

Nutanix White Paper



Desktop Virtualization and Health Care

This whitepaper explores the usage of desktop and application virtualization in health care. It covers the concepts and benefits of VDI, discusses the challenges with traditional IT infrastructure, and presents the economic and operational value of using Nutanix for desktop virtualization.

Table of Contents

Executive Summary.....	3
Audience and Purpose	4
What Is VDI and How Does it Differ from SBC.....	5
VDI Benefits for Health Care.....	6
Reducing IT Costs with VDI and Nutanix.....	9
The Challenge with Traditional Storage.....	10
Enabling VDI ROI with Nutanix	10
Why a Strategic Approach to VDI Is Imperative	13
Conclusion.....	14

Executive Summary

Virtual Desktop Infrastructure (VDI) continues to build momentum as a potentially transformative technology in increasing IT efficiency. VDI can be particularly beneficial to the health care industry by enabling health care institutions to better meet the requirements for quality, speed, and privacy in patient care and data.

Given the high cost of health care professionals' time, the increased productivity facilitated through VDI may have a greater economic impact than any infrastructure-based cost reduction. And while infrastructure-based costs can represent immediate savings, VDI deployments in health care facilities enjoy a myriad of benefits in terms of increased efficiencies and data security enhancements.

Hospitals planning to take advantage of VDI for cost, efficiency, and security reasons have an opportunity to incorporate virtual desktops as an integrated component of an overall virtualized data center. From an IT perspective, virtualizing the desktops enables IT's transformation to a private cloud with automated self-provisioning and functionality such as metering, monitoring, and chargeback.

Implementing virtual desktops for health care environments, however, does not mesh well with traditional storage architectures. Organizations face either purchasing storage infrastructure up-front with far more capacity than required, or risk forklift upgrades down the road. The initial capacity must be adequate to handle any future growth in the users, new applications, or other unanticipated resource requirements, as well as spikes in intermittent resource utilization.

Nutanix helps health care facilities move to desktop virtualization by bringing the value of web-scale technologies used by Google, Amazon Web Services, and Microsoft Azure to the enterprises. Web-scale enables consolidation, linear scalability, fractional consumption, and an abstraction of the intelligence from traditional hardware arrays into software-defined storage. The compute and storage tiers combine into a single consolidated infrastructure.

Nutanix brought this model to the enterprise by leveraging the hypervisor to virtualize the storage controllers. Since every server is a virtual storage controller, the challenges facing traditional storage architectures, including overprovisioning and unpredictable performance, inability to quickly scale, and complex management are eliminated. In addition to being able to realize the productivity and secure benefits, Nutanix enables IT organizations tied to health care delivery get an excellent ROI on their VDI projects. A Nutanix customer with a plan to move 2,500 PCs over to Nutanix over 5 years will be able to realize a 296% ROI with a payback period of just 9.6 months.

Virtual Desktop Infrastructure, when built upon the Nutanix architecture, can serve as a unifying platform that simplifies the environment, eliminates technology islands, and secures patient health information, while reducing overall costs.

Audience and Purpose

This whitepaper is intended for datacenter/desktop managers, architects, and consultants responsible for infrastructure for desktops and end-user applications. Some familiarity with virtualization (i.e., VMware vSphere, Hyper-V) is assumed. This paper evaluates the usage of VDI in health care including:

- What is VDI and how does it differ from server-based computing (SBC)?
- VDI benefits for health care:
 - Improved clinical efficiency
 - Improved IT efficiency
 - Improved security of PHI
- Reducing IT costs with VDI and Nutanix
- The challenges with traditional storage
- Enabling VDI ROI with Nutanix
- Why a strategic approach to VDI is imperative

What Is VDI and How Does it Differ from SBC

Many health care organizations are familiar with Citrix Presentation Server and/or Microsoft Terminal Server (now called RDS), which they use as part of a server-based computing (SBC) deployment. SBC allows multiple users to share the same Windows Server (RDS) operating system. Alternatively, VDI allows each user to run a separate Windows OS (i.e., Windows 7 or Windows 8) desktop session. Both VDI and SBC are similar in that they intelligently separate the personality of the user from the applications and abstract both from the OS. They enable a model of personal computing where the information belongs to the user and the device becomes a “choice” whether a PC, laptop, thin client, Mac, iPad, iPhone, or Android tablet. Users can securely establish a session from anywhere they can access a browser. The session remains exclusively in the data center where it is secure, managed, backed up, and replicated off-site for disaster recovery purposes.

