VDI: A SIMPLE IDEA SOLVING COMPLEX PROBLEMS

Lenovo Health

Meaningful Use, HIPAA, HITECH, value-based care, ACA — the list goes on and on. Regardless of whether it's a government regulation or market demand, the mandates on IT in healthcare organizations are at odds with each other: Deploy more advanced, usable, secure applications while also reducing IT infrastructure costs.

These priorities create a never-ending battle on the modern IT playing field, but healthcare IT leaders and technology providers have come together. Healthcare organizations are recognizing dramatic gains in three key areas of healthcare delivery by embracing the full potential of virtualization.

Every once in a while, the tech world develops an innovative technology representing a simple idea that solves some very complex problems while enabling whole new solutions. Virtual desktop infrastructure (VDI) is one of those technologies.

Virtual desktop infrastructure (VDI) is the technology and process for providing and managing user desktops inside a virtual machine hosted on a centralized server in the data center or in the cloud. Virtualized desktops are accessible by end users regardless of their device or location, yet remain secure because all computing activity related to the applications and data within the virtual desktop happens in the data center. IT administrators can reduce device management costs and enable mobile access while streamlining infrastructure and securing data.

VDI's central management, scale, and security have drawn the healthcare industry spotlight — a game-changing tool organizations deploy to help clinicians reach patient engagement goals. Healthcare organizations opting for virtual workspaces deliver a more efficient and cost-effective IT infrastructure. Clinicians are freed to deliver more focused care and increase patient satisfaction when they reduce the time spent logging in and out of systems. IT managers gain greater control over data, user access, and devices when desktops never leave the security of the data center.

intel

KILLING THREE BIRDS WITH ONE VIRTUALIZED STONE

According to a 2017 report by Login VSI, the number of IT professionals interested in or already using desktop as a service (DaaS) technology has increased from 18% to 55% over two years.[1] Other surveys indicate that healthcare, traditionally conservative in its technology adoption, has a VDI adoption rate rivaling early adopting industries such as financial services.[2]

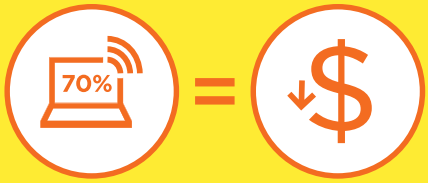
VDI is delivering dramatic impact in three of the biggest healthcare IT focus areas:

- **Protecting data across the organization.** When users' desktops are virtualized, sensitive patient, financial, and operational data and applications stay in the data center where they're safest. Centralized data management allows IT to streamline data backup and recovery and more effectively secure data from cyberthreats.
- **Streamlining clinical workflow.** Virtualized desktops, especially when combined with single sign-on (SSO) solutions, provide clinicians anywhere, anytime access to patient-critical data and applications. Instant accessibility via roaming-friendly desktops, mobile devices, and connected specialty devices delivers millions of dollars in measurable efficiencies while freeing up valuable time for clinicians to engage more effectively with patients.
- **Facilitating effective compliance.** VDI provides compliance-driven IT organizations with a platform for more effective user authentication, access, and authorization. It enables password management and authentication options that are inherently stronger. With data and access centralized in one place, compliance oversight and reporting become easier to maintain.

Is VDI the Proverbial "Killer App" for Healthcare?

This paper examines virtualization and its positive impact on data security, clinician productivity, and patient engagement. Killer app or not, it's hard to ignore the dramatic gains healthcare organizations recognize with VDI.

VDI is delivering benefits to IT that seemed unattainable without sacrificing quality of service and security. Gartner reports that with VDI, 70% of IT support for infrastructure services can be performed from a remote location, reducing labor costs by 10%–50%, resulting in a 3%–30% overall net savings (excluding one-time transition charges).[3]



PROTECT THE DATA BY REMOVING THE DATA

VDI Changes the Data Protection Game from Desktop to Data Center

While healthcare organizations might have different end goals or priorities for their VDI implementations to address, nearly every VDI solution is driven by one fundamental objective: greater data protection. The very act of centralizing data with a VDI solution creates a cascade of data protection and security gains that are neither subtle nor nuanced. They are, in fact, dramatic and game-changing.

Taking a step back, the impact of VDI shouldn't be so dramatic. Virtualization is not new technology. It's been around for a while. But when straightforward, no-nonsense solutions are applied to a high-cost, high-complexity, highly regulated environment like healthcare, these solutions have the potential to deliver impressive gains. VDI is doing that, creating a domino effect that addresses a host of perennial issues faced by IT administrators — the first being data security.

