

Benefits of Intelligent Desktop Virtualization for the Healthcare Enterprise

A Flexible New Solution for Improving Productivity, Manageability, and Security



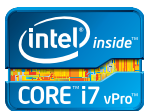
NEW CLIENT-SIDE SOLUTIONS FOR DESKTOP VIRTUALIZATION OFFER:

- Centralized management capability
- Lower costs because client images are managed centrally on a server
- Protection of sensitive health information through centralized management of security policies
- Improved user experience due to multimedia redirection and local execution of applications

Value for Health IT and Improved Productivity for Employees

The healthcare industry is in the midst of a transformative change. Emerging reform initiatives that focus on improving the overall health of patient populations tie provider reimbursements to measurable quality metrics rather than traditional fee-for-service. Regulations such as HITECH are intended to improve the quality of care while reducing cost by accelerating the adoption of Health-IT, such as electronic health records (EHRs). However, adoption alone is not sufficient. It is the intelligent application of Health-IT across the care continuum that will lead to success in this new environment. Meaningful, collaborative exchange of health information between patients, primary care physicians, specialists, hospitals, long-term care facilities, and family members is required to enable improved accuracy and timely decisions at the point of care.

Under significant pressure to bring the spiraling cost of care under control, IT departments are being asked to do more with less. Having realized significant benefits with server virtualization in the data center, many organizations are now turning to desktop virtualization to enable centralized management and security of applications and support of new devices such as smart phones and tablets. However, traditional desktop virtualization solutions require increased data center infrastructure and do not always provide an acceptable user experience. As new enabling technologies emerge for client compute delivery, IT must determine the optimal enterprise client computing strategy—deciding which combination of client platforms and service delivery models will best meet the needs of employees and the IT organization, now and into the future. Adoption of virtualization for client computing is increasing because it has many compelling benefits. New client-side



virtualization solutions running on devices with the 2nd generation Intel® Core™ vPro™ processor family promise to meet the needs of both Health-IT administrators and users. These solutions give IT an efficient, cost-effective, and more secure way to centrally manage client devices. They also deliver local performance and compute capabilities that enable healthcare workers to interact with a broad range of peripherals, draw on a growing set of rich imaging capabilities, and make use of real-time collaboration tools required for emerging workflows for care coordination.

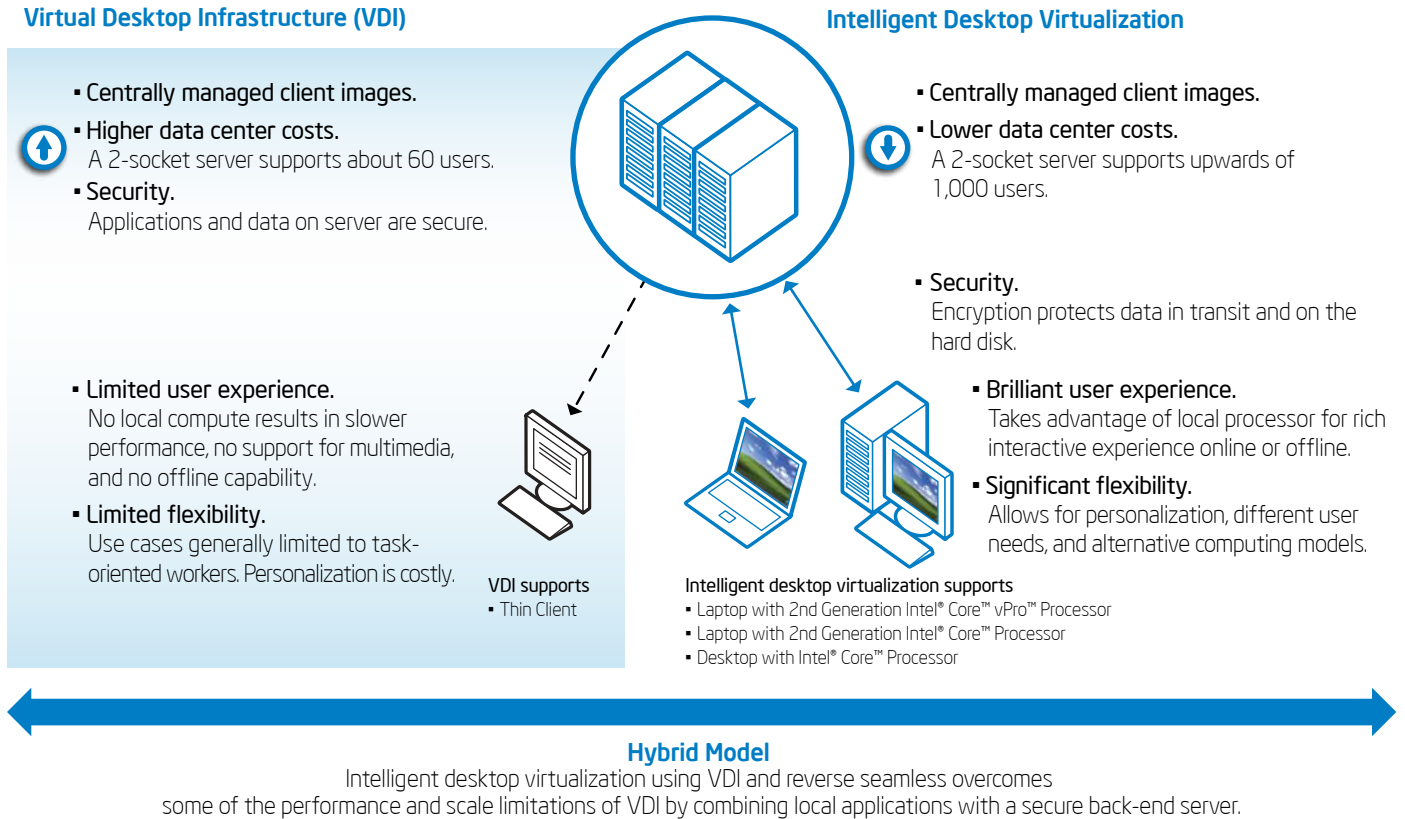
Client Computing Virtualization Models

All client virtualization models abstract and separate the computing elements—OS, applications, user profile, and data—from each other and from the underlying hardware. This helps make the clinical workspace and data more accessible and portable. The main distinction between the different models lies in where the virtualization occurs: either centralized in the data center or distributed to the endpoints. While virtualization promises a higher degree of control over application management and data, and potentially can lower IT costs, which model is the best option for users and for IT departments?

Server-hosted Virtual Desktop Infrastructure and Thin Clients

Significant interest in client virtualization has centered on server-hosted virtual desktop infrastructure (VDI) and thin-client computing (Figure 1). This model is used to host multiple, unique client images, or virtual machines (VMs), on a single server or group of servers managed by a server-side hypervisor. Because the computing occurs in the data center, healthcare professionals can access their applications and data securely through a variety of devices, including PCs, smart phones, tablets, and thin-client terminals.

Figure 1. Comparison of Server-hosted Virtual Desktop Infrastructure (VDI) and Client-side Virtualization



Healthcare IT departments often find thin-client solutions attractive due to perceived cost savings and improved protection of sensitive information as compared to traditional management of an intelligent PC fleet. This can be a misconception, however: As workflows become media rich—supporting medical imaging, patient education, and collaboration—thin clients can place a heavy burden on IT infrastructure, overloading the network and servers in already density-constrained data centers.

VDI provides a means to access basic information, including calendar, e-mail, patient record information, and an occasional medical image, from client devices such as smart phones or tablets. However, the user experience of VDI for use cases that require multimedia performance or real-time collaboration tools can be inconsistent or nonfunctional. In addition, many employees require specialized applications that run best locally and typically wouldn't be included in a standard software image build. This level of flexibility is not possible on a thin client.

Intelligent Desktop Virtualization Solutions Benefit Both IT and Users

Intelligent desktop virtualization technologies enable compute models that don't compromise the performance and mobility that users expect; in addition, they offer many of the same benefits that IT departments find attractive by extending traditional VDI. These solutions use the client-side processor and compute capabilities as needed to run CPU-intensive and rich multimedia applications for a great user experience. For example, with local processing capability, intelligent desktop virtualization can support voice and video applications such as Microsoft Lync Server*.