While Citrix created server-based computing nearly 20 years ago, it has primarily been utilized for application delivery. Difficulties in resolving application incompatibilities, providing users with a familiar “look-and-feel” desktop, session lock down, printing, and administrative requirements have kept SBC from wide-scale adoption despite the cost advantages. Virtual Desktop Infrastructure (VDI), on the other hand, started around 2006, and increasingly captured the interest of IT professionals and business leaders already familiar with server virtualization. IT is generally more receptive to the simplicity of the virtual desktop concept than to the idea of enterprise SBC.

Gartner refers to the concept of VDI as Hosted Virtual Desktops (HVD), while IDC calls it Centralized Virtual Desktops (CVD). The VDI industry has prodigious momentum and now not only includes VMware and Citrix, but also Microsoft, Red Hat, Dell, and many smaller niche players along with a rapidly growing ecosystem including organizations such as Unidesk, Liquidware, and AppSense.

SBC enables the use of thin clients, while VDI enables the use of either thin clients or zero clients. Zero clients are manufactured today by LG, Samsung, EVGA, Dell, Cisco, and many others. Zero clients have no local OS at all, and are therefore particularly easy to support.

Both thin clients and zero clients are fairly inexpensive and have no moving parts, local drives, or fan noise. The devices are configured simply by plugging them in, enabling quick and simple replacement in the event one fails. They eliminate the requirement for upgrading PCs or laptops on a regular basis, as well as the necessity for users to double as desktop administrators. User productivity is enhanced while IT support time is reduced.

Both SBC and VDI can reduce anti-virus costs, slash power consumption (by using terminals), and reduce downtime while users await new upgrades or help desk support. They empower users – giving them a new level of flexibility and agility. They facilitate acquisitions by enabling quick assimilation of new organizations into the existing desktop infrastructure while still allowing them to run their existing environments in parallel. They enable fast set-up of remote facilities and reduce time to market by accelerating application provisioning.

Unlike SBC, the ability for users to work on a rich Windows 7 or Windows 8 desktop is one of the most compelling aspects of VDI, along with no concerns about application incompatibilities due to running on a specialized version of Windows Server (RDS). Other advantages include enhanced security posture, fault tolerance, superior load-balancing, easier backups, lack of DLL conflicts, and a potential pristine desktop every time a user logs in. VDI

administrators do not need to be specialists in RDS or server registry hacks, and can utilize standard Windows printing.

One of VDI's most attractive capabilities is the ability for health care workers who use multiple devices in order to work from home, outpatient facilities, or even from multiple rooms. VDI offers an efficient alternative where users simply and securely log onto their virtual desktop from any device, from anywhere, and are consistently presented with an identical user interface.

VDI Benefits for Health Care

Unlike many businesses and organizations that may have only a handful of applications to support, health care facilities have scores or even hundreds. Increasing regulations in health care make information control more important than ever while expensive staff necessitates IT systems enabling as efficient use of their time as possible. The prevalence of outpatient services, industry consolidation and the push for Accountable Care require faster, simpler, affordable, and more secure deployments.

The high cost of health care professionals means that increasing productivity through VDI may have even a more significant economic impact than any infrastructure-based cost reductions. And while infrastructure-based costs can represent immediate savings, VDI deployments in health care facilities are poised to enjoy a myriad of benefits in terms increased efficiencies and data security enhancements.

Improved Clinical Efficiency

- **Improved Mobility.** VDI truly lets mobile workers access their desktops efficiently and securely from anywhere they can get to a browser. In the world of ever expanding Accountable Care Organizations, industry consolidation, and consultative partnerships, the ability to deploy desktops in a matter of minutes saves time, money, and improves access to critical patient data. With a web browser and user credentials, end users, regardless of their location, have secure access to all desktop tools and available patient information.
- **Follow-Me Desktops.** Clinical staffs tend to log into desktops frequently – 50 times in a shift is not uncommon. It typically takes around three minutes or longer to boot up a standard desktop with data and applications. Utilizing Virtual Desktops, clinical staff can both log on and disconnect from sessions very quickly, reducing access time by around 50%. Consistent desktops also eliminate the confusion of user interface changes when sharing or rotating between multiple workstations or device types.
- **Reduced Downtime.** Failed devices are easily replaced and running in a matter of minutes without the need of rebuilding local drivers and connections to additional end point devices. The ability to quickly return care stations to working status improves the ability to keep utilization of expensive assets like the operation room, MR, and CT areas at high levels.
- **Access.** Ubiquitous access to health care applications will translate into productivity and patient care improvements, which can yield significant benefits. Easier, universal, and secure access to EHR, PACS, labs, and centralized applications will empower end users at the point of care on any device. Eliminating the need for specific task dedicated workstations, virtual desktops will remove the need for multiple logins on different devices and merge the remote silos of clinical data onto a common platform.

- **Rapid Scaling Capabilities.** The rapidly changing health care market forces the need to maintain flexible and adaptable operating environments. With the vast amount of changes in health care today, providers need to remain flexible. Unlike PCs and laptops, which must be ordered, configured, and provisioned – virtual desktops can be deployed in minutes. Health care facilities consequently gain much faster access to desktops required when acquiring new facilities, joining care networks or simply adding new applications.

Improved IT Efficiency

- **Improved Backup.** Since all the virtual desktops reside in the data center, they are backed up regularly without requiring expensive local backup software on individual PCs and laptops. VDI also enables backing up the full desktop image, meaning that it can be redeployed in a matter of minutes rather than the much longer period of time it can take to reimage a physical desktop. Third-party applications by companies such as Unidesk and AppSense give users the ability to roll back their own desktops without requiring IT administrative assistance should they need to recover deleted files.
- **Superior Disaster Recovery.** While organizations may spend a great deal of money implementing data center DR plans, they often forget about the client side of the equation. Even the most sophisticated data center DR plans are rendered ineffective if users can't access the client-server software needed to connect to their applications at the recovery site. And, if the data is sitting on the hard drives of PCs or laptops in the affected building, their ability to fully recover can be seriously compromised. Virtual desktops eliminate all of these issues since they are continuously replicated to the DR facility along with the virtual servers. In the event of a disaster, users just need to get to a browser on any device, from any location, and they can easily and instantly gain secure access to their applications and data at the recovery site.
- **Superior Desktop Management Capabilities.** Pushdown software applications are no longer required for effective desktop management. Indeed, virtual desktops provide the most efficient and effective desktop management possible by separating the desktops from the underlying hardware and associated issues that defective or incompatible hardware can cause. Dozens of desktop images no longer need to be maintained and deployed. Additionally, virtualizing the applications themselves adds yet another layer of abstraction and helps prevent application freezes due to DLL and registry conflicts.
- **Increased IT staff productivity.** The IT staff no longer needs to maintain and deploy a vast array of desktop images. Virtual desktop snapshots (backups), management, and administration are conducted as part of an overall virtual infrastructure environment utilizing optimized toolsets for the tasks. A failed PC or laptop is no longer a crisis or even an inconvenience since a user can simply plug in another device and resume work. Remote clinics no longer require emergency visits to replace failed servers or tape backup units. The IT staff's ability to more effectively add hardware, troubleshoot remotely, and even budget is all significantly enhanced.
- **Improved Software License Compliance and Cost Control.** A VDI environment puts IT in control of all software since it all runs on the virtualization hosts. IT can easily track usage trends and help minimize licensing costs. More importantly, IT is now better able to both identify best practices in terms of optimal software as well as emphasize the elimination of redundant and overlapping software packages.
- **Superior User Support.** In most organizations, there are users who seem to have a dark cloud over them when it comes to PCs or laptops. Their power supplies burn out,

corrupting their desktops. They lose critical files, even though they're sure they've saved them. They inexplicably run slower or freeze up entirely every 3 or 4 weeks, but IT is never able to replicate the issues. These types of problems are dramatically reduced when an organization implements a cohesive virtual desktop strategy. The hardware-based challenges are eliminated and IT now has the ability to quickly monitor, test, replicate, and recover virtual desktops as needed.

- **Less Downtime.** User downtime is slashed in two ways. On the data center side, the virtual desktops now benefit from the same advantage that virtual servers have in very rapid recovery in the event of failure. As with servers, they can even utilize real-time clustering (using VMware Fault Tolerance) if needed. On the client side, downtime caused by hardware issues or incompatibilities is eliminated entirely while lock-ups due to DLL conflicts or malware are significantly reduced. Downtime is also no longer required for PC/laptop upgrades or refreshes.
- **User Device Proliferation.** Users are increasingly demanding effective utilization of non-traditional devices such as iPads, smart phones, and Android tablets. VDI enables IT to provide Windows 7 based desktops to these users, complete with all of the authentication, security, reliability, and management required as part of the organization's governance policies.

Improved Security of PHI

- **Enhanced Logical Security.** When users have access to their physical PCs or laptops, they are easily able to infect their devices with viruses, spyware, or other malware. The Advisory Board Company estimates the black market price for an Electronic Medical Record at \$50. Theft of patient data is on the rise. Combined with painful HIPAA Omnibus fines - of up to \$1,500,000 - and crippling damage to brand goodwill, mitigating data breaches is paramount in health care. VDI limits the ability of end users to modify devices and centralizes control to help prevent against network-based data breaches.
- **Enhanced Physical Security.** According to the [Fourth Annual Benchmark Study on Patient Privacy and Data Security](#) by Ponemon Institute, 38% of healthcare respondents reported that they had more than five PHI breaches in the last two years. Couple that fact with the Ponemon Institute estimates that the financial impact of breaches cost organizations \$2 million over the last two years. The numbers are staggering - costing US healthcare over \$5.6 billion annually. Security gaps with business associates and employee negligence are leading causes of PHI breach and lost or stolen edge devices accounted for 49% of incidents. Centralizing data in a VDI deployment removes secure information from employee or business associate endpoint devices and therefore, eliminates the need for purchasing and managing local firewalls and encryption software. Strategically implemented lost or stolen devices do not contain PHI in a VDI deployment and in the event of theft, VDI will increase the likelihood of determining a low probability of compromise.
- **Enhanced Regulatory Compliance.** The ability to monitor every virtual machine in a central location makes it easier to prevent patient privacy issues and to comply with regulations concerning PHI. Eliminating the always-on workstation, end users are required to provide credentials when accessing a workstation. Not only can access be restricted, but in a VDI deployment, desktop permissions can limit access to approved functionality only.
- **Improved Patching.** The ability to automatically and centrally patch monthly or weekly software updates enhances the capability to immediately and universally deploy at risk security updates. Compare VDI patching to the existing labor-intensive and incomplete

method of patching to hundreds if not thousands of physical end devices, and the cost and compliance savings are enormous. Even if achieving a high success rate with current deployment methods, the time and effort spent to guarantee and document compliance is a challenge not worth risking. VDI can centralize, standardize, and simplify patch application.

Reducing IT Costs with VDI and Nutanix

It has been a commonly accepted industry maxim that virtual desktops might improve management, enhance user productivity, facilitate BYOD, enable superior DR, and so on – but forget about saving money.

Virtualizing servers is fairly predictable for most organizations. IT can use various tools to gauge the number of likely candidates up front, and purchase the required infrastructure to enable an orderly transition to a virtualized environment. Users should, hopefully, not be impacted – other than by improved performance and less or eliminated downtime from server maintenance or failures.

Virtualizing desktops is far more challenging than virtualizing servers. Applications or usage patterns can easily change over time requiring unexpected resources. A health care VDI initiative typically includes hundreds or thousands of users – each with their own expectations, application requirements, and perceptions. Consider the workload generated by a standard clinical EMR user, versus a user in radiology processing advanced CT images. Every user and therefor every workload in a VDI deployment is unique.

Virtual desktops utilize write-heavy workloads with random storage I/O. This makes achieving consistent performance difficult: IOPS requirements can swing wildly depending upon usage patterns, time of day, and type of applications being accessed. Boot storms, anti-virus scans, and patch update cycles can all put sudden loads on the infrastructure and impact general performance.

Users tend to be adverse to change in even the best of cases. If their performance varies under VDI – even if only during occasional boot or write storms, they often become quite vocal and can slow or kill a virtual desktop initiative. Ironically, it is better to have consistently sub-par virtual desktop performance rather than randomly fluctuate between sub-par and good.

Other variables can also affect virtual acceptance. Many laptop users, for example, may be happy to exchange their devices for a virtual desktop that follows them around – particularly between offices or between their homes and offices. But other laptop users may require or simply demand a truly mobile device.

As a result of the uncertainty regarding both the ultimate VDI user population and performance requirements, health care institutions generally deploy a virtual desktop environment over a number of years, making adjustments as appropriate. IT commonly migrates users to virtual desktops during their normal PC or laptop refresh cycles by either locking down their devices to act like thin-client terminals, or replacing them with thin-client or zero-client devices.