VDI-Enabled Data Security Starts at the Endpoint

VDI dramatically reduces the risk of intrusion and information theft by removing applications and data from network endpoints such as workstations, desktops, and mobile devices. There's no need to encrypt the endpoints because, simply put, there's no data there.

Sean Updegrove, associate vice president and chief technology officer of Children's Hospital Los Angeles, a 495-bed pediatric facility, described virtualized desktops simply in a March 2018 *HealthTech* interview: "The best part about it is the data doesn't ever leave my warehouse or my data center. We're just shooting screenshots, essentially, so nobody can intercept the traffic and know what's going on."[4]

Centralizing Data Minimizes Potential Data Loss and Disruption

When applications and data are not spread across the network, recovery of VDI systems from a disaster can be faster and more reliable. VDI environments still require a robust backup and recovery strategy, but the very nature of virtual desktop deployments — including those that allow virtual hard drives and other personalization — enables a smoother, even seamless recovery.

In fact, running virtual desktops is almost like having a secondary site available for your end users in the event of a full-scale disaster, which makes business continuity planning easier and offers a more sound solution than trying to recreate a site full of independent desktop PCs.[5]

VDI Deployment Best Practices at a Glance[6]

VDI solutions offer tremendous benefits to organizations in terms of manageability, performance, and security. However, there are key deployment best practices that should be considered. Here's a quick look at several VDI best practices to assess before, during, and after installation:

Understand end user requirements. Identify what types of end user applications are utilized in order to properly size the VDI solution. Take into consideration simple practical requirements such as monitor support, profile persistence, USB redirection, and peripheral device needs.

Design and size VDI networks and storage correctly. Be sure to assess desktop display/experience performance requirements when connecting from either high-speed LAN connections or slower WAN links. Incorporate hybrid all-flash SAN arrays, or other software-defined storage such as vSAN, to avoid VDI storage saturation and slow performance during I/O storms.

Explore persistent vs. non-persistent desktop provisioning. Persistent virtual desktops provide users a dedicated virtual desktop each time they log in, but they add management overhead and storage space requirements. With non-persistent desktops, admins set up a "pool" of generic desktops created from a "gold" virtual desktop image. Non-persistent desktops are more efficient from a storage perspective but add complexity to managing user profiles and data.

Decide which thin client management solution works best for you. End users still need a physical way to access their virtual desktops. Organizations can now deploy new, less expensive, more lightweight thin clients. These newer models support a stripped-down OS for more efficient use. Organizations that do not want to invest in new hardware can consider thin client software apps that turn an existing PC into a thin client — achieving a similar outcome.

Make VDI environments highly available. Unlike traditional client/server infrastructures, virtual desktops rely on the availability of the shared back-end VDI solution. Make sure your hypervisor and storage solution have enough hosts in the VDI cluster, redundant data paths to storage and network connections, and redundant power to alleviate concerns about availability.

Shielding Data from Cyberthreats

Always evolving — and never for the better — cybersecurity threats to healthcare providers are especially dangerous. Few are as potentially vicious as a ransomware attack on a healthcare organization. While paying millions of dollars in ransom is a significant event for any organization, an attack on a healthcare provider could quite literally mean life or death as critical patient data and systems become inaccessible.

In an interview with HITInfrastructure.com during the 2017 VMworld conference in Las Vegas, Nebraska Medicine Vice President of IT Brian Lancaster noted, "Healthcare is transforming, and the needs of healthcare infrastructure teams are transforming." He further stated, "The industry's rapid digitization is outpacing security controls. Healthcare providers are also becoming a larger target due to the premium people can get for PHI on the dark web. It's a perfect storm."[7]

In addition to other security measures, VDI is a particularly effective cybersecurity tool. For example, lost or stolen devices pose a far smaller risk of a security breach since there is no data stored on the device.[8] By significantly reducing the attack surface, VDI simplifies downstream security management. Critical data resides in the cloud while preserving a rich app experience for device users.

CLINICAL WORKFLOW WITH NO BARRIERS — OR DATA

VDI Drives Improved Clinician Productivity and Patient Engagement

The IT-centric benefits of VDI alone don't explain the widespread acceptance of desktop virtualization. For that, you need to look at the benefits that extend beyond the IT organization to the end users — the clinicians — and their patients.

