Hardware-Assisted Workspace Virtualization
RingCube vDesk on Intel® Core™ vPro™ Processors

About the Authors

Dr. Charlton Barreto
Platform Architect
Intel Corporation
Charlton Barreto is a member of Intel's End-User Platform Integration group focused on Cloud Client and DC technologies. Charlton is currently driving platform strategy and architecture for Balanced Compute Cloud for Intel. He has worked over the last 15 years in architecting, developing and introducing new technologies in the Cloud, RIA, Web, and Distributed Computing markets. His more notable efforts include the development and standardization of Choreography, Process Management and Automation; Policy Management; and Reliable Messaging, Service Definition, Discovery. He writes and presents regularly on Cloud, Web and RIA strategies and technologies, and advises on what businesses and vendors can do with Cloud computing, and how to approach and leverage Cloud models, architectures and technologies to meet strategic goals and business requirements.

Dr. Tom Speeter
Chief Architect
RingCube Technologies
From 2002 through 2006, Dr. Speeter was director, founder and CTO of Cendura Corporation, a leading provider of configuration and policy compliance software. Cendura was acquired by CA in September of 2006. Prior to Cendura, Dr. Speeter was a Fellow and Chief Engineer at Healtheon Corporation (now WebMD). Prior to Healtheon, Dr. Speeter worked at Silicon Graphics as chief network architect in the Interactive Media Group. From 1986 to 1993, Dr. Speeter was a Principal Investigator in the research division at AT&T Bell Laboratories. Dr. Speeter holds a Ph.D. in Biomedical Engineering from Case Western Reserve University, a M.S.C.E from the University of Southern California, and a B.S.C.E from Michigan State University.

Mike Larkin
Co-founder & CTO
RingCube Technologies
Mike has over 13 years of experience in embedded systems, OS development and grid computing areas. Prior to co-founding RingCube, Mike worked in various management and engineering roles at IBM’s Storage Systems Division. In addition to holding an MS degree from SJSU, Mike holds a Computer Science degree from Cal Poly Pomona. Mike is also an adjunct faculty in the Computer Engineering department at San Jose State University.

Executive Summary ........................................... 2
Introduction to Hardware Assisted Virtualization 2
Introduction to Intel vPro ................................. 3
Intel Virtualization Technology (Intel VT) ....... 4
Introduction to Workspace Virtualization and
RingCube vDesk ................................................ 5
Workspace Virtualization Technology ....... 5
RingCube vDesk Overview ......................... 6
How Does vDesk Work? .......................... 6
Hardware-Assisted Workspace Virtualization:
RingCube vDesk on Intel vPro PCs ............ 7
Today’s Benefits ........................................ 7
Future Benefits ......................................... 8
Conclusion .................................................. 10
Executive Summary

Intel vPro technology is a set of capabilities built into the hardware of all 2010 Intel® Core™ vPro processor based PCs that provides hardware-assisted security, expanded management capabilities and improved power efficient performance. Intel vPro technology was designed to enhance the security and performance of virtualization solutions using local PC hardware resources to deliver a high-performance desktop virtualization experience.

As a Workspace Virtualization solution, RingCube vDesk is uniquely positioned to take advantage of Intel vPro technologies such as Intel Trusted Execution Technology (TXT), Intel Virtualization Technology (Intel VT) and Trusted Platform Module (TPM). Because vDesk workspaces are so lightweight (40MB-55MB), they can be delivered on a PC, on a removable drive or over the network, while executing the desktop computing environment locally to maximize performance and take advantage of local hardware resources including the capabilities of Intel vPro technology. As RingCube vDesk customers purchase new desktop and laptop computers, they should consider the current and future benefits of using vDesk on the Intel® Core™ vPro processor -based PCs with Intel Core i7 vPro or Intel Core i5 vPro processors:

Today’s Benefits

- Windows 7 64-bit Support (Intel VT)
- Isolation from Host PC (Intel VT)
- Secure Provisioning (Intel Active Management Technology, Microsoft SCCM, McAfee ePO)
- Anti-Theft Protection (Intel® Anti-Theft Technology, Microsoft SCCM, McAfee ePO)

