WHITE PAPER

VDI: A New Desktop Strategy

A Guide to Managing User Desktop Environments with Virtual Desktop Infrastructure

vmware®

foedus

Contents

Introduction 1
A Brief History of Desktop Management 1
Execution Models 1
Early Centralized Computing 1
Distributed Computing 1
Windows Server Based Computing 2
Problems with Terminal Server Designs 2
What is VDI? 3
VDI's Contributions to Desktop Management 3
VDI offers the Benefits of Server Based Computing 3
VDI offers the Benefits of Distributed Computing 4
New Benefits for Desktop Management 4
VDI and Desktop Stability 5
VDI Cost Savings 6
Business Drivers and Common Use Cases 6
VDI Architecture 7
Design Components for a complete VDI Solution 7
Client Access Device 8
Secure Access 8
Client Integrity Checking and Connection Termination 9
Connection Brokering 9
Boot Image Management 10
Application Virtualization and Streaming 11
Turbocharged Performance with Data Caching 11
Deployment Scenarios 13
Scenario 1: Outsourced Development 13
Scenario 2: Support Solution Managing Hybrid Resources 14
Scenario 3: Local and VDI Apps with Application Virtualization 15
Customer Testimonials 16
Conclusions 16
About the Author 18

Introduction

Virtual Desktop Infrastructure (VDI) introduces a new way of managing user environments. VDI allows IT administrators to host and administer user desktops on Virtual Infrastructure in the datacenter. Users access their desktop using a remote desktop protocol. While sharing similarities with other computing models, VDI offers many new and compelling benefits for increasing manageability, performance, and security of user desktops/PCs. VDI is a solution rather than a product and this paper compares VDI to other user management strategies and highlights VDI's benefits for particular use cases. The paper covers VDI architecture, complimentary third party products and specific design scenarios in order to give the reader a deeper understanding of VDI. Combining the benefits of both distributed and server based computing, VDI provides improved stability, superior performance, and simplified manageability for user desktops in a variety of situations.

A Brief History of Desktop Management

Management of user desktops has always presented challenges. Several execution models and a variety of management paradigms have attempted to tackle these challenges, each with varying degrees of success.

Execution Models

Within computing, the relationship between the user interface device and the location of application execution sets the parameters for both performance and manageability of the user environment. Program execution, can be centralized, distributed, or clustered. Each approach brings unique benefits and challenges described below.

Early Centralized Computing

The expense and complexity of early mainframe based centralized computing excluded consumers and small companies from the benefits of computing technology. As a group, consumers must be able to operate in a stand-alone mode yet seek support for a wide range of software. The confluence of consumer demand for computing, affordable microcomputers and standardized operating systems such as DOS and Windows led to an explosion of software development. Suddenly, application software was a commodity rather than build to order creations of highly skilled programmers. Small to medium sized businesses quickly adopted PC technology as much for access to the diversity of software as for the affordable hardware.

Distributed Computing

Distributed computing spreads application execution across a number of stand-alone or networked computers to meet the needs of an organization. Until the mid-nineties, the growth in distributed computing seemed unstoppable. Users needed their own PC and there seemed little reason to question this approach while companies enjoyed the new efficiencies brought about by the PC. In the early days of distributed computing, networks were primitive and many companies either lacked appropriate bandwidth and infrastructure or deployed them selectively. PC designers focused their efforts around stand-alone functionality. Networking was more of an add-on than the focus of computing efforts. Slow or unreliable networking made basic design features like the local hard drive a universal and critical feature to maintain any personalization of the PC across reboots.

Distributed computing continues to be the dominant computing model and for this reason, software designers continue to make design and performance assumptions around the PC. Developers often assume that users will have full and exclusive use of their CPUs, memory and hard drives. While desktop based software generally functions on server platforms, examples of PC centric designs pervade the world of business software. Examples include a CPU pegging at one-hundred percent while programs poll for receipt of data from a remote server. The writing of temporary working files into program directories, or failure to release unused memory also show the bias towards a PC centric design. Key advantages of distributed computing include offline operation and the highest video bandwidth facilitated by the display's close proximity to CPU, memory, and video rendering resources.

Windows Server Based Computing

Deployed in scale, PCs created an ever-increasing management burden on IT staff. Hardware and software upgrades are frequent, tedious, and error prone. Geographical dispersion amplifies these problems. In the mid-nineties, Citrix pioneered a new approach to managing user environments. Citrix introduced a server based computing model that retained the flexibility of x86 Windows based software while creating opportunities for geographic consolidation and centralized management. Citrix and later Microsoft Terminal Server are similar in their multi-user session aggregation within a single operating system.

The management and cost benefits of server based computing have been documented from reputable sources such as the Gartner Group[1] and touted by thin client vendors like Wyse[2] for many years. The inherent portability, ease of software upgrades and powerful user management tools have continued to make server based computing a popular choice in the enterprise. Until recently, Citrix and Terminal Server based approaches were the only way to access the benefits of centralized computing while using x86 based software.

Problems with Terminal Server Designs

Windows kernel development has focused on the ability to handle a large variety of applications, facilitate tremendous end-user functionality and accommodate a wide variety of device drivers. The focus on broad functionality has taken the Windows kernel in directions that overlooked the kinds of advanced resource allocation and end-user isolation features necessary to manage demanding multi-user workloads. Adding the multi-user functionality of Terminal Server extensions to the Windows operating system has also magnified issues derived from the single-user general-purpose design of Windows including:

- **Device Driver Incompatibilities**: Drivers and devices from different vendors are not regression tested for multi-user shared functionality and unpredicted problems can occur under heavy workloads.
- **Performance Volatility:** The longstanding bias in application design towards dedicated PCs leads to assumptions about resource availability that often degrade performance. As the OS supports higher user session densities, unpredictable loads create erratic user experience. CPU intensive applications used simultaneously by a few users can degrade performance for all the other users on a server.
- **Scheduling Limitations:** While the Microsoft NT kernel includes many innovations, its focus has not been on sophisticated resource allocation. The NT kernel's thread management limits its ability to balance physical CPU loads. A thread executing in kernel space can tie up processor resources until it exits the kernel and returns to user space. One program or driver can deprive another of CPU time, degrading the user experience under heavy multi-user workloads.

[1] Mark A. Margevicius, Michael A. Silver, "TCO Comparison of PCs With Server-Based Computing", 15 June 2006 published by The Gartner Group.
[2] See Wyse article "Thin-Client ROI: The Untold Story", Nov 2005 at http://www.wyse.com/resources/whitepapers/IDC_ROI.asp

Terminal Server based computing continues to grow in popularity as companies recognize the value of server based computing. The performance and compatibility issues of Terminal Server have also limited its.

What is VDI?

Building on VMware Virtual Infrastructure 3 (VI3), Virtual Desktop Infrastructure (VDI) effectively addresses and resolves key problems in Terminal Server based approaches to server based computing. VMware ESX Server allows multiple user desktops to run as separate virtual machines while sharing underlying physical hardware resources such as CPU, memory, networking and storage. This isolates users from each other, giving each user their own operating system, allowing granular resource allocation and protecting users from application crashes and operation system faults caused by the activities of other users.

Taking advantage of ESX Server features and VirtualCenter Server management features, VDI reduces device driver incompatibilities with standardized virtual hardware and a tightly screened Hardware Compatibility List (HCL) for physical ESX Server host hardware. Performance volatility is reduced with ESX Server scalable CPU scheduling and the multi-host balancing of VMware Distributed Resource Scheduler (DRS). VMware ESX Server can halt and reschedule a virtual machine without regard to the activity of threads inside the guest operating system. This creates a more deterministic resource sharing that improves user experience in a VDI environment.

In contrast to Terminal Server based centralized computing, Virtual Desktop Infrastructure (VDI) gives each user an independent virtual machine for desktop computing. Running Citrix, Terminal Server, or any multi-user operating system by itself is not an example of VDI. By giving each user their own operating system, VDI provides the stability and performance management features necessary for enterprise deployment of centralized desktops.

VDI's Contributions to Desktop Management

VDI brings together the benefits of centralized and distributing computing. With a number of unique features, VDI provides a new alternative to the traditional computing models.

VDI offers the Benefits of Server Based Computing

VDI is a new server based computing model that achieves the benefits commonly associated with Terminal Server deployments. The areas where server based computing shine are:

- **Data Security:** Keeping data within the confines of the datacenter improves security.
- **Reduced Hardware Expenditures:** Consolidation and reduced upgrades cycles minimizes hardware costs for server and client side equipment.
- **Easier Management**: Perform centralized patching and application installation or streaming without loading the network.
- **Mobile Workforce:** User desktops are portable – users can reconnect from any location with a variety of devices.
- **Resource Pooling:** Server based computing improves a company's ability to use resources as a common pool.

VDI offers the Benefits of Distributed Computing

VDI retains many of the benefits associated with distributed computing. By giving each user their own operating system, VDI retains many of the strong features of distributed computing including:

- **End User Isolation:** The majority of crashes on Terminal Server derive from "blue screen" events. Terminal Server entrusts user sessions to the good behavior of other users' applications. Untested combinations of software together with the strain of large complex workloads often contribute to blue screen events. In contrast, VDI does not need to trust the operating system's stability for multiple users or assume that the many permutations of running software will remain stable. VDI protects each user from problems generated by other users. This protection eliminates the kind of operating system crashes that affect 30 or 40 users at a time while VDI users can retain the level of isolation taken for granted in distributed computing. Power users can install software and reboot their desktops without affecting other users.
- **Improved Performance Isolation:** PC users expect full access to their own CPU, memory and disk resources. Terminal Server suffers from resource contention between users. Introducing heavy applications to an existing farm of two-way Terminal Servers with published desktops can create erratic performance because the actions of a few users will periodically degrade performance for all other users on the server. VI3 allows nearly linear scaling of VDI sessions on up to 16 CPUs and farm wide session portability through VMware Distributed Resource Scheduler (DRS). The ESX Server scheduler can locate spare CPU cycles for heavy users on the largest servers and use VMware VMotion™ to move select user sessions to other hosts using DRS.

Companies can now deploy centralized computing with the confidence that their infrastructure can accommodate deployment of unforeseen applications without compromising user's desktop experience. Virtual desktops are now free to utilize spare CPU cycles across a whole farm of ESX Server hosts. In this way, VDI shares in the CPU borrowing typical of clustering solutions while maintaining the user isolation of PC environments.

New Benefits for Desktop Management

VDI brings together desirable features of traditional Terminal Server based while retaining important features of distributed computing. VDI also introduces new and unique benefits such as:

- **Performance and Stability Benefits:** VDI is the first computing model that allows user sessions to use resources across a farm of servers. Centralized execution of user sessions is possible without relying on the Windows kernel to coordinate multi-user sessions. The ability to create a self-balancing farm with transparent user migration between hosts greatly expands the number and type of applications deployable on a server based computing model.
- **Opportunity to Redesign the Desktop:** By leveraging the unique memory management of ESX Server, gigabit networking, and high-speed shared storage, VDI desktops can achieve new levels of performance, exceeding what stand-alone PCs can deliver.
- **No Downtime Maintenance:** Hardware maintenance on any ESX Server host can proceed without waiting for users to logoff and without interrupting user sessions. Placing an ESX Server host in maintenance mode will migrate all active VDI sessions elsewhere within the farm. This feature allows IT staff to perform maintenance during regular business hours without affecting users.
- **Integrated Server and Desktop Management Platform:** For the first time, companies have the opportunity to unify the management of user desktops and servers. IT can simplify datacenter processes and improve coordination between server and desktop support groups. A single design for backup and disaster recovery functions can serve the needs of both server and desktop areas.

- **Business Continuity Benefits:** Users that traditionally needed their own PC can now benefit from the portability of centralized computing.
- **Licensing Benefits:** VDI opens new opportunities for conserving licenses. Products based on the number of concurrent installations can take on a concurrent-usage licensing model if used with one of the several connection broker tools offering dynamic provisioning capabilities.
- **Granular Performance Control:** While resource leveling products allow more granular control of application priorities within Terminal Servers, VI3 introduces resource pools that can be used to designate groups of user desktops that receive farm wide priority. VI3 allows VIP users or CPU heavy applications to execute in separate pools distributed across ESX Server clusters.
- **Elimination of Multiple N+1 Computing Silos:** Due to application compatibility issues, Terminal Server deployments often segment applications onto their own server pools. This requires the addition of servers to each published application group for fault tolerance regardless of capacity. VDI's user isolation allows provisioning of servers based on capacity alone, reducing server count while maintaining fault tolerance.
- **New Options for Application Management:** Leveraging Templates and Cloning, administrators can establish departmental machine templates and quickly deploy new user desktops as needed.

VDI and Desktop Stability

Each application launched inside a shared operating system has the potential to conflict with any other application, and to exert pressure on underlying drivers, system services, and kernel scheduling. VDI isolates each virtual desktop from malfunctions caused by the activities of other users. No multi-user platform is immune to hardware failures, but the hypervisor design of ESX Server provides substantially more protection for user sessions than the shared services design of Terminal Server.

ESX Server manages resource allocation using the VMkernel, a mini-operating system built from the ground up for stable resource allocation. The VMkernel is a compact yet sophisticated resource manager enabling many VDI desktops to share underlying physical resources while maintaining user isolation. VMkernel faults are exceedingly rare as compared to the frequency of Windows blue screen crashes inside a busy Terminal Server running a heavy load of diverse application software. The many functions and services of the Windows operating system create more opportunities for conflicts than are seen in the more compact VMkernel.

Terminal Server creates many more opportunities for conflict than a single-user PC. Rare incompatibilities manifest more frequently in proportion to the number and diversity of applications running together inside a single operating system. The number of application combinations that can appear inside the operating system contributes to the instability by elevating the number of ways in which applications can interact and exert stress on the operating system.

A Terminal Server serving twenty-five users running five applications each will host 125 applications concurrently. This exerts twenty-five times more strain on the operating system than a single user generates on their PC. The extra strain on the operating system combined with the typically larger number of installed applications leads to an inherently higher level of instability in multi-user operating systems.

By giving each user their own operating system, VDI contains the risk of application conflict to a similar level experienced by PC users with their own operating system. VDI mitigates risk to the shared ESX Server host by containing fatal conflicts to one user operating system. This drastically

reduces the chance of software conflicts causing large-scale disruption. VDI provides a new centralized computing model without excessive risk of negative application interactions.

VDI Cost Savings

When considering the total cost of ownership, simplistic evaluations of costs fail to show the full picture. There are hidden costs and risks with each desktop management model and each execution model. Key areas of cost savings for VDI include:

- **Hardware Provisioning Logistics:** VDI simplifies deployment of new infrastructure.
- **Hardware Maintenance:** VDI offers the least complexity and most advanced management options for zero-downtime hardware maintenance.
- **Hardware Duration:** The pooled resource model of a VMware Virtual Infrastructure 3 (VI3) farm offers very dynamic performance balancing and tuning. This flexibility allows IT to repurpose ESX Server host hardware for any combination of virtual desktops and application servers as performance needs change and newer hardware becomes available. This extends the useful life of ESX Server host hardware.
- **Less Downtime:** The stability of ESX Server combined with the isolation of end-users limits downtime related to software malfunctions. VI3 contains several features that contributed to improved uptime for a VDI deployment. VMware High Availability (HA) allows VDI desktops to restart automatically after a hardware failure. VI3 also includes the ability to place ESX Server hosts in "maintenance mode" causing VDI desktops to migrate to other ESX Server hosts without interrupting user sessions during maintenance windows. The well-scrutinized Hardware Compatibility List (HCL) of ESX Server further contributes to improved uptime for a VDI deployment.
- **System Performance:** VI3 offers unparalleled platform balancing, superior resource allocation, and new opportunities for performance enhancements that leverage specific ESX Server memory management features as described in the "Turbo Charged Performance" section below.
- **Application Management:** Application streaming performs even better in a VDI environment due to proximity within a datacenter allowing gigabit Ethernet connections between virtual desktops and their supporting servers. Shared image strategies and use of virtual machine templates also simplify application management.

VDI brings a wealth of new features and cost saving possibilities to the problem of managing user environments. It will be some time before IT departments discover all the new opportunities. The most significant long-term cost reduction VDI brings to the enterprise might prove to be the cost savings associated with increased use of centralized computing. The stability and software compatibility issues of Terminal Server have limited these savings for many companies prior to VDI. Companies can now shift their focus towards server based computing more aggressively with the confidence that critical features like end-user isolation, scalable performance balancing, and decreased application interactions will ensure successful deployment of current and future software.

Business Drivers and Common Use Cases

Early adopters of VDI technology seek to solve problems that non-VDI solutions fail to address. The major use cases currently driving adoption of VDI are:

- **Outsourcing:** Companies looking to outsource development while retaining close control of their data and source code can use VDI to present developers with a fully functional desktop capable of installing development tools and rebooting without affecting other users.
- **Extending PC Lifecycle:** Companies facing a PC upgrade cycle or deployment of a major operating system upgrade might instead migrate to a server based computing model, redeploying existing PCs as Thin Client access devices.
- **Pandemic Planning:** New mandates in nearly every industry require preparedness for pandemic scenarios. VDI provides the needed assurance that existing desktop application suites are deployable in a server based computing model without the software compatibility or performance problems often encountered when deploying a large number of applications on a Terminal Server platform.
- **Unifying IT Strategy:** Companies that have already invested in virtualization strategies in the data center and are seeking to unify desktop and server side processes have an opportunity to leverage server and client side computing loads across a common platform. Simplified disaster recovery, enhanced data security, and reduced headcount can result from such consolidation.
- **Performance Driven VDI:** Companies needing to introduce a demanding new application that strains current PC hardware might elect to deploy the new application as a link from the native desktop to a VDI session. This offloads CPU demands from the local desktop, both extending the PC lifespan and ensuring adequate performance of the new application.
- **Enterprise Desktop Replacement:** Companies seeking to escape the constraints of legacy desktop computing and move towards utility computing will benefit from more advanced VDI configurations with dynamic provisioning and personalization of the virtual desktop made available to stateless user access devices.

VDI incorporates features of both server based and distributed computing, offering business solutions to a number of challenges.

VDI Architecture

VDI is an architecture requiring carefully crafted solutions that meet specific needs. All VDI solutions have virtualization of the user's desktop in common. A complete VDI solution may also include other design elements that compliment, extend, or leverage the core features of VMware Infrastructure virtualization platform. A full spectrum VDI solution starts with the user's access device and includes a number of logically sequential components spanning the full lifecycle of user activity. The section below describes the full spectrum of components together with helpful products in each category and several design examples meant to illustrate various problems solvable within a VDI framework. The list of products is not inclusive due to lack of space and meant to highlight significant products in each category.

Design Components for a complete VDI Solution

A complete VDI solution involves several components selected to meet the specific requirements of the situation. This section describes each design component in detail. Figure 1 shows VDI design components and related products:

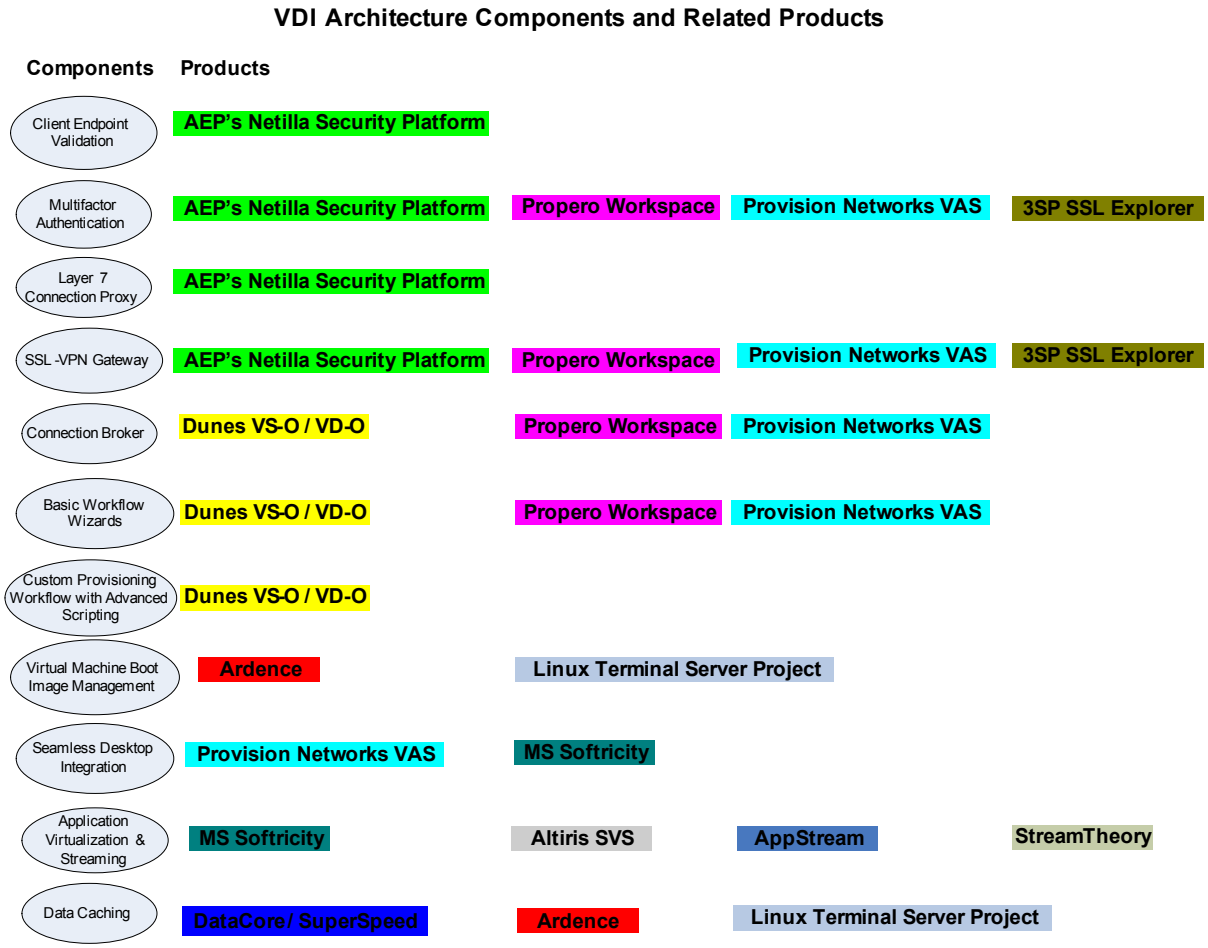

Figure 1 – VDI Architecture Components and Products

Client Access Device

On a PC running Microsoft Windows, users can initiate a remote session to a VDI resource using the bundled remote desktop client. Thin Client devices such as WYSE terminals have many advantages as access devices including reduced cost, stateless configuration and simplified management. An RDL (Remote Desktop License) might be required to connect back to the virtual desktop.[3]

- **Terminal Makers:** Leading Thin-Client device manufacturer WYSE makes quality low cost graphical terminals. WYSE terminals lead the market with their small footprint, low power consumption and flexible Thin-OS firmware.[4]
- **PCs:** An older underpowered PC can make a very capable VDI access device. Hybrid solutions with some local execution and select VDI assisted application execution might also be appropriate.

Secure Access

If the PC is outside the company firewall, an SSL or IPSEC VPN may be required to avoid exposure of multiple mapped IP addresses on the external firewall and to improve security for VDI session. Without an SSL-VPN, RDP is vulnerable to "Man in the Middle" spoofing attacks that an SSL-VPN

[3] We recommend checking with Microsoft Licensing for more details.
[4] Learn more about WYSE products at http://www.wyse.com

can prevent using certificates. Companies providing access only to internal parties may not need an SSL aggregation point in the DMZ.

- **AEP Networks:** The AEP Netilla Security Platform (NSP) is a hardened appliance offering a full spectrum SSL-VPN solution with many security features. Dynamic firewall and just in time port mapping together with client integrity checking, connection proxy, and protocol translation features make the NSP a great choice for SSL aggregation.[5]
- **Propero Workspace for VMware:** Propero offers a sophisticated server based SSL-VPN gateway solution with the ability to make remote VDI applications appear to be running on the local taskbar as local applications. Propero Workspace for VMware includes an advanced connection broker function for pooled virtual machines and the ability to connect users to a wide range of datacenter resources.[6]
- **Provision Networks Virtual Access Suite:** The Virtual Access Suite offers an SSL-VPN gateway solution focused squarely on Windows VDI desktops and Terminal Server resources. The product allows shortcuts to VDI hosted applications to appear on the local desktop and program menus.[7]
- **3SP SSL Explorer:** This is a low cost yet capable SSL-VPN without advanced security or connection broker features.[8]

Client Integrity Checking and Connection Termination

Companies may wish to restrict VDI access to PCs that meet specific requirements such as an updated anti-virus, anti-spyware, or patch levels. Other companies might want to terminate the TCP connection in the DMZ and have the SSL aggregator proxy the RDP session.

- **AEP Networks:** AEP offers flexible client integrity checking and the ability to translate RDP, ICA, X11 and VNC into a single common "Thin" protocol based on an adaptive compression protocol accessible through a java-based client. This approach guarantees that user sessions terminate with the NSP device. RDP sessions are initiated from the NSP to the Virtual desktop, providing a true layer 7 proxy.

Connection Brokering

Providing users their own virtual desktop and ensuring they always reconnect to the same machine might be the best design for small scale VDI implementations. For larger VDI implementations, a connection broker is necessary to avoid tying up memory and CPU resources when users are not using their virtual desktops. Connection brokers can suspend and resume virtual desktops or provision new desktops based on policies and workflows. Connection brokers make API calls to VMware VirtualCenter and ESX Server systems to perform their core functions.

- **Dunes Technologies:** Dunes Virtual Desktop Orchestrator (VD-O) product provides simplified connection brokering functions. Additional functionality may be achieved when VD-O is paired with Dunes Virtual Service Orchestrator (VS-O), a capable workflow engine ideal for complex provisioning processes involving coordination of multiple products. VS-O helps create custom workflows well beyond simple power on/off and suspend/resume operations. VS-O enables full lifecycle management of the virtual infrastructure and business processes surrounding VDI deployments. Dunes products do not include an SSL VPN access infrastructure.[9]
- **Propero Workspace for VMware:** Users can connect to one or more desktops or single applications published from within virtual desktops. The Propero Tunnel server can even connect users to virtual

[5] Learn more about AEP products and the Netilla Security Platform at http://www.aepnetworks.com
[6] Learn more about Propero Workspace for VMware at http://www.propero.com/workspace-for-vmware.html
[7] Learn more about Provision Network's Virtual Access Suite at http://www.provisionnetworks.com/solutions/vas/vas.aspx
[8] Learn more about SSL Explorer at http://www.3sp.com/showSslExplorer.do
[9] Learn more about Dunes Technologies SA at http://www.dunes.ch

desktops on un-trusted networks using SOCKS tunneling. Propero combines SSL-VPN access with pooled management of virtual desktops. Propero does not include a custom workflow engine but has many predefined functions for provisioning and user management. Propero Workspace for VMware excels in heterogeneous environments with a rich variety of resources including mainframe, Terminal Server and VDI desktops and applications.

- **Provision Networks Virtual Access Suite**: Building on success in the Terminal Server arena, Provision Network's Virtual Access Suite (VAS) targets Windows based environments. VAS offers excellent desktop integration with published shortcuts on the desktop and start menu, SSL-VPN, web access and the best "last mile" features such as USB redirection, multi-monitor support, resolution up to 4096x2048, session sharing and more. Basic workflows and wizards help automate provisioning and maintenance functions while providing policy based controls for VDI resources.

Boot Image Management

The need for each user's operating system to have its own hard drive comes from the days where off-network usage was the norm and slow networks prevailed. Virtual desktops reside in the datacenter with gigabit Ethernet connections. Booting virtual machines over the network using the virtual machine network interface card's built in PXE boot feature is a smart way to share a single boot image across large numbers of virtual desktops. A deployment of 5000 users each with a five-gigabyte Windows XP boot disk would consume twenty-five terabytes of shared storage. A shared image strategy saves on storage and provides a single location to patch and deploy applications. Patching or modifying shared boot images is easy and changes propagate to virtual desktops the next time they boot. Products enabling diskless VDI desktops include:

- **Ardence:** Ardence provides advanced image sharing technology. An association between virtual machine MAC addresses and boot images enables virtual desktop personalization on boot with predetermined machine names. Ardence tools map diskless virtual machines to their own shared boot image, storing changes in either a client side RAM disk, a server side RAM disk or a client side hard drive. Ardence tools conserve storage and allow a central boot image to serve a large number of virtual desktops.[10]
- **Linux Terminal Server:** For companies interested in Linux based desktops, the Linux Terminal Server Project (LTSP)[11] provides a similar ability to boot diskless virtual machines that auto configure and run partially from the network and partially from client side RAM disk. Distributions such as Cluster Knoppix[12] go further by allowing transparent process migration between virtual desktops through use of the Open Mosix Kernel extensions.[13] This Single System Image (SSI) clustering enables virtual desktops to borrow CPU cycles from other virtual desktops. One virtual desktop could tap over 30GHz of CPU cycles on a farm of two four-way servers. Stacking of Single System Image clustering on virtual infrastructure delivers the benefits of supercomputing without dedicated physical clusters or physically dispersed cluster nodes. Many Windows based applications run on clustered Linux Desktops using WINE[14] or CodeWeaver's *CrossOver Office*[15] emulator product. Single System Image clustering stacked on VDI creates a computing model combining elements of distributed, centralized, and clustered computing models. This approach extends the concept of resource pooling to a more granular level while retaining the benefits of end-user isolation for non-clustered applications.

[10] Learn more Ardence Desktop Edition at http://www.ardence.com/enterprise/products.aspx?ID=83
[11] Learn more about the Linux Terminal Server Project at http://www.ltsp.org
[12] Learn more about Cluster Knoppix at http://clusterknoppix.sw.be
[13] Learn more about OpenMosix Single System Image clustering at http://openmosix.sourceforge.net/
[14] Learn about WINE at http://www.winehq.org
[15] Learn about CodeWeaver's CrossOver Office at http://www.codeweavers.com

Application Virtualization and Streaming

The growth of distributed computing brought the challenges of management to the forefront of the IT agenda. The needs of distributed computing shaped the early management toolsets. Each node on the network was a stand-alone resource silo. Each node needed its personality maintained separately. Server based computing allowed for a more consolidated approach but brought new management challenges related to performance, network stability and software compatibility. Recently, streaming technologies such as Microsoft Softricity[16], AppStream and others have introduced a unified application management approach that simplifies application lifecycle challenges in a way that can benefit both distributed and server based computing models.

Combining application streaming and application virtualization, Microsoft Softricity adds value by simplifying application lifecycle management. After sequencing applications, the Softgrid client publishes shortcuts to users based on their group membership. Administrators can upgrade applications while users work by publishing a new version available at next application launch. Application virtualization features can aid application compatibility by allowing applications with different versions of the same DLL or conflicting registry settings to run together. When deployed with Ardence shared boot imaging, it is possible to deploy VDI architecture with diskless virtual machines booting against a shared Windows image with only the Softgrid client installed. This one image can serve the entire company. Sequenced applications can be pre-cached to the shared boot image, eliminating the network traffic and launch latency associated with application streaming. AppStream focuses on application delivery while Altiris SVS focuses on application virtualization without all the isolation features of Microsoft Softricity. These new technologies complement VDI by further centralizing management of the desktop and providing application access without the need to persist application software inside the virtual machine hard drive.

Turbocharged Performance with Data Caching

CPU advances have followed Moore's law for many years now roughly doubling in speed every 18 months. Memory technologies have gained ground almost as quickly. In sharp contrast, hard drives have taken over 10 years to double in speed. This widening gap in performance makes the rotational and seek time latency of hard drives the biggest performance bottleneck in modern computers. Caching and RAM disk tools address this gap by moving data close to the operating system.

Shared storage systems contain RAM caches but usually have only a few gigabytes of memory for the entire flow of company traffic. Deploying cache technology will greatly accelerate performance by reducing disk queues and eliminating CPU cycles spent waiting for disk I/O. In a VDI ecosystem, every CPU cycle saved within the virtual desktop is a cycle ESX Server can allocate elsewhere. Cache technology is a good fit with VDI, enabling desktops that are more responsive and offsetting virtualization overhead. If Ardence boot tools are used, caching can greatly reduce the network load between the virtual desktop and the Ardence image distribution server, replacing network latency with memory latency.

The transparent page sharing feature in ESX Server will actively de-duplicate underlying memory. Identical disk blocks cached in multiple virtual desktops will be stored only once in the ESX Server host's memory. Leveraging this powerful underlying memory management feature allows VDI to facilitate the benefits of RAM caching without the need to purchase large amounts of additional RAM for the ESX Server hosts. The following products provide caching tools that can assist VDI deployments:

[16] Learn about Microsoft Softricity at http://www.softricity.com

- **DataCore:** DataCore's UpTempo[17] product installs a block level cache that sits under the file system and above the device driver. UpTempo assigns about thirty percent of available memory in the guest OS to the cache. A write cache also allows instant commits and periodic de-staging of data blocks down to disk.
- **Ardence / SuperSpeed:** SuperSpeed sells a product called SuperVolume[18] that completely caches a disk partition into memory. Ardence plans to release a built in RAM disk with version 4.1 of their image management suite creating the only solution that combines image management and accelerated performance. All disk reads come out of RAM and all writes get instant commits and de-stage to disk periodically.

Cache Design Alternatives

The following design alternative integrate data caching with VDI deployments:

- **Block Cache:** Block caching using tools such as UpTempo allocates a preset amount of memory to storing data blocks requested by the file system. Pre-fetching of data block based on usage patterns further accelerates data access. Writes can be written to memory and flushed to disk periodically for improved performance.
- **Boot Partition Caching:** VI3's 16GB of memory per virtual machine is adequate for full caching of the boot volume including application installations to memory on 64-bit virtual desktops. A Assuming a Windows XP boot image containing installed applications is 9GB, VDI desktops could be allocated 10GB for a 64-bit Windows XP or Windows Vista.boot image, providing the virtual desktop 1GB of working RAM and lightening fast access to applications and operating system functions.
- **Application Partition Caching:** For 32-bit virtual desktops, caching the boot partition would leave no room for working memory. Creating a dedicated partition of several gigabytes for application installations can accelerate launch times and improve application responsiveness. SuperVolume can cache the contents of this volume on boot. Use of Microsoft Softricity or AppStream minimizes the disk space consumed by application installs by locating only a small fraction of application code locally (known as feature block one) and streaming the rest on demand.

VDI Memory Efficiencies

Allocating a large amount of RAM for caching would normally be cost prohibitive in a distributed computing model. ESX Server transparent page sharing ensures that additional VDI instances will consume only a portion of the 1GB of working RAM that is unique to each desktop. The balloon driver included with VMware tools will yield unused working memory to the underlying memory pool. The ability of ESX Server to locate common memory pages within the working memory will usually reduce memory consumption by thirty percent or more, compensating for the extra RAM used by caching strategies. Booting multiple machines from a shared Ardence controlled boot image ensures that the cached boot volumes will all be nearly identical. This in turn ensures that memory page signatures will be identical and transparent page sharing will achieve maximum efficiency.

To minimize the percentage of RAM allocated to cache, it is best to deploy this strategy with large ESX Server hosts dedicated to VDI. On an eight-way ESX Server host with 48GB RAM, perhaps seventy-five or more users could obtain the benefits of RAM disk performance with only 9GB of RAM allocated to caching for 64bit virtual machines or as little as 2GB for 32bit virtual machines with cached application partitions.

[17] Learn more about DataCore's UpTemo product at http://www.datacore.com/products/prod_UpTempo.asp
[18] Learn more about SuperSpeed's SuperVolume product at http://www.superspeed.com/desktop/supervolume.php

Within a year, an eight-way quad core host with 64GB RAM could provide RAM disk performance to 120+ users with only 9GB dedicated to caching. The ability to provide both user isolation and RAM disk levels of performance affordably is a fundamental improvement in desktop computing that only VDI on VI3 can provide. The density of memory chips is growing much faster than the size of boot partitions. High capacity memory chips combined with quad core CPUs and VI3's memory management brings a caching strategy well within reach for enterprise VDI deployments. The dramatic performance gains resulting from a RAM based desktop will improve user productivity, extend the ESX Server host hardware lifespan, and set new standards for user desktop experience.

Deployment Scenarios

Having examined the design components of VDI architecture along with third party tools, the following design scenarios illustrate how VDI solutions meet varying requirements.

Scenario 1: Outsourced Development

Requirements: A company wants to provide secure desktops to five-hundred developers outside the country. Offshore developers will access their virtual desktop through the Internet. Developer PCs will be considered un-trusted and must qualify to access the virtual desktop by passing a series of tests that include checking anti-virus versions, Windows updates, and Windows firewall settings. Each user will have their own desktop mapped one to one and will need the ability to reset their Virtual Desktop through a web interface. The company also wants a custom provisioning workflow for new desktops that includes Active Directory account creation, provisioning of virtual desktops, deploying application software using an existing distribution tool and finally, notification of the project manager by email when the new developer's desktop is ready for use. Developers have over 220 millisecond of latency in their WAN connections and require the most responsive desktop possible to offset this performance handicap.

Design Solution: The need for SSL-VPN aggregation together with rigorous client integrity checking makes AEP's NSP security appliance an excellent choice. Connection broker functions are minimal since virtual desktops are not pooled. Requirements for a complex provisioning workflow suggest that DUNES VS-O would be a good choice. The combination of AEP's NSP appliance for access infrastructure and DUNES VS-O for powerful workflow customization make this a capable and secure VDI solution. Installation of developer applications on a cached partition improves performance, helping offset WAN latency. See Figure 2 for diagram.

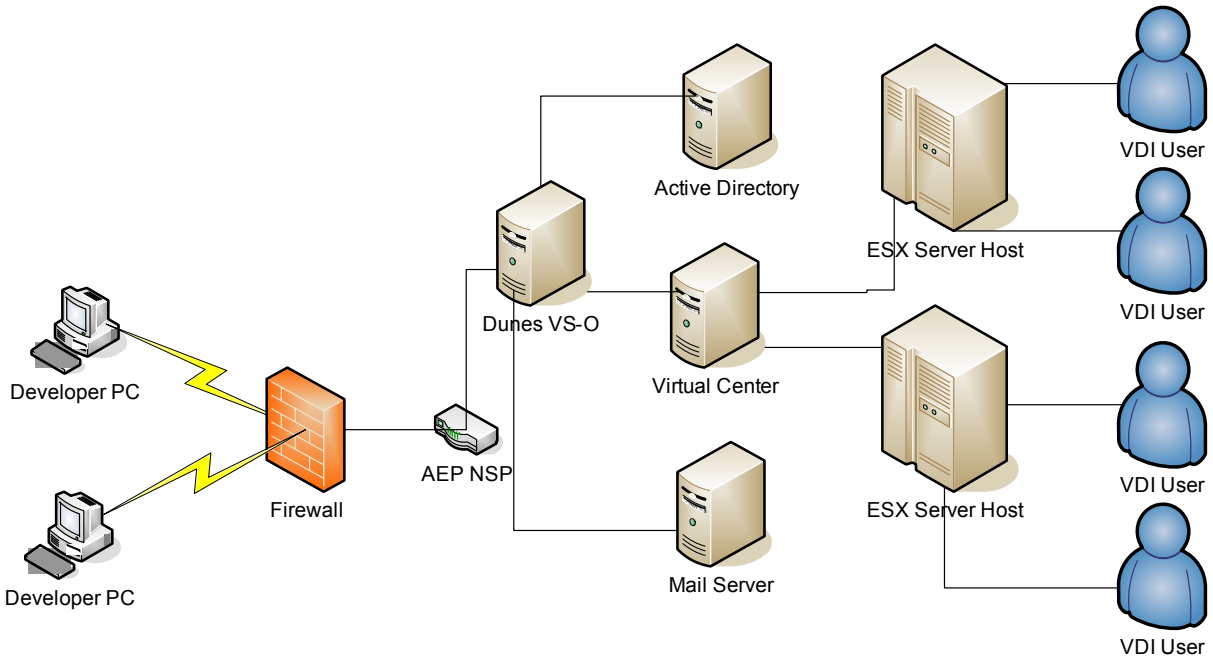

Figure 2 – VDI Solution combing *AEP's NSP & Dunes VS-O.*

Scenario 2: Support Solution Managing Hybrid Resources

Requirements: A software and services company has support contracts worldwide for a variety of companies. Supported platforms include mainframe, x86, UNIX, and Novell. Technicians across multiple time zones need to access supported company networks with a common access infrastructure from their homes or offices using an Internet based VPN solution. Each technician has multiple virtual desktops that connect back to different company networks together with Terminal Server sessions, 3270 sessions, and some Windows 2000 and Windows XP desktops. Technicians also need to access their own personal desktops using VDI. The company is looking for a single vendor solution that meets all their requirements in a secure and elegant manner.

Design Solution: The diversity of application platforms combined with connection brokering functions, SSL-VPN and connectivity to outside networks through a common access infrastructure make Propero's Workspace for VMware product an excellent choice. In a single product, it provides seamless support for a wide range of platforms, mature SSL-VPN, and the ability to tunnel into other networks using SOCKS protocol. Propero support Windows 2000 desktops using Danware's NetOp remote access product. These wide-ranging features and flexibility set it apart as a good choice for heterogeneous environments. See Figure 3 for diagram.

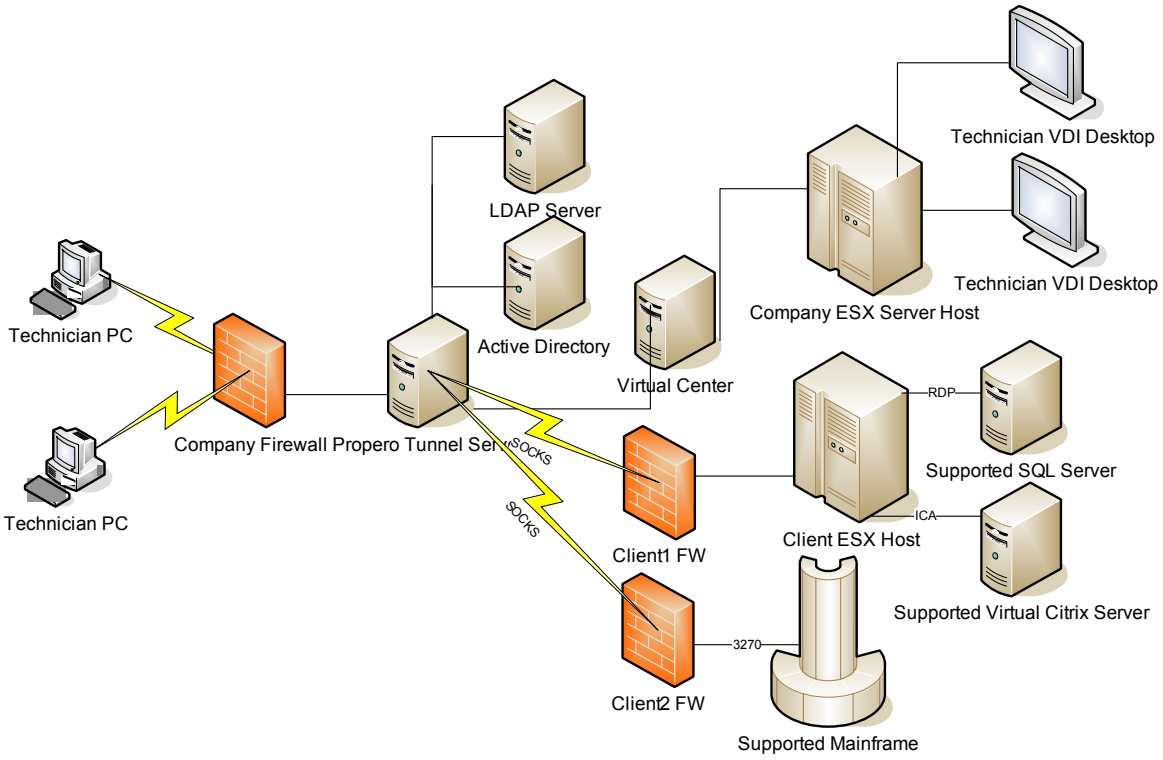

Figure 3 – VDI Solution using *Propero Workspace for VMware*.