Clinical workflows are very fluid. They call for flexible IT systems that support, rather than hinder, a clinician's dynamic responsibilities. Unfortunately, standard desktop environments tend to be a hindrance because they lock user information to a single location. Watch a hospital or clinic floor for a few minutes, and you realize the users aren't fixed to a single location — nor are the patients.

To support end users, IT has one of two choices in this environment: (1) invest an extraordinary amount of time and money to create and support robust, custom PC-based user applications, or (2) centralize the applications, customize or configure them in one location, and make them ubiquitously accessible throughout the enterprise. Healthcare organizations are choosing the latter — and with impressive results.

Anywhere, Anytime Access to Clinical Applications

The impact of a secure, convenient, frictionless log-in/log-out process shouldn't be underestimated. With the power of VDI and SSO working together, clinicians are truly enabled to seamlessly move to and from any station across the connected enterprise, picking up their desktop session where they left off — anytime, anyplace — as they move through their workday.

Personalized desktops and applications retain their state even as physicians and nurses change locations and devices. Envision a doctor walking into a patient room and a shared terminal quickly transforming into a tailored desktop. A badge tap or finger swipe log-in renders familiar apps and information relevant to the patient engagement. When the physician walks away, the computer locks itself.

If work continues into the next day, as it often does, all settings are carried over from one day to the next, so critical settings are not lost when users leave for the day.

Increased User Satisfaction with EMRs/EHRs

Management of clinician turnover (especially among nurses) is an ongoing challenge for many hospital systems. Improvement in these clinicians' satisfaction with the hospital work environment and clinical workflow enhances the organization's retention efforts and reduces costs associated with high turnover.[9]

Organizations deploying VDI report increased clinician satisfaction.[10] The combination of VDI and SSO brings flexibility, security, and "flow" to patient engagement. Clinicians can focus their attention on patients as barriers to engagement fade. VDI-enabled workflows offer both incremental real and meaningful liberation of clinician time and improvement in patient engagement.

More and Better Time with Patients

Making technology accessible is key, but VDI provides an even more effective, more immediate benefit that drives better patient outcomes and satisfaction: the gift of time.

In a recent survey of healthcare professionals conducted by the *New England Journal of Medicine,* 59% of respondents said that increasing time with patients was the best patient engagement strategy among options ranging from shared decision making to mobile healthcare tools.[11]

Time wasted logging in and out of applications could be better spent interacting with patients or responding more quickly to patients in need of immediate care. By implementing VDI, clinicians and IT administrators dramatically reduce time spent logging in or monitoring systems, devices, and applications; they increase their attention to patient interaction.

Case Study: Follow-Me Clinical Desktops for Nurses[12]

The nurses at Metro Health of Grand Rapids and Western Michigan are very mobile. They use a variety of endpoints ranging from desktops in staff rooms and workstations-on-wheels (WOW) to laptops and tablets carried to patient rooms. In a typical 10-hour shift, a nurse needs to access an endpoint at least 50 times. Each secure log-in can take up to three minutes.

With VDI, each nurse connects to their "session," which maintains its state as the user moves from endpoint to endpoint. Nurses can log into any endpoint at any location and instantly resume their session. This "always live" workflow delivers significant productivity improvements. The new VDI-enabled workflow reduced log-in times by 50% and increased nurse productivity over 30%.

The One-Two Punch of VDI and SSO Saves Thousands of Hours and Millions of Dollars[13,14]

- **Christus Health** reported 26,301 hours and $1.6 million in projected savings per year across its facilities.
- **Metro Health** has saved $10–$15 million annually by having clinicians spend more time at patient bedsides than logging into systems and working at conventional PCs.
- **Johns Hopkins** rolled out SSO to 34,700 users and reported a total time savings of 2,550 man-hours in the first month.
- **South Shore Health** deployed VDI and SSO with badge access and realized an overall savings of 583 hours per day, $5.69 million in annual benefit, and 695% annual ROI.
- **Kootenai Health** saved each nurse 27 minutes per day and each physician 10 minutes per day, equating to a cost savings of $7 million over five years.

A REMEDY FOR COMPLIANCE

Centralizing Data and Access for Better IT Oversight

Convenient, secure access enables doctors and nurses to spend less time looking for the information they need and more time caring for patients, but VDI's benefits help healthcare organizations achieve another important outcome: **compliance and control.**

Compliance and control have become even more important as electronic health records (EHRs) become the norm and anywhere, anytime access grows in importance. But the risks couldn't be higher, given the fact that healthcare providers — subject to HIPAA regulations — can incur staggering fines of up to $1.5 million per year per violation.[15]

The good news is that, when paired with complementary technologies such as SSO, VDI offers cost-effective ways for healthcare companies to be compliant and maintain data controls while expanding and improving access to EHRs and other healthcare data.

VDI-Enabled Authentication and Access

When protected data and applications are in one place, analysis, identification, and implementation solutions designed to meet regulatory compliance mandates (e.g., HIPAA, HITECH) become easier to manage and maintain.

For example, when a VDI solution is paired with added security safeguards like two-factor authentication and full-disk encryption on both the server side and the backup storage side, organizations gain a HIPAA-compliant solution. User desktops can be easily accessed without exposing protected health information to unauthorized users. Administrators can create and enforce a single set of access control policies for all users, regardless of endpoint location or device used.[16]

SNHH Desktop Configuration Engineer Scot Tymowicz told HITInfrastructure.com in a July 2018 interview that virtualization assists healthcare organizations in reaching and maintaining HIPAA compliance. "As HIPAA compliance and medical regulations become more complex, IT's job is to make sure that the environment is secure. IT can't do that if nurses are putting sticky notes with their son's birthday on it as their password right on the computer — that's not a secure environment."

Tymowicz continued, "What is a secure environment is IT enforcing a 10- or 20-character alphanumeric password with dollar signs and periods and numbers that staff never have to type, because all they have to do is wave their badge. We have a highly secure environment, but it's extremely easy and seamless for the end users. It's a win-win for everyone."[17]

Compliance and Controls that Can Be Proven

Auditing and reporting are key components of compliance — ensuring that data and systems are secure with regular reviews of access and activity. VDI-enabled centralization of data and access streamlines audits and regulatory compliance. VDI makes access investigation simple, helping investigators determine who accessed what applications and data and rapidly identify security threats. There is no need to collect extensive logs from remote devices and users because virtualized desktops, applications, and associated data are secure within the data center and protected through standards-based encryption, secure remote access, event logging, and multi-factor authentication.[18]

But the security and compliance challenges facing healthcare IT departments extend well beyond HIPAA, HITECH, and protecting data. As technology continues to shape the care delivery landscape, IT leaders will evaluate tools designed to enhance productivity, promote patient safety, and improve care outcomes. VDI offers a cost-effective and compliant way to meet many of today's regulatory requirements while providing greater access and confident data control.

VDI STRIKES THE BALANCE

The stakeholders in the healthcare industry — patients, physicians, payors, administrators, and even politicians — have a lot to gain and a lot to lose. Increasingly, VDI-driven solutions are helping the industry strike the right balance between innovation and security. More secure yet easier-to-access desktops are increasing clinician efficiency. In turn, clinicians can spend more time with patients, who are more engaged because of easier access to healthcare apps and tools. It appears that VDI is indeed the technology strategy helping healthcare providers kill two, three — maybe more — birds with one virtualized stone.

Lenovo Health

Citations

[1]Spruijt, Ruben, and Plettenberg, Mark. "State of the VDI and SBC union 2017." Login VSI, June 2017. Last referenced: January 2019. https://info.loginvsi.com/acton/attachment/25205/f-0121/1/-/-/-/-/State%20of%20the%20VDI%20and%20SBC%20Survey%202017%20Edition%20v2.1.pdf?sid=TV2:g4MGwTlJe

[2]"Virtual desktops in hospitals: Streamlining clinical workflows." Citrix Systems, Inc., 2015. Last referenced: January 2019. https://citrixready.citrix.com/content/dam/ready/assets/healthcare/virtual-desktops-in-hospitals-streamlining-clinical-workflows.pdf

[3]Angwin, David. "VDI: The sensible option for addressing healthcare IT challenges in Europe." *Building Better Healthcare.* 11 January 2016. Last referenced January 2019. https://www.buildingbetterhealthcare.co.uk/news/article_page/VDI_the_sensible_option_for_addressing_healthcare_IT_challenges_in_Europe/114449

[4]Van Wagenen, Juliet, and Bowman, Dan. "How USC's Keck Medicine Taps the Benefits of VDI to Increase Security and Accessibility." *HealthTech* Magazine. 14 March 2018. Last referenced: https://healthtechmagazine.net/article/2018/03/uscs-keck-medicine-taps-vdi-boost-security-accessibility