Future Benefits

- Network Access Control (Intel TXT)
- Protected Launch Mechanism (Intel TXT)
- Secure Storage for Encryption Keys (TPM)
- Secure Background Updates (Intel AMT)

Introduction to Hardware Assisted Virtualization

Hardware assisted virtualization, which has been in use since 1972, leverages host hardware (typically processors) to make virtualization more efficient and provide additional security. Since 2006, hardware assisted virtualization has been available on on select Intel architecture processors. Over time, Intel has added capabilities in the processor to improve desktop virtualization including:

- Hardware acceleration for virtualization
- Secure storage
- Remote management
- Network Access Control
- Anti-Theft technology

When running on a host PC with a processor that supports hardware-assisted virtualization, desktop virtualization solutions should take advantage of its capabilities to increase performance and security.
Introduction to Intel vPro Technology

Intel vPro technology is a set of IT capabilities – security, manageability, and power management – embedded into the hardware of all 2010 Intel Core vPro processor based PCs. Because the capabilities are built into the hardware, they are available virtually anytime, even if the OS is inoperable, the PC is powered off, or the hard drive has failed.

**Intelligent Security** – Allows disabling a PC and/or disabling access to data even if the PC is lost or stolen. Encrypted PCs are also fully manageable if the PC power is off, the OS is unavailable, or the hard drive has failed. Trust attestation can be enforced on the BIOS, Firmware, OS and Virtualization Managers.

**Expanded Management Capabilities** – Remotely access, control and manage client PCs “as if you were there” with hardware-based KVM Remote Control. Save power and keep up with compliance by scheduling PCs to wake from off to run local tasks according to policies.

**Improve power management and rapid ROI** – Realize rapid ROI simply by implementing better power management enabled by Intel vPro technology.

For more information on Intel vPro, visit: [http://www.intel.com/products/vpro](http://www.intel.com/products/vpro)

**Table 1. Supported Features for 2010 Intel Core Intel Core vPro Processor Families**
Intel Virtualization Technology (Intel VT)

The 2010 Intel Core vPro Processor family includes Intel Virtualization Technology (Intel VT). Intel VT is the technology of choice for hardware-based virtualization. With Intel VT, IT administrators can centralize image management and data security. IT can now give users the client-side performance they need for multi-threaded applications, video, OS streaming, and other compute-intensive software, while still achieving robust security.

Intel VT includes hardware enhancements that shift much of the burden of software-based virtualization into the hardware. This simplifies and reduces the overhead of virtualization, making it easier for RingCube to build lightweight virtual environments. It also helps make virtualization more efficient, secure, and significantly improves performance to near native levels or better, depending on the virtualization model.

Intel VT Features

**Improving Isolation and Security** - Intel VT includes hardware enhancements that virtualize memory, the CPU, and directed I/O. These features provide a significant level of hardware enforcement for the virtualization technologies' memory manager, and significantly improve isolation of the virtual environment. In turn, this helps improve security for critical processes and sensitive data.
Establishing a trusted execution environment – One of the persistent challenges of virtualization is ensuring the integrity of the virtualization technology and the Host PC. Intel Trusted Execution Technology (TXT) addresses this important security issue using a hardware-rooted process that establishes a root of trust, which allows software to build a chain of trust from the “bare-metal” hardware to the fully functional virtual environment. Using hash-based measurements protected by hardware, Intel TXT can detect changes to the virtualization layer during its launch, which helps ensure that the virtual environment will run as expected. The process allows the virtualization layer to be verified earlier than with current software protection mechanisms (such as virus detection software).

Intel TXT also protects secrets (security credentials) during power transitions. With Intel TXT, during OS and application launch, passwords and keys are stored in protected memory. When the PC is rebooted, Intel TXT detects that secrets are still stored in memory, remotely stores the secrets, and then allows a normal boot process.

