okta, and Ping Identity—that your organization may already be using to enable authentication across on-premises, software-as-a-service (SaaS), web, and native applications without the need to rearchitect the identity environment. Its capabilities help ensure your organization can deploy new applications of any type with a consistent user experience.

Figure 2. VMware Workspace ONE Access Hosted in the Cloud



Source: Enterprise Strategy Group

The key features of Workspace ONE Access include:

- **Access broker:** Integrates with existing on-premises and cloud identity providers to reduce deployment times and enable more secure access to any application while improving user experience.
- **Adaptive MFA and SSO:** Provides native MFA or integrates with exiting MFA providers, and delivers SSO to web, SaaS, mobile, and legacy apps through integration with Workspace ONE Intelligent Hub.

- **Risk-based conditional access:** Uses dozens of access policy combinations that leverage device enrollment, network, SSO, automated device remediation, Workspace ONE Intelligence, and third-party information to establish levels of trust, enabling intelligent access decisions.
- **Cloud-hosted option:** Dramatically reduces implementation time and maintenance overhead.
- **Smarter digital workspace:** Unlocks new Workspace ONE features and capabilities, including Workspace ONE Hub Services and Workspace ONE Intelligence, on day one without scheduling and prioritizing upgrade cycles.

ESG Economic Validation

ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. ESG conducted in-depth interviews with end-users to better understand how Workspace ONE Access has positively impacted their organizations compared to the way that they previously managed user and device access before deploying Workspace ONE Access and taking into account any feedback that they had heard from end-users and business operations. The organizations included in the study consisted of larger enterprise organizations in the technology, finance, and healthcare verticals supporting more than 10,000 users and a mix of internal and public applications accessed by corporate-owned and BYOD devices including laptops, desktops, tablets, and phones.

Workspace ONE Access Economic Overview

ESG found that Workspace ONE Access had improved the overall effectiveness of their IT organization around device and application deployment, access, and security and allowed these organizations to provide the line of business with significant savings and benefits in the following categories:

- **Lower cost and faster time to value** – We found that Workspace ONE Access allowed organizations to lower both the expected capital and operational cost of managing devices and applications, while also minimizing the time required to roll out new services and applications.
- **Improved business mobility, agility, and flexibility** – Customers confirmed that Workspace ONE Access reduced a number of historical barriers to the speed of business by reducing the overall complexity of deploying and securing applications while providing a consistent application experience for end-users at any location on any device.
- **Reduced risk to the organization** – IT organizations were able to lower risk to the organization by lowering the risk of downtime and providing comprehensive security intelligence across users, endpoints, applications, data, and the network.



Cost Savings and Faster Time to Value

Workspace ONE Access allowed organizations to deploy and manage devices faster and more securely while reducing both capital and operational costs.

- **Faster time to value** – By choosing to deploy Workspace ONE Access in the cloud rather than on dedicated on-premises infrastructure, organizations were up and running in days to a week instead of months, allowing the organization to roll out services and realize economic benefits sooner.
- **Reduced management complexity** – Customers reported that Workspace ONE Access was very simple to configure and manage once rolled out, saving them considerable time that might otherwise be spent configuring access through several interfaces, and having to manage and configure end-user devices or applications in person. Workspace ONE enabled these organizations to consolidate several MDM solutions provided by a number of vendors into a single, easy-to-use solution. This reduced complexity allowed the IT resources to focus on initiatives like faster response to issues and new proactive projects.
- **Elimination of hardware** – Hosting Workspace ONE Access in the cloud eliminated the need to plan, purchase, deploy, maintain, update, and operate the physical hardware. All of the organizations that we spoke with that were running on-premises had chosen to move the deployment to the cloud and reported the many operational advantages of not having to deal with hardware and updates as well as improved system availability with automatic failover.
- **Faster rollouts of new applications** – Customers consistently reported the ability to onboard and roll out applications much faster than before, quoting a reduction from weeks (for a manual, helpdesk-led rollout) to

“Workspace One Access is very simple - there is not a lot of management overhead. We just set it and forget it. It was a game changer.”

“We are able to deploy mobile applications in minutes instead of 4 to 6 weeks of manual IT-led installation. Users can just go to one spot and get access to all of their apps.”

“We started with a small rollout and it worked great. Once people saw how easy it was, they wanted it. All of the sudden we had all these other departments that wanted their apps on there.”

minutes for a user-performed installation through Workspace ONE Intelligent Hub. End-users are automatically connected to Hub services for notifications and updates, and confusion is reduced with simple Mobile Flows for task workflow notifications. Overall burden on the IT resources was reduced, and applications are available for use faster, with fewer issues, providing modern capabilities to the business in less time.



Improved Business Mobility, Agility, and Flexibility

Workspace ONE Access works seamlessly with Workspace ONE UEM, Hub Services, and Intelligence to allow access to company resources from inside or outside the corporate network on any corporate controlled or BYOD device. This makes end-users more productive and allows the business to operate in an agile manner—quickly integrating modern applications and reacting to new opportunities that positively impact revenue.

- **Improved end-user experience** – Customers reported that end-users were thrilled with the Workspace ONE Access experience of app-store like simplicity and not having to wrestle with logins and passwords. IT organizations noted that they received far fewer complaints and support requests related to the inability to access resources after implementing the service.