[5]McKeon, Scott D. "How VDI Can Improve Your Cloud Solutions." TBConsulting blog. 16 August 2016. https://www.tbconsulting.com/how-vdi-can-improve-your-cloud-solutions

[6]Lee, Brandon. "VDI deployment best practices: A guide." Cloudtech. 09 May 2018. https://www.cloudcomputing-news.net/news/2018/may/09/vdi-deployment-best-practices-guide/

[7]"Why Cloud, Virtualization Are Key to Healthcare Infrastructure Strategy." HITinfrastructure.com. Last referenced 30 March 2019: https://hitinfrastructure.com/features/why-cloud-virtualization-are-key-to-healthcare-infrastructure-strategy

[8]Hickman, Mark. "Security meets flexibility: A checklist for virtual desktop infrastructure." BAI. 01 August 2018. https://www.bai.org/banking-strategies/article-detail/security-meets-flexibility-a-checklist-for-virtual-desktop-infrastructure

[9]Gellert, George A. et al. "Clinical impact and value of workstation single sign-on." *International Journal of Medical Informatics.* Volume 101 May 2017: Pages 131 - 136. Last referenced: https://doi.org/10.1016/j.ijmedinf.2017.02.008

[10]Kelly, Dr. Sean. "Healthcare organizations report thousands of hours and millions of dollars saved with SSO and VDI." Imprivata, Inc. 29 March 2017. Last referenced: https://www.imprivata.com/blog/healthcare-organizations-report-thousands-hours-and-millions-dollars-saved-sso-and-vdi

[11]Volpp, Kevin G. and Mohta, Namita Seth. "Patient Engagement Survey: Improved Engagement Leads to Better Outcomes, but Better Tools Are Needed." *New England Journal of Medicine Catalyst.* 12 May 2016. Last referenced: https://catalyst.nejm.org/patient-engagement-report-improved-engagement-leads-better-outcomes-better-tools-needed/

[12]"Optimizing Clinical Workflows with VMware View and Cisco VXI." VMware, Inc. white paper. 2011. Last referenced: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/partners/cisco/cisco-vmware-optimizing-clinical-workflows-with-vmware-view-and-cisco-vxi-white-paper.pdf

[13]Kelly, Dr. Sean. "Healthcare organizations report thousands of hours and millions of dollars saved with SSO and VDI." Imprivata, Inc. 29 March 2017. Last referenced: https://www.imprivata.com/blog/healthcare-organizations-report-thousands-hours-and-millions-dollars-saved-sso-and-vdi

[14]"T2 Tech Group Continues Successful Rollout of VDI and SSO at Kootenai Health." T2 Tech Group, Inc. 6 July 2018. Last referenced: https://www.t2techgroup.com/vdi-sso-roll-improves-clinical-workflows/

[15]"Yes, VDI Is Enhancing Healthcare Delivery While Protecting Patient Data." VDIworks. 14 October 2015. http://www.vdiworks.com/yes-vdi-is-enhancing-healthcare-delivery-while-protecting-patient-data/

[16]"VDI Offers Healthcare Organizations Access and Compliance." Informa: *ITProToday.* 27 April 2016. https://www.itprotoday.com/business-resources/vdi-offers-healthcare-organizations-access-and-compliance

[17]O'Dowd, Elizabeth. "Using Virtual Desktop Infrastructure in a Healthcare Setting." HITinfrastructure.com. 11 July 2018. https://hitinfrastructure.com/news/using-virtual-desktop-infrastructure-in-a-healthcare-setting

[18]"Innovations for Security and Compliance in Healthcare." Citrix Systems. 2017. https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/security-and-compliance-in-the-mobility-transformed-healthcare-organization.pdf

About Lenovo Health

Lenovo is a trusted provider of healthcare technology with a 20+ year history of world-class innovation, industry leading partnerships, and more than a decade of proven healthcare experience. Lenovo Health powers tailored care delivery in 160 countries and 1,600 healthcare organizations worldwide.

Lenovo Health's vast portfolio supports the administrative, clinical, and remote care needs of healthcare facilities with cloud, security, and mobility solutions and accessories that streamline workflow and bring data closer to the patient and clinician. Learn more about Lenovo Health: www.Lenovo.com/Health