Introduction to Workspace Virtualization and RingCube vDesk

Workspace Virtualization Technology

Sitting in the architectural middle-ground between application virtualization and hypervisor-based virtualization (virtual machines) is workspace virtualization. Workspace virtualization is an approach that encapsulates and isolates an entire computing workspace. At a minimum, the workspace is comprised of everything above the operating system kernel – applications, data, settings, and any non-privileged operating system subsystems required to provide a functional Windows desktop computing environment. For deeper workspace virtualization, the virtualization engine implementation virtualizes privileged code modules and full operating system subsystems through a kernel-mode Workspace Virtualization Engine (WVE).

For more information, see Introduction to Virtual Desktop Architectures.

Workspace Virtualization Advantages

High-Performance and Small Footprint - Unlike hypervisor-based desktop virtualization, workspace virtualization operates at near-native speeds (99.7% of host), approximately 45MB of host PC memory and occupies only 40-55MB of disk space by eliminating the need to run and store two operating systems (host PC OS and guest virtual desktop OS).

For more information on Workspace Virtualization performance, see vDesk Performance Advantage Details.

Complete Desktop Environment, Broad Application Support, No Packaging – Unlike application virtualization or streaming, workspace virtualization provides a personalized desktop environment (applications, data and settings), supports virtually all applications and does not require any special packaging or sequencing of applications.
## ringcube vdesk overview

ringcube vdesk is a high-performance enterprise desktop virtualization solution that simplifies the creation, access and management of windows desktops through workspace virtualization. the vdesk solution increases user productivity, lowers desktop management costs and eliminates the performance and resource overhead of legacy virtualization technologies. users may run their virtual desktop at the office or on unmanaged pcs – such as at home or at a client site. when users start their vdesk workspace, it transforms any pc into their own familiar and personalized workspace where they can access their files, applications, settings and entire desktop, just as if they were on their own pc.

ringcube’s innovative desktop virtualization platform, workspace virtualization engine (wve), is the industry’s first workspace virtualization solution to deliver a lightweight and complete virtual desktop that can join an enterprise domain, has an isolated network stack and supports applications such as endpoint security, databases, and pc management software that require drivers and security services. today, vdesk is the only desktop virtualization solution that meets the enterprise cost, management, mobility, performance and security requirements to deploy desktop virtualization throughout an entire enterprise.

### how does vdesk work?

vdesk’s virtualization technology, with 24 virtualization patents pending, separates the user’s desktop environment, including applications, data, and settings, from the operating system and encapsulates it into a virtual workspace. to self-provision vdesk workspaces, users login to the vdesk client portal, select a master workspace, and create their own personalized workspace instances. vdesk has the flexibility
to deliver virtual desktops to users wherever they are through a variety of deployment options, including:

- **vDesk on a PC** – vDesk is stored and runs locally on a user’s PC
- **vDesk on a Drive** – vDesk is stored on a USB drive or other removable media and runs locally
- **vDesk over the Network** – vDesk is stored on a network file share and runs locally
- **vDesk over VDI (Virtual Desktop Infrastructure)** – vDesk is stored in a data center and is accessed remotely over VDI

### Hardware-Assisted Workspace Virtualization: RingCube vDesk on Intel vPro PCs

As a Workspace Virtualization solution, RingCube vDesk is uniquely positioned to take advantage of the Intel vPro and the security and performance enhancing technologies of Intel Trusted Execution Technology (TXT), Intel Virtualization Technology (Intel VT) and Intel Trusted Platform Module (TPM). As RingCube vDesk customers purchase new desktop and laptop computers, they should consider current and future benefits of using vDesk on Intel Core vPro processor family-based PCs with Intel Core i7 vPro or Intel Core i5 vPro processors.

### Today’s Benefits

#### Windows 7 64-bit Support with Intel VT

vDesk on Windows 7 x64 requires Intel Virtualization Technology (Intel VT). If customers are considering using vDesk on Windows 7 x64, they should ensure that they have Intel Core i7 vPro or Intel Core i5 vPro processors on their PCs. In addition, Intel vPro processors are designed to ensure high-performance on Windows 7 for multi-threaded Office applications, provide integrated 64-bit graphics support and make upgrading to Windows 7 seamless.

#### Isolation from Host PC with Intel Virtualization Technology (VT)

RingCube vDesk is a Workspace Virtualization technology that runs on top of the PCs host operating system. vDesk provides integrated software-based isolation and security functionality on any PC. With Intel Virtualization Technology (VT), vDesk is protected by deeper hardware-based isolation on Windows 64-bit systems by separation of host processes from virtual workspace processes. This can provide protected execution and memory spaces where sensitive data can be processed out of view of other software.

#### Secure Provisioning with Intel AMT (Microsoft SCCM, McAfee ePO)

When PCs are outside the corporate firewall, client software can only communicate with servers if a secure communication channel, such as a virtual private network (VPN), is established by the user or if the server is placed on the public Internet (not recommended). vDesk Integrates with desktop management products such as Microsoft
SCCM and McAfee ePO to provision virtual workspaces.

To enable provisioning of vDesk virtual workspaces outside the corporate firewall, Microsoft SCCM or McAfee ePO take advantage of Intel vPro and its “PC-Initiated Secure Communications” capability to establish a TLS tunnel between the vPro enabled PC and the desktop management system. For example, a user working from home on a laptop with a public Internet connection could be provisioned with a new vDesk workspace. In addition, IT could schedule the laptop to wake itself – even from a powered-down state – to receive the new vDesk workspace.

Because of the authentication protocols, this communication capability relies on collaboration with the industry to establish secure gateways for client-initiated communication.

For a list of Intel vPro technology enabled gateways, visit the Intel Active Management Technology website.

Anti-Theft Protection with Intel Anti-Theft Technology

When a vDesk workspace is stored on a laptop and that laptop is stolen, Intel Anti-Theft provides IT with a set of programmable hardware-based triggers and a “poison pill” feature to help identify a lost or stolen laptop and respond rapidly to the situation. Triggers include repeated pre-boot login failures, failure of the system to check into a central server within a particular timeframe, or a receipt of a notice from the central server to disable the PC or data access. The laptop itself can deliver a self-initiated defense, even when outside the corporate firewall, or, IT can remotely trigger defenses based on notification of a stolen laptop. Reactivation from a lock-down can easily be accomplished by local passphrase or a recovery token generated by IT.

For a list of products/services that support Intel AT, see Intel Anti-Theft Technology.

Future Benefits

Network Access Control (NAC) with Intel TXT

RingCube vDesk has an integrated Host Security Scanning capability that verifies the security posture of the host PC based on policies set in the vDesk Administration Server prior to allowing the vDesk workspace to start. For example, enterprises could configure vDesk to verify that an Antivirus and Personal Firewall are running and that the system has a certain service pack level prior to launching the vDesk Workspace.

In the future, vDesk could take advantage of Intel vPro port network isolation and hardware-based continuous host security checking to prevent the spread of malware on corporate networks from compromised host PC operating systems and ensure that the Host PC does not become compromised after the vDesk workspace has been started.

For network isolation, Intel Core vPro processors include programmable filters that monitor inbound and outbound network traffic for threats. IT managers can use third-party software (RingCube vDesk, NAC, or Endpoint Security Products) to define the policies that will trigger hardware-based isolation of a PC.

For continuous host security checking, Intel Core vPro processors use a regular, programmable “heartbeat” presence check, which is built into the Intel Management Engine. The heartbeat uses a “watchdog” timer so third-party software (RingCube vDesk, NAC, or Endpoint Security Products) can
check in with the Intel Management Engine at programmable intervals, to confirm that the agent responsible for checking host PC security is still active.

Operating System Integrity Check with Intel TXT

Prior to system startup, Intel TXT compares the hash of the trusted state of the operating system with the current state and can be configured to block system startup if a compromise is detected. In the future, vDesk could extend its Host Security Scanning policies to include verifying operating system integrity using Intel TXT prior to launching vDesk. If the PC was not using Intel vPro with TXT or the system was compromised, administrator could configure the vDesk policy to prevent the workspace from starting on that PC or warn the user of the risk.

Protected Launch Mechanism with Intel TXT

RingCube vDesk is a Workspace Virtualization technology that runs on top of a PCs host operating system. vDesk provides integrated software-based isolation and security functionality on any PC. However, with Intel vPro Trusted Execution Technology (TXT), vDesk is protected by security functionality that offers a higher level of assurance that the integrity of the virtualization layer is maintained on the host PC operating system.

The protected launch feature of Intel TXT ensures that all system software components are in a known state, referred to as “trusted” before launching. This is accomplished with three mechanisms:

A. The processor executes new SMX (Safer Mode Extensions) instructions, which generate a binary hash (a number generated by a formula) of all system software, including operating systems, applications and VMMs. The hash is performed in a secure area of the processor and the results are stored in the TPM. The new hash values are verified with the previous values before any software is allowed to start execution, thus preventing system tampering.

B. Launch control policies (LCP) define the trusted platform elements. The policies are written by the OEM or VAR and reside in a protected region on the hard disk drive. A hash of the LCP, stored in the TPM, is verified during system boot. Additional LCPs can be created by the system administrator.

C. A BIOS authentication code module, consisting of signed binaries from Intel, is stored in the BIOS and helps secure the boot procedure.
Secure Storage for Encryption Keys with Intel TPM

When you use vDesk workspaces on a laptop, RingCube recommends encrypting the workspace to ensure confidential data is not exposed if the laptop is lost. If you are in the financial services, retail, government, or healthcare industries, you may be required to encrypt your workspaces just as you would be required to encrypt the file system or hard drive of a physical PC. Whether you prefer to use vDesk Integrated Encryption to create an encrypted volume on the laptop or encrypt the entire hard drive of the laptop, protecting the encryption keys is critical to preventing unauthorized access to data. Intel TPM provides sealed storage for security codes, like VPN or data encryption keys, which keeps data secure in vDesk workspaces and when data is transmitted from a vDesk workspace using VPN encryption. Intel TXT encrypts and stores critical security codes and ensures they are only released (decrypted) to the executing environment that originally encrypted them.

Secure Background Updates with Intel AMT

To enable secure background updates of vDesk virtual workspaces outside the corporate firewall, vDesk could integrate with Intel AMT’s “PC-Initiated Secure Communications” capability to establish a TLS tunnel between the vPro enabled PC and the vDesk Administration Server. For example, a user working from home on a laptop with a public Internet connection could receive updates to their vDesk workspace including a new policy, upgrades to applications, changes to configurations. In addition, IT could schedule the laptop to wake itself – even from a powered down state – to receive the updates.

Because of the authentication protocols, this communication capability relies on collaboration with the industry to establish secure gateways for client-initiated communication.

For a list of Intel vPro technology enabled gateways, visit the Intel Active Management Technology website.

Conclusion

There are many different forms of desktop virtualization such as local virtual machines (type II hypervisors), Virtual Desktop Infrastructure (VDI), application virtualization and workspace virtualization. Workspace virtualization delivers a lightweight and high-performance (99.7% of native host) desktop virtualization solution that provides a complete desktop environment with broad application support and no specialized packaging requirements. RingCube vDesk enables IT to deliver virtual workspaces on a PC, on a removable drive or over the network, while executing the workspace using local PC resources including the Intel vPro capabilities. In order to run vDesk on Windows 7x64, customer need to ensure that they are running Intel vPro i5 or i7 processors. When vDesk is running on a PC with Intel vPro, vDesk workspaces can be configured to have hardware-assisted isolation and the security of Anti-Theft Protection. In the future, vDesk can take advantage of additional Intel vPro capabilities such as enhanced Network Access Control (NAC), hardware-based encryption acceleration and secure WAN communication.

Additional Resources

1. Introduction to vDesk Whitepaper
   http://www.ringcube.com/portal/content/files/whitepapers/wp_intro_vdesk.pdf
2. Introduction to Virtual Desktop Architectures
3. Desktop Virtualization Buyer’s Guide  
   http://www.ringcube.com/request/register/buyers_guide.html
4. PC Benchmark Results: vDesk Performance Advantage  
   http://www.ringcube.com/portal/content/products/vdesk/demos/performance/perf.pdf
5. Intel vPro Whitepaper  
   http://www.ringcube.com/portal/content/products/vdesk/tco_report_req.jsp
6. