WHITE PAPER – **JANUARY 2017**

VMWARE'S MOVE TO A DIGITAL WORKSPACE

A business value analysis of deploying Workspace ONE

Table of Contents

Introduction

Workspace ONE is VMware's digital workspace solution, designed to give access to any application from any type of device under automated and granular policy control. VMware was one of the first adopters of Workspace ONE, deploying across its full user population in early-to mid 2016. This white paper describes the objectives that drove VMware's decisions of how and when to deploy, plus an overview of the business results we've achieved so far.

Background

VMware has grown rapidly over recent years and many of the end-user computing assets currently in use were deployed to meet urgent and specific business requirements. Corporate owned devices are less standardized than in many other organizations and the percentage of non-corporate owned devices in use (is high, particularly for smartphones and tablets.

As a relatively young company, VMware has few traditional desktop applications that require a local operating system (Microsoft Windows or Linux) and functional/data integration close to the user. Where such applications are used, they are often accessed in a device-independent manner from a virtual desktop running in one of our data centers. Some industry-standard client/server business applications are used to access key corporate systems, but the majority of the end-user application portfolio is Software-as-a-Service (SaaS) or web-based with a small, but growing number of mobile applications.

VMware's end-user workspace and application portfolio are thus more modern than those of many of our customers, with a lower dependence on local/native applications than the market average. This simplifies many of the practical aspects of making changes to the way our workers (both employees and non-employees) are equipped. However, this relative simplicity is offset by two considerations of growing importance:

- Many web-based and SaaS applications were deployed through local or departmental initiatives, with 'official' adoption by VMware IT happening afterwards. Some of these were developed internally and operate entirely behind the VMware firewall. The result is a lack of efficiency in some management and security processes. This scenario is common to any organization that responds rapidly to shifting market and user demands.
- Like most businesses, VMware's risk management strategies and processes evolve constantly in response to emerging and identified threats. Unless these processes are 'baked-in' to new application deployments, the cost and delay of responding to vulnerabilities and security incidents will continue to rise.

Risk management and overall security posture were core considerations in VMware's deployment of Workspace ONE. Although some aspects of risk management and security are referred to in this paper, the main focus is end-user service and infrastructure. A fuller description of Workspace ONE's role in VMware's risk management approach will follow.

Incremental Deployment

Although Workspace ONE was rolled-out in early-to-mid 2016, some preparatory steps had been made over the previous five years, beginning with the deployment of the (then) Horizon Application Manager in 2011. The VMware team were able to take advantage of these to accelerate their implementation. Access to SaaS and business applications had been gradually centralized to a single user interface on all desktop devices, as updates to VMware's emerging digital workspace solutions evolved. This common user interface (which some readers might consider a portal), was extended to mobile devices in 2015, following the integration of VMware's AirWatch EMM technologies into the solution.

However, the process of integration was not seamless. Business applications required a dedicated connector, each of which had to be developed in partnership with the application vendor. Some applications required VPN access, adding to the complexity of launch for the users. Some applications remained outside of the workspace completely. At the back-end, management of user credentials evolved piece-meal, with multiple repositories and methods in use.

Workspace ONE allowed all of the above to be brought together, providing seamless integration across all end-user applications and services. Identity management was centralized and simplified, using VMware Identity Manager™ (part of Workspace ONE) and this represented the main additional area of deployment. In parallel, VMware deployed Microsoft Office 365, which is also accessed and fully managed through Workspace ONE, so removing the last 'native application' requirement of most users. Any user who needs a native Windows or Linux application is equipped with a virtual desktop, which is accessed through Workspace ONE in the same way as other end-user services.

Two Sets of Objectives

From the outset, VMware's decision to deploy Workspace ONE was motivated as much by risk management and security goals as it was by the improvement of end user service delivery. VMware's Head of Infrastructure, Chief Information Security Officer (CISO), Head of End-User IT and Head of Applications were all co-sponsors and partners in leading the project.

End-User Service Objectives

Our end-user service objectives fell into two main categories:

- Respond faster
  The fast-moving and fragmented history of device and application deployment had led to a gradual erosion of adaptability in end-user service delivery. Keeping up with new business and technology developments was becoming more difficult as the heterogeneity of devices and applications grew. It was also ever more challenging to keep pace with ongoing demands for personnel adds, moves and changes (the need for which accelerated as our business expanded and grew).