Implementing virtual desktops over time for an ultimately unknown population does not mesh well with traditional storage infrastructures. Organizations face either purchasing storage arrays up-front with far more capacity than required, or risk forklift upgrades down the road. The initial capacity must be adequate to handle any future growth in the user population, new

applications or other unanticipated resource requirements, as well as spikes in intermittent resource utilization.

The Challenge with Traditional Storage

Most organizations, not unexpectedly, do a poor job of estimating their storage requirements up-front. A recent [Gartner study](#) of 19 organizations that deployed either VMware View or Citrix XenDesktop showed that 17 of the 19 spent more on storage than expected, and that storage, on average, accounted for 40% - 60% of the entire VDI budget. A Gartner analyst commented that the only reason two of the organizations managed to stay within their storage budget was that they purchased so much of it up-front.

High initial storage costs combined with the difficulty in forecasting the parameters of a VDI deployment in terms of users and resource requirements years down the road tends to create project inertia. Adding to the consternation is the obvious disadvantage of consuming the excess storage capacity at a future date when it will be markedly inferior in comparison to new technologies.

A virtual data center also changes the dynamics of the traditional stovepipe IT organizational model whereby the server, network, and storage teams can no longer work effectively in silos. VDI requires further collaboration with desktop and application teams. A 2011 [InfoWorld article](#) stated that IT collaboration was the #1 obstacle to VDI adoption.

Virtualization customers have demanded solutions that reduce management complexity, enhance collaboration, and help eliminate inevitable finger pointing from different manufacturers of storage and servers. The datacenter manufacturers have responded. All the leading players have a version of what they refer to as a “converged infrastructure” that combines compute, storage, and network resources either as products or as reference architectures.

But, calling these solutions “converged” is a misnomer. A better description would be “adjacent infrastructure” since the underlying compute and storage tiers must still be managed separately, and they still require an intermediate network to move data continuously between them. While these pre-packaged compute + storage solutions can substantially reduce the time required to implement the back-end VDI infrastructure, they can also exacerbate the difficulties organization face in moving ahead with VDI. Now IT must purchase not just the storage, but in some cases much of the server resources, upfront as well.

Enabling VDI ROI with Nutanix

Google pioneered the web-scale infrastructure in the cloud provider space, and it is now utilized by every leading cloud provider. Web-scale enables consolidation, linear scalability, fractional consumption, and an abstraction of the intelligence from traditional hardware arrays into software-defined storage. The compute and storage tiers combine into a single consolidated infrastructure.

Nutanix brought this model to the enterprise by leveraging the hypervisor to virtualize the storage controllers themselves. Since every server is a virtual storage controller, the crippling boot and write storms common with traditional storage arrays are eliminated. The local disk combined with integrated flash and auto-tiering of workloads provides for a consistent user experience and, consequently, much greater user acceptance of the virtual desktop environment.

The Nutanix Virtual Compute Platform installs in under an hour, and is managed by the virtualization administrators through the virtualization platform console, eliminating the requirement for storage and compute administration collaboration. Unlike traditional arrays, storage administrators do not continually field requests from the desktop team for more LUNs or IOPs.

Most importantly, Nutanix enables the VDI environment to expand one server at a time. The much lower initial investment enables a quick payback period. And, the overall spend is also reduced since Moore's Law ensures declining costs relative to VM density.

Utilizing Nutanix, health care institutions can inevitably fund their entire VDI projects, including infrastructure, licensing and services - with just their normal refresh budgets for PCs and laptops. In fact, they almost certainly will have plenty of budget left over.

The example below is based on one of Nutanix customers in the health care space, a California County that virtualized 2,560 PCs and laptops over five years at the rate of 606 virtual desktops created the first three years, and then 521 the last two years (to match the refresh rate of five years for PCs and three years for laptops).

Existing PCs and laptops are locked down as thin-clients, and kept for three years after their normal refresh cycle, then replaced with 22" LG integrated zero-client monitors. The LGs are purchased for new users. Microsoft SA costs \$50/user/year and VDA \$100/user/year.

Utilizing Nutanix rather than the conventional storage and converged infrastructure solutions provides a projected 5-year positive cash flow of \$247,902 vs. an initial investment of \$595,843 which equates to an ROI of 42% and a 10.9 month payback.