New Techniques Enhance Server-hosted Virtual Desktops with Local Applications

Multimedia redirection (MMR) technology enables media files to be delivered directly to the client device for local rendering. MMR technology offloads computing from back-end servers to reduce cost and improve the user experience. Major desktop virtualization providers support this technique

for compatible client devices, which currently include endpoint clients based on the MPEG media format for Microsoft Windows*. Figure 2 illustrates a new technique called reverse seamless technology that enables local client-side applications to run within a central server-hosted desktop environment. This solution uses the local processor and compute capabilities in the client PC to run CPU-intensive and rich multimedia applications for a great user experience while maintaining central management and storage of sensitive data. For example, with these technologies IT can support seamless integration of imaging, voice and video collaboration, and centralized access to patient records. This offloads compute cycles from the server while maintaining control of sensitive data. Figure 3 illustrates the server utilization of a production server with and without this technology. Without reverse seamless with MMR, server CPU utilization increases as additional user VMs with media are added. In this example, the sixth incremental media-based VM session added drives server utilization above 70 percent, the point at which user experience

Figure 2. Collaborative Workflows with Client-side and Reverse Seamless Virtual Desktop Infrastructure (VDI)

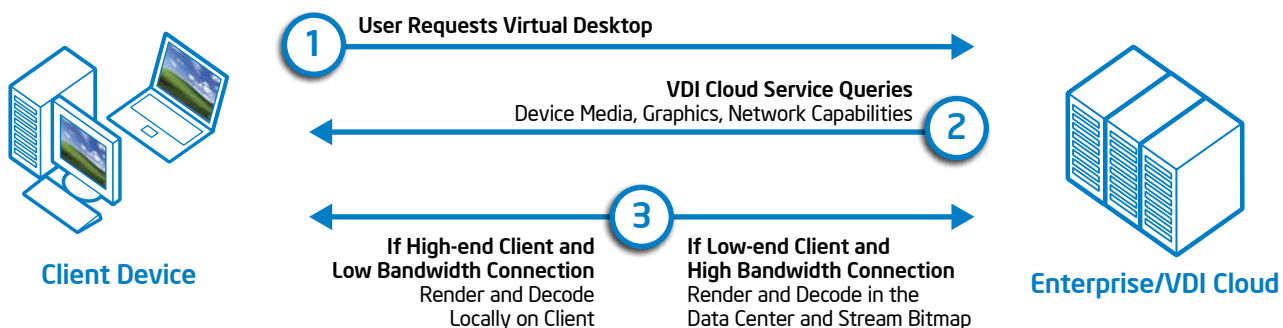
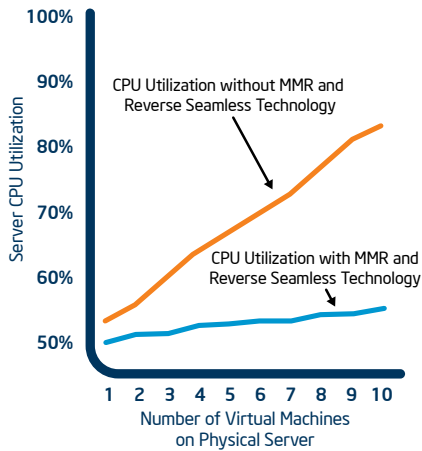


Figure 3. Server Utilization of Virtual Desktop Infrastructure (VDI) Before and After Reverse Seamless Enhanced Redirection Technique



Source: Intel internal test: Citrix XenDesktop 5.0* on server based on Intel® Xeon® processor 5600 series, 96 GB RAM. Base condition of user VM loading at 50 percent server CPU utilization before and after adding 1 to 10 addition VM sessions with Multimedia Redirection (MMR) and reverse seamless.

“The overall cost of a rich-client solution is less expensive than a thin-client solution due to the increased processing in the backend/server-side associated with thin-client deployments.”

– Dr. Peter Krcho
Head of the Neonatal Clinic, Perinatal Center, Neonatal Clinic LF UPJS and DFN Kosice Slovakia

begins to degrade significantly. With reverse seamless, 10 additional VM sessions can be added with less than a 5 percent increase in server utilization.

As collaborative care models continue to proliferate across the healthcare industry, the need to support real-time collaboration applications such as these will increase. VDI on thin clients cannot support these types of applications. However, combining VDI with technologies such as reverse seamless offers IT organizations significant benefits, including centralized manageability, security, and reduced operating costs.

Centralized Management

Like traditional VDI, intelligent desktop virtualization solutions offer efficient management and control of corporate data and applications because corporate images are managed centrally on a server. One class of intelligent desktop virtualization solutions is called virtual containers. In this model, client systems running a hypervisor download these images and run them locally. Products such as Citrix XenClient*, Microsoft Med-V*, Microsoft Virtual PC*, MokaFive Suite*, RingCube vDesk*, Virtual Computer*, and Wanova Mirage* offer fully managed virtualized client solutions with a variety of features to simplify and automate image management.