Scenario 3: Local and VDI Apps with Application Virtualization

Requirements: A company specializing in multimedia needs to get control over its application deployment across nationally dispersed branch offices. Technicians work on video editing software that requires demanding low latency local video. Post processing video transformations using the same program can take several hours and often lock up local PCs, detracting from productivity. Management needs a way to keep workers productive during video post processing but also minimize the burden of software deployment and OS patching. Access from home is important so that batch jobs can be set up during off hours. The solution must be highly integrated with local desktops since users are non-technical outside of their editing software. Each branch office has its own ESX Server hosts and data stores.

Design Solution: Sequencing the video editing applications with Microsoft Softricity provides a way to publish the same application for both local execution on PCs and centralized execution on VDI desktops without the need for manual installation. Provision Networks' Virtual Access Suite (VAS) provides a connection brokering solution that seamlessly publishes desktop icons that launch VDI hosted applications without the need to log into a web portal. Users launch the local version of the video editing application for editing tasks using a shortcut published with Microsoft Softricity's Softgrid client. Users launch a VDI hosted instance of the editing software for post processing jobs using a shortcut published by VAS AppPortal. Access from home through the VAS web interface will facilitate remote post processing setup. Ardence image tools allow all VDI hosted applications to share a common boot image with only the Softgrid client installed. See Figure 4 for diagram.

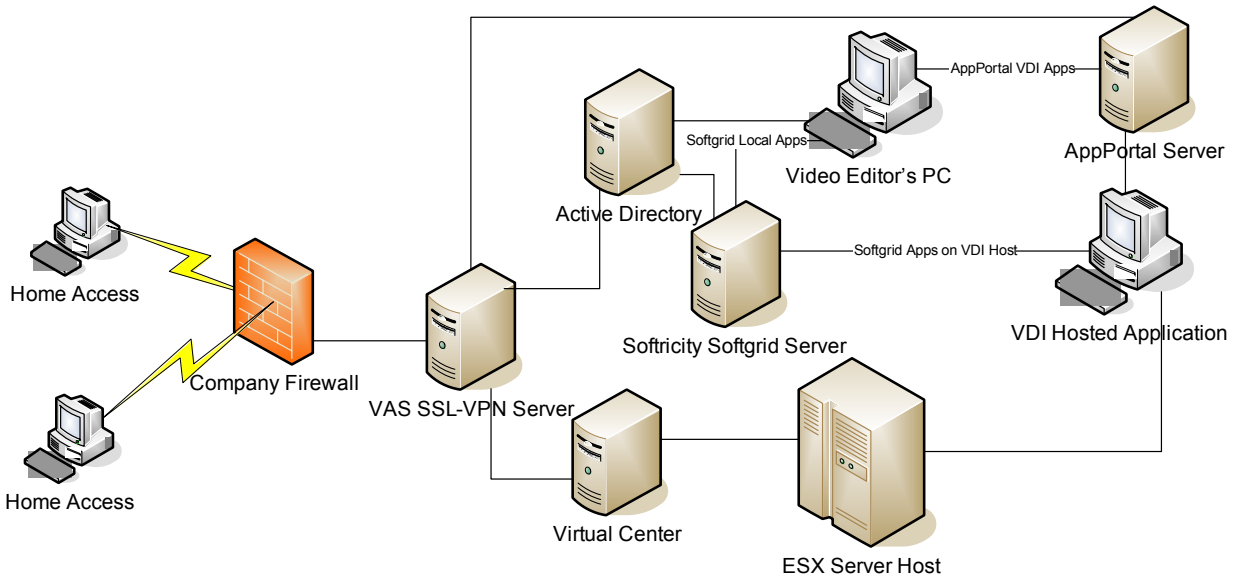

Figure 4 – VDI Solution using Provision Networks *Virtual Access Suite*.

Customer Testimonials

A large number of organizations have successfully deployed and leveraged the VMware virtual desktop infrastructure in their deployments. Bell Canada uses VMware software to provide 1700 customized desktops environments. According to Martin Quigley, CGI Senior Technical Consultant to Bell Canada, "With VMware virtual desktop infrastructure, we are able to manage complex, secured desktop environments from our datacenter. This has made it easy for Bell Canada to create and manage 1700+ desktop environments for call center agents. We will continue to utilize the solution because it gives us the flexibility to easily and cost-effectively provide customized desktop environments."[19] VDI is gaining momentum and many more customer stories will be available over the next year as creative VDI solutions are put in place around the world.

Conclusions

When deployed with complementary products, VDI retains the best features of Terminal Server based desktops and distributed PCs while bringing new performance and management possibilities to the mix. With increasingly prevalent wireless technology like 4G cellular (100mbit), WiMAX , and WiFi on Airplanes becoming the norm, the need to work offline will become increasingly rare. Quickly advancing CPU and memory designs will heighten the benefits of centralized computing, allowing improved use of shared resources.

The unique performance and security characteristics of VDI position it as a strong contender as well as a value-add to current server based computing technologies. Desktop management is evolving towards an increasingly sophisticated blend of VDI, Terminal Server, and distributed computing. This new blended approach will have a stronger bias towards server based computing models which best use shared resources. Applications with lighter CPU loads and no Terminal Server compatibility issues will continue to leverage Terminal Server, while heavy applications and published desktops will migrate towards VDI where the benefits of isolation and improved resource allocation will benefit the user experience.

[19] Read more about Bell Canada's deployment at http://www.vmware.com/customers/stories/bell_canada.html

Application virtualization and streaming platforms that provide centralized application distribution and management across distributed and centralized computing platforms will supersede tools focused on distributed computing. Within the new hybrid framework, utility VDI based desktops will help craft a unified server and desktop management strategy that delivers operational simplicity and improved business continuity. VDI might even eclipse server side virtualization as a driver of Virtual Infrastructure, establishing for itself a dominant position at the center of IT strategy.

About the Author

Daniel Beveridge is a Senior Solution Architect with Foedus, a leading provider of Virtual Infrastructure consulting and integration services. Daniel has three years experience managing a mid-size company's entire server infrastructure on ESX Server, and prior to that, fifteen years experience in programming, system and software architecture design, and implementation of infrastructure solutions. Daniel has developed innovative VDI designs that bring together multiple products to create new business solutions in Fortune 100 companies in the financial, pharmaceutical, and other industries.

Revision: 20061129 Item: WP-009-PRD-01-01

VMware, Inc. 3145 Porter Drive Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com

© 2006 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,961,941, 6,961,806, 6,944,699, 7,069,413; 7,082,598 and 7,089,377; patents pending.

VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

vmware®

foedus