WHITE PAPER – **JUNE 2018**

EUC TRANSFORMATION BEST PRACTICE GUIDE: TRANSFORMING WINDOWS APPLICATION DELIVERY

vmware®

Table of Contents

Executive Summary

The need to work with diverse and untrusted devices, multiple operating systems (OSs), and consumer-oriented applications in what has historically been a highly standardized and controlled IT environment is creating chaotic end-user computing (EUC) estates for many organizations. At the same time, more demanding business users, increasing focus on security issues, and the pace of change in EUC are reducing the ability of IT to ensure and demonstrate compliance with corporate policy. The pressure on IT organizations to change the way they approach and manage the delivery of EUC applications is significant.

Despite this growing diversity of device and application type, most organizations also need to continue making Windows applications available to their workforce. In many cases, these applications are business critical and offer no easy route to replacement with a more device-independent application type (web-based, SaaS, or mobile). Making these applications available from unknown or untrusted devices and from a range of OSs is a functional necessity. As the lines continue to blur between corporate-owned and personally owned devices and between work offices and home offices, today's mobile and global workforce requires and expects access to Windows applications anywhere, at any time, and through any device.

Even when IT organizations had relatively homogeneous Windows environments, managing their corporate-owned desktop PCs and laptops was a challenge that obliged many IT administrators to rely on manual processes and disparate endpoint management tools for provisioning, configuring, securing, and maintaining PCs. Now this challenge has become significantly more complex.

The highest priority for many organizations looking to meet the current and future EUC needs of both users and the business is to change how they deliver Windows applications. This means rethinking Windows application delivery, management, provisioning, and enablement.

In this paper we offer an overview of different delivery methods for Windows applications, discuss the pros and cons of each, and examine common scenarios for their use. We also look at how organizations should evaluate their own environments, so they can build a strategy for giving users access to the Windows applications they need.

What's Different?

Running applications natively on Windows on PCs is now a limiting factor for many organizations. Tying applications to the OS on a physical device can ensure the best performance and allows the tightest control of integration with other local functions, but these are diminishing requirements: Few EUC applications are now performance-constrained by hardware and the "plane of integration" with other functions has shifted from devices to the cloud. With these requirements receding, other aspects of distributed computing have become more visible: inherent complexity in security, multiple points of failure, and reactive management.

Modern web and cloud delivery models avoid these distributed issues by pushing application execution and integration back to the data center (cloud), where applications and data are centrally managed and maintained. Dependencies on device and OS type are removed from the management equation.

This centralized approach is now the preferred app/dev architecture for almost every organization. The move to the cloud and data center has happened for very good reasons:

- Improved security and risk management
- Easier administration
- Faster delivery times
- Easier deployments
- Scale
- Lower operational costs

These valuable attributes (and others not listed) are why a centralized architecture is a preferred method for most organizations and can also be used to deliver Windows applications that normally execute on PCs. By removing the desktop operating system and applications from the endpoint, disaggregating them, and delivering them to the end-user device from the data center, application and desktop virtualization offer the promise of improved security, management, operations, and cost.

Early adopters found that virtualizing applications and desktops could be costly, due to the need for complex and high-performance infrastructure. Operational savings from centralization and standardization were offset by the higher cost of data center infrastructure, and often it was only organizations that prioritized mobility or security over short-term costs who could justify the change. Many of those that did embrace application or desktop virtualization found it necessary to produce sophisticated financial models to demonstrate how operational savings over a multi-year period would deliver a return on the investment. For those that were able to build such business cases, the user experience delivered limited adoption.

Rapid and recent innovations in technology, process, and licensing changed all of that. The capital acquisition cost of desktop and application virtualization is now often lower than that for equivalent physical PCs. What was previously a 'spend more to save later' value proposition for mainstream users is now "save now and save later." User experience has also improved significantly, so that even organizations with more challenging technical or functional requirements can easily deliver adequate performance to their workforce. The remote delivery of Windows desktops and Windows desktop applications has moved into the mainstream.

Virtualization of Desktops and Applications

Two forms of desktop centralization are used: virtual desktop infrastructure (VDI) and Remote Desktop Services application publishing (RDS). The most common approach to centralizing a full desktop environment is VDI. VDI leverages server virtualization so that instances of Windows can be launched and run in their own virtual machines and then remotely delivered to users.

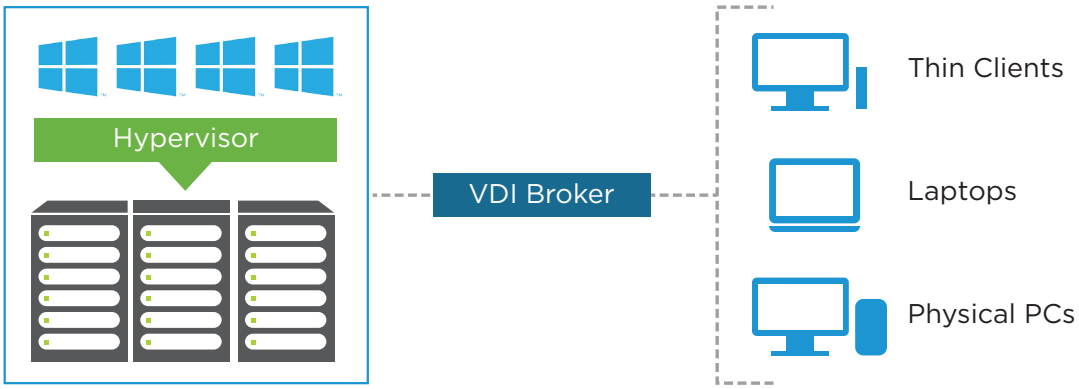

Figure 1: VDI Architecture

With RDS, applications are installed and configured on Windows Server OS (instead of the client OS) in a multiuser environment, so that many users can simultaneously access the application remotely. Like VDI, RDS is a remote solution that alleviates the need for local execution of applications on a PC. RDS is a shared environment, meaning that the delivery, access, and management of applications is simpler and easier as compared to distributed PCs.

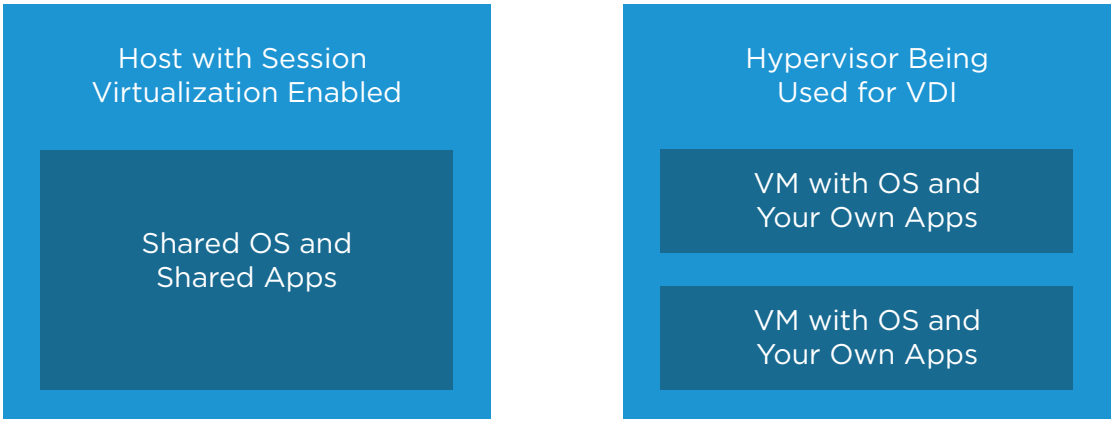

Figure 2: VDI and RDS Comparison

Both VDI and RDS are used by organizations for application delivery. VDI is most commonly used for those users that require the full fidelity of Windows, so that users can install, configure, and use their desktop just as they would a normal PC. RDS is common for applications that are targeted to many simultaneous users (for example, those working in a call center). It is not uncommon for organizations to use both VDI and RDS, depending on user need and application requirements.

A clear advantage of remote delivery is that it enables IT organizations to centralize their applications in a corporate data center or on cloud-based services. As a result, IT staff can more efficiently provision new applications or environments, simplify and standardize a broad range of desktop management tasks, and provide more robust endpoint security. Virtual desktops and applications also provide IT organizations with greater consistency across system settings and policies, meaning they can rationalize and streamline the targets of their management processes.