Including projected 5-year IT staff savings of \$2,372,348 from migrating to virtual desktops brings the ROI up to 298% and reduces the payback period to 9.6 months.

	Year 1	Year 2	Year 3	Year 4	Year 5	Totals
Scenario 1: Maintain existing PCs/Laptops. Scenario 2: VDI						
VDI Investment (= Year 1 CapEx)						
Nutanix, ViewPremier, AppSense, LG 22", & Services	(\$595,843)					
CapEx						
¹ Refreshed PCs/Laptops, New User DTs, DT Disposal	\$610,743	\$610,743	\$610,743	\$610,743	\$610,743	\$3,053,717
² Nutanix Cost, ViewPremier, LG 22", AppSense, Services	\$595,843	\$387,317	\$353,619	\$471,324	\$403,928	\$2,212,030
Net CapEx Cashflow	\$14,900	\$223,426	\$257,124	\$139,420	\$206,816	\$841,686
OpEx						
¹ Backup, AntiVirus, Encrypt, Microsoft SA, DT Pwr, VPN,	\$254,508	\$260,035	\$265,561	\$271,088	\$276,615	\$1,327,807
² Nutanix Mnt, ViewPrem Mnt, AppSense Mnt, MS SA, MS VDA, DT Pwr, VPN,	\$209,836	\$305,016	\$347,433	\$493,647	\$565,659	\$1,921,591
Net OpEx Cashflow	\$44,672	(\$44,981)	(\$81,872)	(\$222,560)	(\$289,045)	(\$593,785)
Total CapEx + OpEx Cash Flow	\$59,572	\$178,445	\$175,253	(\$83,140)	(\$82,229)	\$247,902

While each organization tends to have unique aspects of its environment to consider when evaluating projected cash flows from implementing VDI, some of the common ones are as follows:

PC Costs: PC costs are calculated both for expected new PC purchases each year as well as for expected upgrades to existing PCs. PC costs should reflect not only the cost of the units, but also the relevant associated costs including: tax, shipping, cabling, set-up, and

configuration. In the county health care example above, this cost was calculated at \$750.

Laptop Costs: Only the laptops that can be virtualized should be considered as part of the cash flow analysis. These include laptops that can effectively utilize off-line VDI, and those laptops that are given to employees to work between the home and office. In the later case, the laptops can often be eliminated and the employees instead given a virtual desktop that is easily accessible from wherever they can access a browser. As with PCs, laptop costs should incorporate all relevant tax, shipping, etc. as well as monitors and docking stations if applicable. The total cost in the example above was calculated at \$1,815, including monitor and docking station.

PC/Laptop Disposal Cost: The health care organization in the example above had \$100 disposal costs for disposing of old PCs and laptops including degaussing drives. This is fairly typical.

Client Devices: Under the virtualization scenario, costs are calculated for expected new devices for new users. Many organizations choose to purchase lower cost thin-client or zero-client devices which also require less power and support and in many cases can provide an improved user experience due to faster boot-up, less space requirements and no fan noise.

IT Staff Costs: There are associated IT staff costs with securing, managing, backing up, and supporting both physical desktops and their virtual equivalents. These include tasks such as help desk support, OS/application patching, desktop imaging/reimaging, user administration, hardware configuration, and application provisioning and upgrades. On the virtualization side, it also includes the appropriate increased cost, if any, for managing the virtual desktop infrastructure component of the private cloud. An [IDC study](#) states that it takes 12.2 hours, on average, to support a physical desktop per year and 5.2 hours to support a virtual desktop.

Remote Clinic Costs: In many cases under VDI, the physical servers and related network infrastructures can be eliminated from smaller remote offices and instead, the users run their desktops as virtual machines from the corporate data center. In these situations, the costs for the remote office servers, backup equipment, UPS, maintenance contracts, staff support, etc. can be calculated and contrasted with the reduced operating costs for consolidating the physical desktops to virtual machines in the data center. The county did not have any remote health care facilities.

Microsoft Licensing Costs: Under a virtualization scenario, there may be increased annual Microsoft licensing costs for Virtual Desktop Access (VDA) licenses if the organization does not purchase Microsoft Software Assurance (SA) or utilizes thin clients, zero clients, or other non-Windows devices. The organization in the example above utilized Microsoft SA. As it began replacing PCs/laptops with zero-client devices, the VDA license costs were accrued. Note that there now is a way around this licensing by using Windows Server Datacenter Edition to make the virtual desktops. In fact, under this scenario, licensing can even be lower than with PCs/laptops. The caveat is that all of the applications need to be Windows Server compatible.

Other Potential Cost Savings: While not part of the county's savings, organizations can also potentially benefit from the following areas:

- PC and laptop maintenance costs
- PC and laptop power costs
- The cost for maintaining and upgrading desktop management software
- Desktop backup software costs

- Encryption licensing costs
- VPN costs
- Office space costs saved from having more employees work from home

Investment Costs

On the investment side, common variables to consider include:

- Nutanix Virtual Compute Platform
- Virtualization licensing (server and client)
- Profile Management software licensing (if applicable)
- Thin or zero clients (if applicable)
- Professional services for VDI design and implementation

Why a Strategic Approach to VDI Is Imperative

Most health care organizations treat physical desktops as a silo with separate IT staff dedicated to platform management, administration, and maintenance. While the high costs of running a physical architecture make this stovetop approach pragmatic, it is no longer necessary when adopting a virtualized architecture. Virtual desktops become just another set of workloads running in the data center alongside the server VMs. They are administered with the same management console and benefit from the same virtual capabilities of snapshots, fault tolerance, DR, replication, etc.

Hospitals planning their VDI environments have an opportunity to incorporate virtual desktops as an integrated component of an overall virtualized data center. This strategic approach makes sense on many levels. A Bain & Company survey showed that hospital CIOs ranked IT interoperability as the most important strategic issue they face. Strategically virtualizing the desktops as part of the data center enables transformation into a private cloud with automated self-provisioning including metering, monitoring, and chargeback.

The increasing familiarity of IT staff with server virtualization frequently emboldens them with the confidence to deploy a VDI solution, applying to the desktop the lessons learned from their server virtualization efforts. This approach, though, inevitably leads to trouble when expanded to an enterprise initiative. Wildly varying usage patterns, for example, can quickly oversubscribe memory and disk IOPs - creating widespread havoc among users. Anti-virus scanning configured for a traditional physical environment can quickly bring VDI performance to its knees. Lack of consideration of more demanding network capabilities or differing security requirements can cause VDI to fail. And, disregard of the all-important user perceptions can torpedo what would otherwise have been a very promising virtual desktop deployment.

Desktop virtualization demands a strategic approach incorporating the prerequisite assessment, planning, pilots, and managed execution required for a successful enterprise project. Objectives, including projected costs and savings, should be identified prior to starting the design. The planning and proof-of-concept phases can then be initiated within the context of providing a virtual desktop architecture optimized to meet the organization's objectives.

A key objective for a VDI implementation should be to provide a very positive user experience from the first pilot all the way through the production roll-out. Carefully planned

deployments should generate a positive buzz among users, leading to an enthusiastic acceptance of virtual desktops.

The architecture requirements largely determine the VDI components, such as hypervisor platform, application virtualization, client devices, personalization capabilities, and multiple other considerations. While Nutanix is a solution for all virtual workloads, not just desktops – it is particularly remarkable in VDI in comparison to traditional servers and storage. Nutanix:

- Enables a consistent high-performance user experience by utilizing virtualized storage controllers and perfectly linear scalability.
- Enables a VDI project to get off the ground with a low cost initial pilot solution that can then be expanded one node at a time as warranted.
- Slashes the overall cost of the VDI project and incorporates advancements in flash, CPU, memory, and disk as the virtual desktop initiative rolls out.
- Eliminates the requirement for storage administration and for collaboration between compute/virtualization and storage teams.
- Dramatically simplifies the VDI infrastructure.
- Slashes datacenter requirements for space, power, and cooling.
- Dramatically reduces the risk of the VDI initiative.

Conclusion

The proliferation of PCs and laptops during the past 40 years has led to an extremely complex computing environment with disparate and often non-interoperable databases, software applications, and equipment. This complexity is increasing further as users demand access to their health care applications via iPads, smart phones, and Android based tablets from multiple locations. Black market demand for health records, and newly regulated security requirements demand renewed attention to securing vulnerable physical endpoint devices. VDI, when built upon the Nutanix architecture, can serve as a unifying platform that simplifies the environment, eliminates technology islands, and secures PHI all while reducing overall costs. The Nutanix VDI solution enables IT to ensure both enterprise-wide productivity and efficiency while providing users with a superior computing experience.