Although virtual container and reverse seamless features differ, these solutions can be managed separately or combined to help IT administrators manage the VMs deployed throughout the enterprise with a central management server and console. IT can update the centrally stored image and push changes out to users to improve the process for software updates, OS patches, and troubleshooting issues. Any changes to the virtual image are kept separate from the user’s personal environment, which means that users can customize their environments without affecting corporate applications or data. In addition, these solutions offer de-

duplication capabilities that eliminate duplicate copies of common files, reducing the need for expensive SAN storage build-out.

IT managers can control the entire VM life cycle remotely, including setting up images on the server for endpoints to download and enforcing usage policies to secure VMs and data. IT administrators can also control VM sessions, including starting, stopping, and locking the VMs, and remotely monitoring clients and troubleshooting issues.

Some intelligent desktop virtualization solutions offer users an automated option to roll back to a previous workspace image if a corruption occurs—reducing calls to the help desk, IT costs, and employee frustration and downtime.

Protection For Data and The Clinical Environment

Intelligent desktop virtualization solutions offer numerous ways to protect VMs as well as data—which may include protected health information (PHI). The central management consoles for these solutions provide the ability to lock down and secure the environment. Data security can be further enhanced with the use of McAfee Data Loss Prevention*, with passive and active enforcement of policies for data at rest, in transit, and in use.

IT administrators can set up authentication and security policies that control access to the VMs and reduce data compromise. For example, policies could be set up to deny a user access to the VM if an incorrect password is entered more than three times, to lock a VM after a predefined idle period, or to set an expiration date for the VM—which could be helpful in managing VMs for contract workers or disconnecting a device that has been stolen. Policies can flag or prevent the transmission of sensitive data or prevent unauthorized access.

For solutions such as VDI enhanced with reverse seamless technology, sensitive information such as PHI typically resides in a central repository in the back-end server

infrastructure. If a client device is lost or stolen, information in this central repository remains protected.

For solutions that distribute VMs to client devices, such as virtual containers, data can be encrypted for protection. Intel® Advanced Encryption Standard - New Instructions (Intel® AES-NI)¹ can help accelerate encryption performance by 3x to 10x over a complete software implementation. Intel® Identity Protection Technology (Intel® IPT)² provides one of the strongest techniques for avoiding the possibility of sensitive data ending up on an unauthorized client. See the sidebar for more details on how Intel IPT strengthens security. IT managers can also set the policy that controls which users are allowed access to the VMs while disconnected from the server, and offline work permissions could be limited to a predefined period of time, after which the VM is disabled until the user reconnects to the management server and re-authenticates. Every time a client system connects to the server, the management server can push out the most recent policies, settings, and patches so that the endpoint is using the most updated, secure workspace.

Furthermore, there are solutions for endpoint security that can be used in combination with encryption, such as Intel® Anti-Theft Technology,³ that not only mitigate the risk of exposing sensitive information but render the client device unusable until it is unlocked by an IT administrator.

Improving Total Cost of Ownership and Flexibility

Intelligent desktop virtualization offers a compelling value compared to traditional VDI. While the cost of thin-client devices is marginally lower than the cost of intelligent PCs, the licensing and infrastructure costs of deploying thin-client computing models and VDI can be complex and expensive, involving

the purchase of servers, software licensing, network upgrades, and SAN storage.

The thin-client approach comes with capacity limits and requires building up data centers and infrastructure to address peak capacity. Because intelligent desktop virtualization solutions take advantage of the client device's CPU to execute applications locally, new users can be added with little impact to data center and infrastructure, providing an inherently flexible and cost-effective solution. Dr. Peter Krcho, Head of the Neonatal Clinic, Perinatal Center, Neonatal Clinic LF UPJS and DFN Kosice Slovakia, reinforces this sentiment: "The overall cost of a rich-client solution is less expensive than a thin-client solution due to the increased processing in the backend/server-side associated with thin-client deployments."

In addition, Intel Ultrabook™ devices and other devices based on 2nd generation Intel® Core™ vPro™ processors are becoming more energy efficient with every new generation, and intelligent desktop virtualization allows employees to use a single device for multiple purposes to preserve the IT investment while potentially reducing hardware and energy costs.

A TCO study sponsored by Microsoft, involving research on more than 100 organizations with 500 or more traditional VDI desktops, found that for office workers in a VDI environment, the TCO was higher than that of a well-managed PC environment by up to 11 percent per user.⁴ While VDI reduced hardware and service desk costs, new software and engineering costs offset those savings, actually increasing overall costs. VDI redistributes IT labor costs, but total labor costs are almost identical in the PC environment.

In addition, in its TCO model, MokaFive claims its client virtualization solution can reduce IT costs by at least 45 percent compared to traditional management of a PC fleet. According to its model, the savings are delivered in three areas: operational cost, help desk cost, and capital cost.⁵

PROTECTING HEALTH INFORMATION WITH INTEL® TECHNOLOGIES

Intel® Identity Protection Technology (Intel® IPT)² provides one of the strongest techniques for avoiding the possibility of sensitive data ending up on an unauthorized client. Built into Intel Ultrabook™ devices and select 2nd generation Intel® Core™ vPro™ processor-based PCs, Intel IPT helps keep your data safe through a tamper-resistant hardware authentication mechanism. Intel IPT is a built-in hardware token (from your security supplier of choice) that eliminates the need for a separate physical token, thus simplifying the two-factor login process, and, most importantly, helping to ensure that the clients accessing your system are those assigned to authorized clinicians. This easy-to-use, two-factor authentication solution is available from a variety of OEMs and security ISVs. To further protect data and the environment, Intel IPT employs encryption, such as an encrypted connection back to the server to protect data in transit and encryption of the whole hard drive or the segment that contains the VM to protect data at rest.

According to guidance provided by the Department of Health & Human Services in association with the HITECH Breach Notification Rule, encryption is an acceptable method for rendering protected health information (PHI) "unusable, unreadable or indecipherable to unauthorized individuals."

COLLABORATIVE WORKFLOWS IN 21ST CENTURY HEALTHCARE

Improving collaboration for teams of clinicians delivering care can improve workflows within the hospital as well as during care transitions such as discharges. We describe two possible scenarios.

In a typical hospital-based scenario, if a surgeon needs a medical consult, it can often take hours. With secure mobile collaboration tools, a surgeon at a patient bedside could initiate a real-time multimedia video conference with one or more on-call consultants. If they could chat and review data from multiple sources—electronic medical records, picture archiving and communications system (PACS), DICOM viewer, and telemetry/monitoring equipment—they could determine a treatment plan

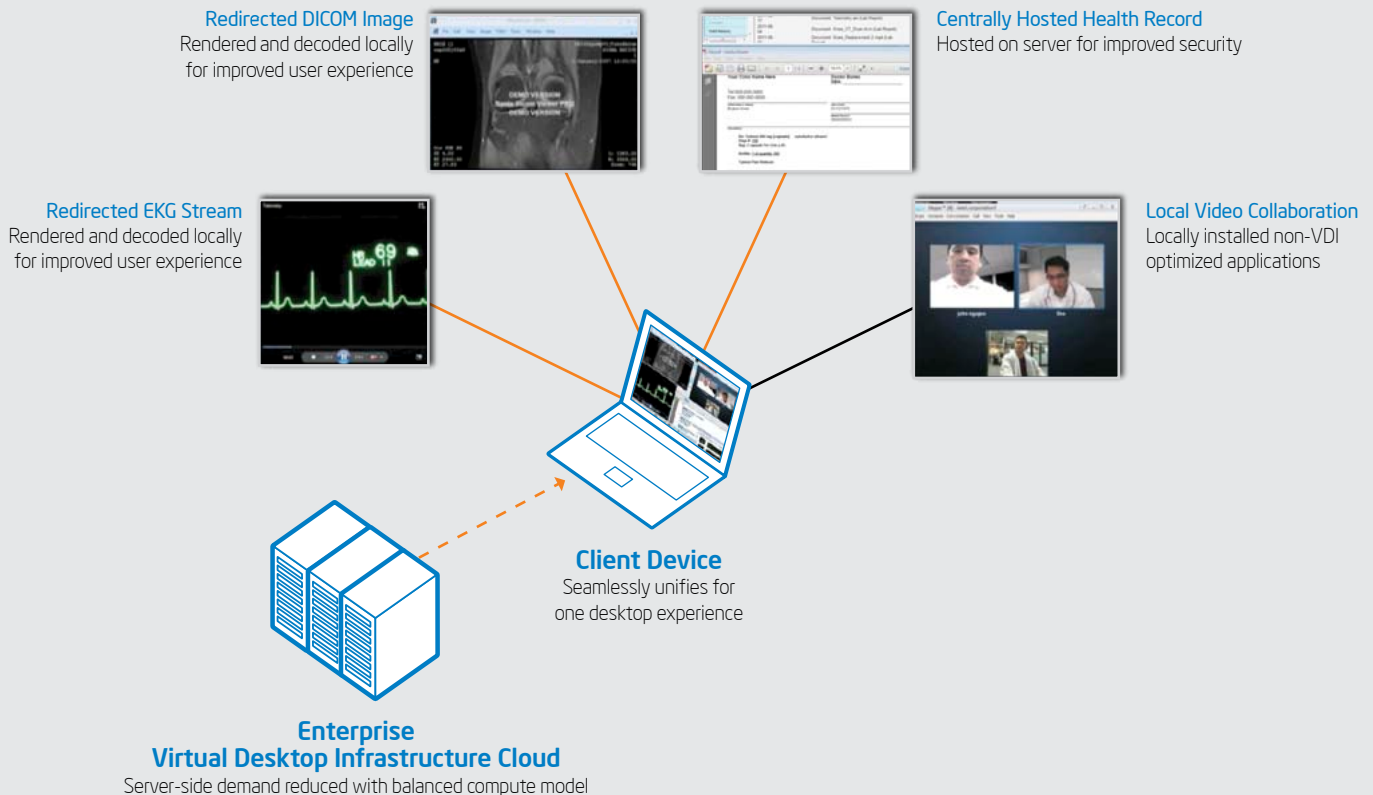
in minutes as opposed to hours. A workflow that enables speedier quality consults makes business sense whether organizations are paid a fee for service or global capitation.

Another area where collaboration tools could improve results is at the time of discharge. In the United States, the current 30-day re-admission rate for Medicare patients is greater than 20 percent. If the discharge nurse could communicate in real time with a nurse in the receiving facility—such as a doctor’s office or long-term care or rehabilitation facility—to review medication lists, discharge summaries, and care instructions, it would lead to an improved re-admission rate outcome.

If family caregivers also participated in the real-time discharge conference, improved patient satisfaction and follow up planning would be easier.

These are just two examples of how real-time collaborative workflows could significantly improve patient care. To enable such collaboration, we need secure mobile tools that can handle video streams from multiple sources. Devices should also deliver a satisfactory user experience given both CPU and bandwidth parameters. The software delivery method should balance the computing burden between the client and the server so as not overwhelm server capacity. (Figure 4.)

Figure 4. Use of Intelligent Desktop Virtualization for Collaborative Healthcare Workflows



Cost of each model may vary widely, and it is important to assess the complete costs of the capital, operational, and associated productivity benefits associated with each. Productivity benefits are often overlooked, but should be a critical part of any IT compute model decision.

Improving the User Experience and Productivity Through Collaborative Workflows

For many healthcare workflows, the user experience delivered by traditional VDI is far from optimal. Users often experience slower performance due to network latency and bandwidth, and thin clients don't support standard multimedia experiences, applications that require local execution, offline operation, or a host of peripherals commonly used in the healthcare industry. While thin clients are acceptable for some applications, their limited flexibility doesn't work well for many emerging healthcare usage models.

With intelligent desktop virtualization, healthcare organizations can realize all the performance benefits offered by using the capability of PCs, including the new multi-core

processing power and integrated high-definition graphics processing available on Intel Ultrabook devices and PCs based on the 2nd generation Intel Core vPro processors (Table 1). IT can give users the client-side performance they need for multi-threaded applications such as Microsoft Media-Player*, Microsoft Internet Explorer*, real-time collaboration tools, and other compute-intensive software, while still achieving robust security. The user experience is intelligently upgraded as compared to a thin-client experience, especially when the solution makes use of the new Intel® HD Graphics capabilities available on these processors.