Virtualization has enabled IT administrators to deliver a more consistent and seamless desktop application experience to the rapidly expanding population of employees who use multiple devices for their work. Users can access the same desktop instance or application from each new session, as well as securely access corporate data and applications anytime and anywhere, through a single set of policies and log-in credentials. All of this takes place regardless of the device type, operating system, or location of the user.

What Changes?

As PC management has evolved, next-generation OSs have created a shift in focus.

The Past: Focus on Native Applications and PCLM

PC and Windows management was born out of necessity, not desire or intent. The earliest Windows versions (3, 3.1, 95, and so on) were designed for standalone PCs with little-to-no management needed. Not until the introduction of native networking did management tools appear. The concept of PC Lifecycle Management (PCLM) was created by organizations that needed to keep better track of PC assets, mitigate PC security risks, and deploy software updates, as well as find a better way to deliver operational and administrative support.

PCLM software began to appear in the late 1990s, primarily targeted at desktop PCs that were network attached. Where a PC was not attached to the network or was a remote laptop, effective management was more challenging and unlikely. Organizations began software imaging, predefining the configuration of Windows, hardware, and settings on their PCs. These predefined images were applied by IT or OEM partners, and often locked to prevent users making changes. Working with standardized images helped IT to provide better support, and reduced the operational costs associated with PC management while also increasing user uptime.

The principle of IT controlling the targets of their management processes to make those processes more efficient was established and is still a best practice for many organizations today. Gradually, many of the limitations of the approach were addressed, but the underlying architecture of PCLM tools was not designed to handle diversity of user requirements. PCLM works best when devices have known configurations and application delivery is tightly controlled, so these tools have struggled to keep pace with mobility and the increasing use of cloud-based delivery models. Most organizations now face a dilemma with their continued use: to loosen control or to scale costs and complexity, which means becoming much less responsive to shifting demands.

The Future: Focus on Dynamic Delivery, Cloud, Application Publishing, and VDI

The way organizations provision, manage, and secure end-user computing devices is changing as the next generation of OSs are deployed on new PCs, Macs, and mobile devices. These next-generation OSs are designed to be managed as mobile devices, through simpler and more frequent updates. The impact promises to be transformational in terms of both ongoing management costs and the speed of dealing with adds, moves, and changes in the enterprise. However, to achieve this transformation, organizations will need to do more than just deploy the next generation of technology: They will also need to adapt current management and security processes, requiring changes in working practices.

Despite rapid adoption of mobile applications, smartphones, and other "as-a-service" offerings by users, native Windows applications are not going away any time soon. In many cases these applications were developed or modified in house for specific requirements and perform business-critical functions: Had it been easy to swap them for a web-based or SaaS alternative, IT would have done so during a previous Windows migration. As organizations embark on their journeys towards a digital workspace, they will need to take these applications with them, which means they still need to provision and manage Windows-based applications as part of their overall EUC strategy. However, that does not mean no change: As organizations adopt and deploy Windows 10, they have opportunities to simplify and improve how they manage and deploy their Windows applications.

Windows-based applications can now be made available and delivered to users in a number of ways:

- Deploying virtual desktop infrastructure (VDI)
- Publishing Windows applications via Remote Desktop Services
- Applying modern management techniques using Enterprise Mobility Management (EMM)
- Subscribing to any of the above via a cloud-based service

Virtual desktop infrastructure (VDI) offers users the full fidelity of traditional Windows PCs, with the same look, feel, execution, and customization as running applications natively on a PC. VDI runs on servers (and not PCs), so the operation and administration are centralized and standardized, meaning they can be simplified and optimized. IT administrators can quickly and easily refresh, update, reboot, secure, and manage Windows and Windows applications. VDI is popular with organizations that have high degrees of similar users but can be used just as effectively for users who are unique. VDI is also the preferred choice when applications require direct access to Windows OS capabilities and resources.

Remote Desktop Services (RDS) is used for customers wanting to make just applications (and not the underlying OS) available to users. RDS is also multiuser, which means that many individuals can access the same instance of an application simultaneously. (It is not uncommon to have single application instances available to several hundred concurrent users.) Like VDI, the benefits of RDS include faster rollouts for updates and the ability to access corporate apps and desktops remotely from any device.

Enterprise Mobility Management (EMM) offers customers deploying Windows 10 a more effective way to manage applications and Windows as compared to PCLM. As a result, the nature of how employees approach and view using their Windows 10 PCs will change. Instead of the "take-it-or-leave-it" approach that is common in many organizations today for imaged PCs, organizations can provision based on the users' specific needs and requirements. EMM offers organizations a way to provision, manage, and secure end-user-computing (EUC) devices. EMM is expected to be transformational in terms of ongoing management costs and the speed of addressing changes in the workforce. Achieving these gains requires more than just deploying the next generation of technology. Organizations must also adopt management and security processes that extend beyond technical skills, because the "what" and "how" of IT responsibilities will change. For more information on EMM, please consult the *EUC Transformation Best Practice Guide: Moving to Modern Management with Windows 10*.

Cloud-based services for desktops and published applications also offer high degrees of flexibility with the delivery and management of Windows applications. For a fixed per-user fee, organizations can subscribe to desktop services from cloud providers as a monthly or annual service. This approach frees the customer from the time, expense, and infrastructure necessary for deploying Windows (via VDI or RDS) internally. Cloud providers typically have significant economies of scale, so the costs can often be at or below what customers could achieve for themselves.

Underlying the approaches described previously is the ability to create layers of abstraction between the normal interdependencies that exist between PCs and Windows. Specifically:

- With VDI, Windows is no longer dependent upon underlying hardware. This independence is achieved through virtualization on servers, which provide Windows the appearance of hardware when in fact it is running in a virtual machine. Removing the dependency on hardware means that customers can present VDI sessions to users in a highly standardized and efficient manner, without regard to the type of device in the hands of the user.
- RDS creates separation between the user's configuration and the application. This means that organizations can deploy highly standardized applications rapidly to hundreds or thousands of users concurrently. RDS is attractive because of its relatively low operational cost, quick time to deploy, and ease of management.

VDI and RDS both deliver reductions in operational costs (through centralization and standardization), improvements in the time to deploy new applications, and simplification of management. Both are well established approaches that provide a straightforward mechanism for delivering previous-generation Windows applications to any device and any location. Organizations typically prefer VDI for more complex environments, where applications require access to capabilities only offered by a desktop Windows OS, and for the closest fidelity with a desktop OS experience. RDS is the first choice for delivering just Windows applications and is more popular when the application count is low.

Delivering Windows applications differently not only addresses the disadvantages of legacy PC deployment but also injects a layer of abstraction from PC hardware that transforms systems management. This approach provides customers with a single platform to extend the power of virtualization from the data center to devices. This approach also helps customers deliver virtual desktops and hosted apps so that costs are driven down, management and operations are streamlined, and users receive better experiences.

Implications of Transforming Windows Application Delivery

By taking advantage of application abstraction and virtualization, organizations can deliver applications independent of Windows, allowing IT administrators to manage application changes as needed. For example, if a business unit requires monthly or quarterly updates to an application, they can do so via VDI or RDS without having to worry about the impact on Windows or the device in the hands of the user. Updates are easier, quicker, and can happen at the cadence determined by business requirements.

However, organizations must also be mindful of the impact that adopting these approaches may have on existing processes. How IT operational teams do their work will change. The impact may also cascade into IT architectures, application development, help and service desks, security, and other areas.

Impact of Transforming Application Delivery on IT Operations

Application delivery changes require careful planning. Preparation is key and must begin with a solid understanding of the applications in question, the users and their support needs, existing infrastructure, and business requirements. Some Windows applications cannot be appropriately reconfigured for a remoted session, while others may have dependencies that require them to run locally (such as interaction with a peripheral device).

The following are examples of questions to ask before undertaking changes in application delivery architecture. It is important to have a solid understanding of the business objectives and other non-technical project requirements and to identify the business factors that could influence project requirements or system design.

- Who are the end users and which business units do the applications serve? Segmenting by use case, need, and by business requirement will help guide any deployment plans.
- How many users will need to access hosted applications or desktop sessions? Servicing a few users vs. thousands has a significant impact on infrastructure planning, support, licensing, and other costs.
- Which locations require access to hosted applications or desktop sessions? Not all locations can guarantee the bandwidth and latency required to deliver a satisfactory user experience for some applications.
- Will the implementation coincide with other major changes to the business, such as acquisition of another company or the launch of a major new product? Implementing a new application delivery architecture is a challenge unto itself. Doing so while the business is undergoing radical changes elsewhere could add unwanted exposure and risk.
- What kind of infrastructure already exists for RDS or VDI? Some organizations can absorb a new delivery architecture with little impact, while others will have to make sizeable investments in additional infrastructure (compute, storage, network).
- Are there existing VDI or RDS solutions already in place? Understanding what already works well or needs improvement is a great way to avoid future pitfalls. Assessing existing strengths and weaknesses correctly will also help gain support from elsewhere in the organization for future adoption and use.
- How many and how critical are the Windows applications for the user and organization? Performing an inventory and knowing the install base of applications and their relative importance helps manage the effort required, associated risks, and other project activities.
- What are the run-time requirements of the applications and their performance characteristics? Legacy screen-scraping applications behave very differently than multimedia, databases, or collaboration tools. Understanding application behavior is critical for design.
- Are there any existing applications ripe for retirement? A goal for any organization should be to reduce and simplify the application portfolio where possible. The needs of the users and business change over time, and being able to remove unneeded applications reduces cost and complexity.

- Do existing applications require significant changes, such as upgrades? Are you planning to replace an existing application with another? Moving from a decentralized to centralized architecture often means changes in the application itself.
- Which devices and peripherals do end users need? Some applications may rely on specific capabilities to deliver the correct function and user experience (for example, large screens, full keyboards). Some users may also require specialized devices (for example, scanners, printers, cash register) to be locally attached to their device.
- What is the best way to educate and train users about how applications need to be accessed? Do not assume that success is determined exclusively by implementation; rather, success happens when the user understands and is comfortable with the new environment.

Impact of Transforming Application Delivery on End-User Support

One distinct advantage of moving to a centralized application delivery strategy is that business users' desktops then reside in a corporate data center, where the IT organization is usually located. As a result, IT staff can more efficiently provision new client instances, perform desktop management, and provide endpoint security.

Virtual desktops and applications also provide IT administrators increased consistency across system settings and policies through the elimination of dependencies on the underlying hardware. This means that streamlining and reducing their image inventory to a few gold images or perhaps even a single image becomes viable without any compromise in the ability to apply adds, moves, and changes.

These changes also mean that the skills normally associated with Windows and desktop application delivery will need to be bolstered with information and further training on virtual desktops, published applications, and cloud provisioning of desktop services. Proficiency in managing PC configurations and application packaging will no longer be sufficient. Critical infrastructure skills in the areas of virtual machine configurations, load balancing, new management tools, and network analysis will also be necessary. Many organizations employ "centers of excellence" that encompass all these skills to ensure their team members can design, deploy, and manage application delivery across a variety of scenarios.

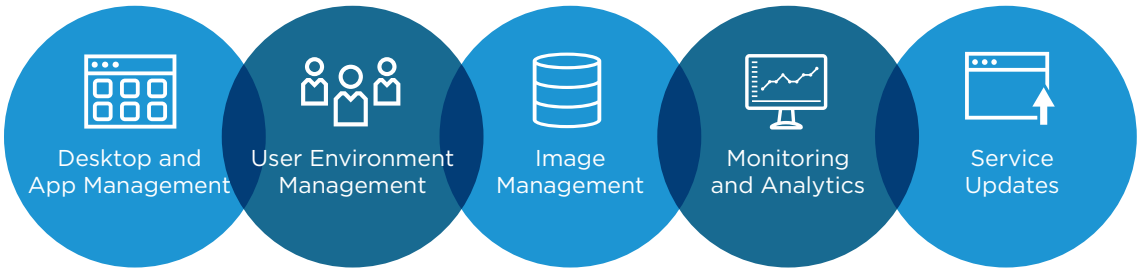

Figure 3: Comprehensive Application and User Management

Cost Changes for PC Acquisition and Management

Market data shows that, on average, organizations spend around $700 per year on the ongoing management of PCs through traditional PCLM tools. This cost is typically regarded as delivering no marginal benefit and so can be subject to high levels of scrutiny. The same market data shows that through centralized and simplified management, the annual savings achieved by moving to VDI, RDS, or cloud-based services can be as high as 60 percent.

Financially speaking VDI, RDS, and cloud-based services offer organizations the opportunity to reduce both direct and indirect costs normally associated with PC management. Direct costs affected include:

- Staff – Help desk, IT admin, and security teams now perform more work in less time, which likely reduces support staff needed for the same number of employees.
- Hardware budgets – Thin clients cost less, are easier to maintain, and last longer.
- Cloud-delivered desktops shift CapEx to OpEx.
- Asset procurement – Used thin clients can have significantly longer (some customers claim 10+ years) lifecycles as compared to 3–5 years for PCs.

Indirect costs affected include:

- More user uptime and productivity, through more consistent delivery of Windows applications.
- Users generally have fewer operational issues because of the static nature of the desktop experience.
- With far less happening on the device in the hand of the user, the time spent to provision and support users is dramatically reduced.
- Flexible application deployment improves quality with fewer incidents and outages.
- Rapid deployment and configuration of user environment improves availability and allows users to commence or resume job functions following workforce adds, moves, and changes.

Preparing for Transforming Windows Application Delivery

IT organizations cannot afford to continue managing application delivery to their end-user environment with a previous-generation and out-of-date PC-centric approach to systems management. The cloud, mobility, and multiplatform environments have rendered that approach ineffective and highlighted its inability to scale. VDI, RDS, and cloud-based services offer organizations better and more modern ways to continue delivering, managing, and protecting Windows desktops, applications, and services. Organizations should:

- *Understand* that VDI, RDS, and cloud-based services offer unique and differentiated capabilities for Windows applications unavailable with PCLM.
- *Recognize* that separating Windows applications from the OS and hardware is necessary to embrace device heterogeneity while delivering on the security, operational, and financial expectations of the organization.
- *Establish* a holistic deployment strategy that allows for the delivery of applications through VDI, RDS, and/or cloud-based services.
- *Leverage* new application delivery methods to establish better SLAs for users with more flexibility and freedom of choice of device, application, and quality of service.
- *Consider* the organizational and operational challenges and changes implied for the security, support, and administrative teams.
- *Build* consensus with key stakeholders so that a unified application delivery strategy can be created and embraced across the organization.
- *Learn* about the new, unique, and strategic features of VDI, RDS, and cloud-based services.

- *Test* a variety of Windows 10 scenarios, use cases, and user types (for example, knowledge worker, kiosk, road warrior).
- *Create* a detailed analysis of existing applications, their users, and requirements.
- *Eliminate* applications that are no longer needed or relevant to the user or organization.
- *Review* all assumptions, configurations, processes, and other aspects of alternative application deployment methods.
- *Justify* further expansion of your application delivery strategy by measuring SLAs, costs (direct and indirect), and value (with ROI, if possible).
- *Understand* that different operational processes will likely coexist for some time.
- *Communicate, communicate, communicate!*

Conclusions

VDI, RDS, and cloud-based services all provide flexible application delivery methods for delivering Windows applications across diverse devices and into a modern, digital workspace environment. Organizations need to devise a strategy for deployment that is achievable, measurable, and is demonstrably better than what is currently being done. The imperative is to transform while also continuing to use the Windows applications that you cannot or will not replace. Organizations should begin this transformation process now, learn, and make all their people (IT, finance, line of business, and end users) much happier.

About the Author

Mark Margevicius, Director of EUC Strategy and Chief Customer Advocate, VMware, wrote this paper. Mark's primary function is to assist customers in understanding the trends and directions of the End-User-Computing landscape. In this advisory role, he provides tactical guidance on EUC initiatives and assists in EUC strategy development in the areas of desktop transformation, mobile computing, DaaS, VDI, and desktop virtualization.

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

6/18