“We wanted to let people focus on what their area of expertise was, without having to wrestle with the technology to connect.”

“We are giving our teams access to data that empowers them to do their job faster from anywhere in a very secure manner.”

Improved mobility and security for end-users – Workspace ONE Access allowed IT to allow workers to access applications and perform their job from locations that they were previously unwilling to support due to technical or security-related complexity. Workers felt that they were better able to do their job, and IT did not have to worry about many of the security issues that they had to deal with in the past. End-users reported much higher satisfaction with the technology services available to them and a reduction in frustration.

- **Improved end-user productivity** – Organizations received feedback from end-users that since the rollout of Workspace ONE Access, they have been able to focus more on getting their jobs done and less on the technology required to install applications, configure their device to connect to resources, and deal with logins and passwords. For some organizations, where end-users are not particularly tech-savvy, this can make a significant difference in productivity.



Reduced Risk to the Organization

ESG found that one of the key drivers for employing Workspace ONE Access was reducing risk to the organization, especially for those organizations that have employed a BYOD policy. By intelligently having greater control around who and what can connect to the network, and reducing the risk around the information that lives on end-user devices, the risk of a potential data breach is greatly reduced, and security teams can be freed up to focus on other threats.

- **Comprehensive security** – Workspace ONE Access provides a more comprehensive security model that combines information about the user, endpoint, application, data, and network before allowing access. Organizations felt this was far more secure than the previous method employed that simply required a username and password. One organization noted far fewer unknown devices on the wireless network since employing Workspace ONE.

“We had 4 variants of MDMs that were procured by different departments before consolidating with Workspace ONE. We had no idea of how many people were connecting with their own device to connect to our resources. This was difficult from a management, legal, and security perspective.”

- **Zero Trust security model** – Workspace ONE Access works in conjunction with other Workspace ONE components like Intelligent Hub, UEM, and Horizon desktops and apps to help organizations deliver a zero trust security model. A zero trust model powered by Workspace ONE combines intelligence around device, user, and network information to enable easier access for lower risk attempts and increased security measures for riskier access attempts. This allows organizations to operate safer, without compromising user experience.

- **More secure end-user devices** – Perhaps the biggest takeaway from our interviews was that organizations were thrilled that they were not only making end-user devices easier to use, but also making them more secure. In addition to making access more secure, one organization reported that their security team was thrilled with the fact that all data was encrypted in transit, there was no data stored on the device, and devices could be securely wiped of any access information if the employee were to leave the organization.

“With Workspace One Access there is no data stored on the device – it is provided through a URL and it is encrypted – there is never any data stored on the device. Our security team loves it.”
- **Lower risk of downtime** – Compared with on-premises deployments, cloud deployments help lower the risk of downtime by providing automatic failover and recovery with a 99.9% uptime SLA. Some organizations that we spoke with also leveraged cloud deployments as the DR site for an on-premises deployment. Automatic updates keep the deployment secure and reduce the risk of human error. In addition, VMware continuously monitors the environment to let you know everything is okay, or alert you if action is required.

“We have controls to make sure that every Workspace ONE user’s device is enrolled in Airwatch. If a person were to leave the company, we can make sure that we remove all of the company’s sensitive data.”
- **Less risk of human error** – Workspace ONE Access greatly simplified the process of configuring a device while also reducing the risk that the device may be configured improperly by an end-user, resulting in a call to IT, or by an IT professional, resulting in a potential unsecured device. The ability to provide a consistent end-user experience while hiding the complexities of constantly dealing with multiple MFA and SSO interactions for native and cloud services also reduces the chances of sensitive login information being lost or identified.

The Bigger Truth

As IT organizations look to modernize, they are hard pressed to empower an ever-growing mobile and remote workforce with the same positive and simplified experience that they have grown accustomed to on their personal devices for legacy on-premises and modern cloud applications in a secure manner. Publicly available videoconferencing tools have allowed face to face meetings to take place from a distance—however, workers still require access to corporate controlled applications and resources to do their job effectively. Providing secure remote access has resulted in significant IT complexity around combining information from hardware, software, and cloud solutions for each supported application and generally requires hands-on configuration of the device by an IT professional.

ESG validated with real-world customers that Workspace ONE Access deployed in the cloud has significantly simplified the task of providing SSO and MFA for applications delivered by Workspace ONE. When used in conjunction with other Workspace ONE components such as UEM, Intelligent Hub, and Intelligence, organizations can greatly simplify their IT operations and enable a path to a zero trust model that provides simplified and secure access to end-users who can better focus on their jobs.

Enabling a remote workforce is no longer an option for IT organizations, but rather a requirement to allow organizations to succeed. Making sure that users have seamless access to applications and resources is a critical factor in keeping employees engaged and productive. But this mobile empowerment must not come at the expense of lowering security standards or slowing the speed of rolling out new applications and services. If your organization is looking to empower a remote and mobile workforce by delivering a consistent and simplified end-user experience from any device while

modernizing toward a zero trust model that reduces risk to the organization, then ESG suggests you consider deploying Workspace ONE Access in the cloud.

“We have a lot of different types of people with a wide range of technical ability. Workspace One Access helped us move access from being a roadblock to an enabler.”

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 from time to time. 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.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