Several intelligent desktop virtualization solution providers are taking advantage of Intel® Virtualization Technology⁶ (Intel® VT), hardware enhancements built into the 2nd generation Intel Core vPro processors. Intel VT shifts much of the burden of software-based virtualization into the hardware, and thus simplifies and reduces the overhead of virtualization, making it easier for third-party suppliers to build lightweight hypervisors. It also helps make virtualization more efficient

and secure in general, and significantly improves performance—to near-native levels, depending on the virtualization solution used.

Conclusion

Intelligent desktop virtualization running on devices based on the 2nd generation Intel Core vPro processor family provides a great value for healthcare IT, offering uncompromising performance, flexibility, centralized manageability, improved security, reduced operating cost, and required support for peripherals. Because intelligent desktop virtualization solutions take advantage of the client device's CPU to execute applications locally, new users can be added with little impact to data center and infrastructure, providing an inherently flexible and cost-effective solution for the healthcare industry. These solutions improve clinician productivity by delivering real-time collaborative workflows that also enhance patient care. The 2nd generation Intel Core vPro processor family addresses client computing needs for the healthcare industry—now and into the future.

Table 1. Recommended Intel® Core™ vPro™ Processor to Meet Your Business Needs

	 Intel® Core™ i7 vPro™ Processor	 Intel® Core™ i5 vPro™ Processor
2nd generation Intel® Core™ processor technology for top-of-the-line performance	2 and 4 cores	2 cores
Improved virtualization performance with built-in Intel® Virtualization Technology (Intel® VT) ⁶	▪	▪
Hardware-assisted security with Intel® vPro™ technology and Intel® Identity Protection Technology ^{7,2}	▪	▪
Remote manageability even when the PC is unresponsive with Intel vPro technology ⁷	▪	▪
Hardware-based acceleration of encryption and decryption with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) ¹	▪	▪
Increased processor speeds when performance is needed with Intel® Turbo Boost Technology 2.0 ⁸	▪	▪
Intelligent energy efficiency	▪	▪
Four-way or greater multi-task processing ⁹	▪	▪
Disable PCs at the hardware level with optional Intel® Anti-Theft Technology (Intel® AT) ¹⁰	▪	▪
Stunning media experience with built-in graphic processing visuals ¹¹	▪	▪

Learn more at:
<http://premierit.intel.com/healthcare>

¹ Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) requires a computer system with an Intel AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. For availability, consult your reseller or system manufacturer. For more information, see <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni>.

² <http://ipt.intel.com/welcome.aspx>

³ <http://anti theft.intel.com/welcome.aspx>

⁴ VDI TCO Analysis for Office Worker Environments," Microsoft, November 29, 2010. <http://download.microsoft.com/download/7/9/A/79AAA903-25B4-4D76-8580-BC47D5700433/Microsoft%20VDI%20TCO%20whitepaper%20customer%20ready%20v1%202.pdf>.

⁵ For more details on the MokaFive TCO model, see <http://blog.mokafive.com>.

⁶ Intel® Virtualization Technology (Intel® VT Technology) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain computer system software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

⁷ Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit www.intel.com/technology/vpro.

⁸ Requires a system with Intel® Turbo Boost Technology capability. Intel Turbo Boost Technology 2.0 is the next generation of Turbo Boost Technology and is available only on 2nd generation Intel® Core™ processors; consult your PC manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit www.intel.com/technology/turboboost.

⁹ Requires an Intel® Hyper-Threading Technology (Intel® HT Technology) enabled system; consult with your PC manufacturer. Performance will vary depending on the specific hardware and software used. Not available on all Intel® Core™ processors. For more information including details on which processors support Intel HT Technology, visit www.intel.com/info/hyperthreading.

¹⁰ Intel® Anti-Theft Technology (Intel® AT). No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware, and software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit www.intel.com/go/anti-theft.

¹¹ Available on the 2nd generation Intel® Core™ processor family. Includes Intel® HD Graphics, Intel® Quick Sync Video, Intel® Clear Video HD Technology, Intel® InTru™ 3D Technology, and Intel® Advanced Vector Extensions. Also optionally includes the Intel® Wireless Display depending on whether it's enabled on a given system. Whether you will receive the benefits of built-in visuals depends upon the particular design of the PC you choose. Consult your PC manufacturer whether built-in visuals are enabled on your system. Learn more about built-in visuals at www.intel.com/technology/visualtechnology/index.htm.


INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Copyright © 2011 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, Core Inside, Intel vPro, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Printed in USA

1111/CSG/KC/PDF

 Please Recycle

326192-001US