  We needed our infrastructure capacity and capability to move with service requirements in a more fluid fashion – in a truly software-defined way. We also wanted to break down the internal silos of supplier-specific knowledge and skills.

- Improve end-user experience
  Almost every work task is technology-enabled, but the technology often gets in the way. Multi-step launch sequences for individual applications, lack of integration in collaboration tools and complex processes for switching between devices made many daily tasks harder and slower than users expected. The result was a reduction in user satisfaction and productivity.

  We needed a workspace that made work tasks quicker and easier, one that just functioned as required with minimal need for support or intervention. We wanted to encourage (rather than implicitly inhibit) collaboration and teamwork, while reducing the cost and overhead of communications. We also realized that we had barely even begun to see the true promise of business mobility and that we could do much more to support and embrace the 'mobile moments' of every employee.

To meet our end-user service objectives, IT would have to 'get out of the way'.

Security and Risk Management Objectives

Our security and risk management objectives fell into three main categories:

- Embrace IT reality
  Non-VMware-owned devices are broadly in use across all parts of VMware and around one worker in four is not an employee. 'Shadow IT' and use of unsanctioned applications (by which, we mean applications that had not been checked for compliance with our security protocols) were commonplace. The underlying assumptions on which our IT security posture was founded did not fully and explicitly reflect these realities.

  We had to shift overall stance, to make these facts non-issues. We also needed to create paths to deployment and tiers of functionality that would encourage both individual users and company buying centers to actively embrace higher levels of security. Security had to become more of a 'pull' function, instead of a 'push'.
- Pro-active risk management
  Like any organization, we are constantly under attack from multiple directions and the threats keep evolving. The time between an exploit taking place and its remediation is of growing importance (as the reputational damage done to some organizations subject to publicized attacks clearly shows).

  We needed to shift our overall stance and investment priorities from 'prevent' to 'detect and respond'. We also needed to reduce the 'dwell time' from exploit to remediation. To meet these two goals would require much more rapid audit trails for access to applications and data. This would also simplify general compliance.
- Improve resiliency
  As our provision of products and services becomes more dependent on partners and hybrid infrastructure, our portfolio of outbound applications and services is expanding. Any lack of availability in these applications and services, or in our own access to corporate data, impacts our ability to support ongoing business and, potentially, our reputation. We needed to do more to guarantee both.

VMware's Digital Workspace Approach

The architecture of Workspace ONE comprises the three main components required for any digital workspace solution:

- Identity management, which decouples users from their credentials for individual services and provides single sign-on (SSO) to all services from any device.
- A service catalog, which exposes available services to the user. The service catalog is shown as two tabs in a browser window; one for all applications available and the other for those activated for the user account.
- An extensible policy engine, controlling which services are made available to each user and applying rules of contextual access (for example, if access to some services is locked from specific locations or adapted for certain device categories)

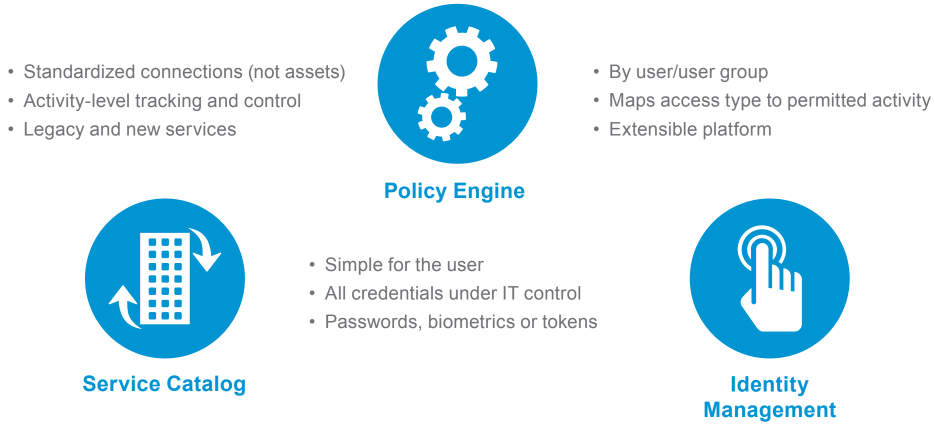

Figure 1: Workspace ONE Architecture

Workspace ONE can be deployed in three different ways (each of which corresponds to an 'edition'), depending on the breadth of device and application support needed. The three core digital workspace components are common to all modes of deployment, so the editions are easily mixed:

- Workspace ONE Standard comprises the three main components plus mobile (one-touch) single sign-on and the ability to enforce basic policy compliance on mobile devices.[1]
- Workspace ONE Advanced adds full life-cycle management capabilities for devices, enabled through an opt-in (device enrolment) capability. Enrolled devices are equipped with a container[2], enabling more local functionality.
- Workspace ONE Enterprise adds support for virtual desktop and application delivery into the service catalog.

---

[1] Workspace ONE Standard uses mobile application management (MAM) to provide data loss prevention (DLP) protection on smart phones and tablets.

[2] When a device is enrolled, a MAM profile is installed, enabling a full suite of AirWatch EMM (Enterprise Mobility Management) device lifecycle management tools to be used.

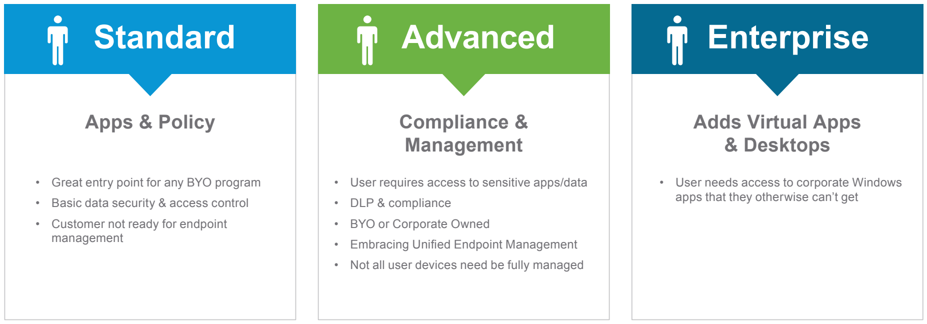

Figure 2 Workspace ONE Editions

In VMware's deployment, every user was equipped with Workspace ONE Standard and encouraged to enroll their devices[3]. Those who enrolled moved automatically to Workspace ONE Advanced, although this move was only visible to them through the extra functionality they received (the service catalog for enrolled devices is device dependent). Workers who require a virtual desktop environment were equipped with Workspace ONE Enterprise.

User Population and Assets

As of October 2016 (when research for this paper was completed), VMware had 30,318 users with access to corporate applications and systems, some of whom were inactive. Of these, 8,353 were contractors or temporary staff and 21,965 employees.

Approximately 51,000 devices were in use:

- 24,000 desktop and laptops, 22,000 VMware-owned and 2,000 owned by employees, contractors or partners.
- 27,000 smartphones and tablets, 14,000 VMware-owned and 13,000 owned by employees or contractors.

The non-owned smartphones and tablets were predominantly in North America, where VMware does not normally provide corporate-owned mobile devices to employees. Corporate-owned mobile devices were mostly in other geographies. For all categories of device, ownership had no bearing on how Workspace ONE was deployed.

Around 5,000 Horizon virtual desktops were in use on a permanent or semi-permanent basis (other Horizon desktops are spun up by our field teams as needed for customer trials and demonstrations, but these are not considered to be part of the end-user portfolio).

Around 400 applications were in use across the globe, of which 377 were SaaS or web-based, 10 mobile and the remainder client-server or native. Approximately 300 of these were unsanctioned (by our security teams), many of which had been deployed through local initiatives.

[3] DLP is required for access to many of VMware's HR and business system of record applications. Any employee who also carries a laptop was encouraged to enroll.

What We Deployed

As of October 2016, Workspace ONE was deployed to approximately 22,000 VMware users, representing 73% of the total user population. Roll-out to the remaining active users was scheduled to be completed by the end of 2016. 13,200 of these Workspace ONE users had chosen to enroll one or more of their devices, including all of the 5,000 virtual desktop users.

What We Measured in Our Business Analysis

From the outset it was clear that any business analysis of deploying Workspace ONE would need to consider a broader range of parameters to those used in traditional total cost of ownership (TCO) and return on investment (ROI) calculations. First, because the incremental nature of the deployment meant that the capital bill of materials (BOM) was very small. Second, because the goals of deployment were motivated more by benefits (user satisfaction, productivity, better risk management) than by costs.

These are the parameters we evaluated:

• Deployment costs, both BOM and the labor to plan and deploy
• Cost savings in IT operations and helpdesk/support
• Increases in user productivity through time savings

VMware's Workspace ONE deployment is cloud-based, so some costs were absorbed by our cloud service provider and Workspace ONE is 'consumed' as a (subscription-based) service. However, for simplicity and transparency in our analysis we evaluated all parameters and costs as though the deployment was fully on-premises.

Deployment Costs

The incremental BOM for deployment comprised some additional infrastructure for identity management functions, new infrastructure for all the Horizon virtual desktop users and Workspace ONE licenses for all users. For the purpose of our analysis, we assigned an internal transfer cost to each of these licenses at a market standard discount against list prices.

The additional infrastructure deployed included 13 hyper-converged appliances, 11 management servers and two racks, each with a 48-port network switch. Although some of these components were redeployed from elsewhere, our cost estimates assume they were purchased as new. In total, we estimate the cost of additional infrastructure to be $1.15M.

Most of this cost comes from the deployment of new, hyper-converged infrastructure for the 5,000 Horizon virtual desktop users. Had the existing virtual desktop infrastructure been fully re-used (an option for any organization with existing Horizon users), the cost of new infrastructure would have been less than £75,000.

For software costs, we consider the current deployment to comprise: 8,800 Workspace One Standard licenses, 8,200 Workspace ONE Advanced licenses and 5,000 Workspace ONE Enterprise Licenses. In total, we estimate the cost of these licenses to be $2.6M.

All the BOM costs above are one-off, capital costs. We did not consider the impact of amortizing our capital investment over multiple years, or annual maintenance fees.

The effort to plan deployment and roll out to the first 22,000 users was spread across many parts of VMware’s IT organization. We estimated the cost of this effort in two ways:

- On a task-by-task basis, using project cost calculation models deployed in our customer facing ROI models
- Through discussion with the project team leaders

In total, we estimate that around 9-person months of effort was involved, spread across the various team members. In dollar terms we estimate the total project costs of deployment borne by IT to be approximately $76,000.

Cost Savings in IT Operations and Support

Labor cost savings in IT operations and support come from two main sources:

- Elimination of password support issues
  VMware was handling a relatively high number of password support requests, many to reset user credentials. VMware uses an automated password reset function, but this only works for ‘system’ credentials (those issued/managed by VMware IT) – passwords for unsanctioned applications were not covered and generated most of the overhead.
- Reductions in the time taken to identify and contain incidents
  Industry analysts estimate the average time to identify incidents and vulnerabilities to be over 200 days and the average time to contain/remediate incidents to be over 60 days. VMware was significantly better than both average figures, but there was still much scope for improvement. The centralization of access to end-user services that Workspace ONE delivered drove a significant reduction in both times (and hence helped us meet our ‘reduced dwell time’ objective).

According to industry analysts and market research, the average support ticket costs $15. VMware had been handling an average of 4 password reset support tickets per user per year. For the 22,000 users now running Workspace one, these have been eliminated, so we estimate the total annual saving to be $1.32M. These annual savings will increase as the rollout of Workspace ONE is extended.

Working with VMware’s security and risk analysts, we estimate the reduction in time to identify and remediate vulnerabilities to be at least 25%. Using internal estimates of the percentage of end-user devices compromised each year, our mean time to identify incidents (MTTI) and mean time to contain incidents (MTTC) data (all confidential data), we estimate an annual saving of approximately $4.46M. Again, this figure will rise as the rollout of Workspace ONE is extended.

Productivity Gains

We evaluated productivity gains from two sources:

- Faster access to end user services
  Prior to deployment of Workspace ONE, users logged into many applications individually. With Workspace ONE, they only login once per day – each application launched afterwards (on the same day) comes 'free', saving time for the user.
- Less time spent getting support for password resets
  Each help desk ticket avoided saves time for the user as well as a cost for IT. The reduction in support overhead for password resets thus drives a proportionate time saving for users.

To estimate the time savings from faster logins, we examined access data for a broad range of our applications: the top 10 are launched approximately 1,000,000 times per month. We determined that each user completes around 13 application launches per day (often launching the same application more than once). The average time to authenticate is around 15 seconds with passwords and 10 seconds with tokens or biometrics (fingerprints). Bringing all this data together, we believe each Workspace ONE user gains about 64 minutes of working time per month through reduced login times.

For the time saved by logging fewer support tickets, we estimated that each ticket cost the user 15 minutes of working time (to discover the problem, log the ticket and then receive help). Given this, we estimate that each Workspace ONE user gains and extra 5 minutes of working time per month.

Business Value Calculations

Using the analysis described in the previous section, we estimated the following totals for our Workspace ONE deployment:

- Costs to deploy (labor, infrastructure and software): $3.83M
- Annual cost savings (operations and helpdesk): $5.78M
- Productivity gains: 3,140 work days per year

From the first two data points, we estimate the year one ROI to be 150% gross (50% net of investment costs)[4].

The savings are annual and future year costs will be significantly lower (maintenance only). Therefore, the ROI of VMware's deployment will increase over time.

[4] If we had elected to re-use the existing infrastructure for our 5,000 Horizon virtual desktop users, the deployment costs would have been $2.75M and the year one ROI would have been 228% gross (128% net).

Benefits Beyond ROI

In addition to a positive financial ROI, we saw two additional areas of significant business benefit through our analysis:

- Improvements in risk management and risk mitigation. Our estimates here are still in review, but it is clear that Workspace ONE has accelerated VMware's progress towards our CISO's goals.
- Low cost development and deployment of new mobile applications. The Workspace ONE architecture decouples back-end business processes from their presentation to users at the point where they are displayed in the catalog. This enables a single process to be delivered as multiple, parallel user experiences, depending on the context of access and use. A first example of this is an application we rolled out to all VMware managers, called vApprove.

About vApprove

A number of VMware's internal applications generate approval requests for managers: expense management, procurement etc. Each approval request is sent to the manager in email and they can either respond to the email, or open the application and approve the report/transaction directly.

vApprove provides a third way of doing this, by bringing together all approval requests into a single, mobile application. This gives the approving manager a third way to approve and is particularly useful when travelling or in constrained locations (for example a plane seat, where privacy is a concern). vApprove provides the same audit capabilities as the full applications, but in a reduced format.

vApprove is only available on enrolled devices and appears as a stand-alone application on the mobile device, although it is (technically) deployed within Workspace ONE. There is no configuration required: once Workspace ONE has been launched (and is running in the background), vApprove is accessed through a single click.

Deployment of vApprove has delivered one of the 'mobile moments' we targeted before our Workspace ONE roll-out began. It also created a strong motivation for many users to enroll their devices and demonstrates part of the new 'pull' model for end-user services. VMware has shown that when managed IT offers greater utility than unmanaged, users will enthusiastically embrace it.

Although vApprove is a single application today, we regard the architectural model and the promise it offers to be a much broader value proposition. We expect more such applications to follow.

Conclusion

Focusing only on the areas that are demonstrably measurable, VMware's internal deployment of Workspace ONE has already delivered a significant financial return on investment – from our previous experience in building end-user computing business cases, a year one ROI in excess of 100% gross is unknown. In reality, we know that even this estimate is low as our cost estimates are cautiously high and there are other cost savings that we did not measure or quantify. Without doubt, VMware's investment in Workspace ONE is highly successful in business terms.

Beyond financial analysis, VMware has already observed many additional benefits from deploying Workspace ONE: a better platform for proactive risk management, improved employee engagement and an architecture that encourages development of innovative mobile applications to highlight just three. Even had the financial ROI been negative, these benefits would have created a strong business case for our investment.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com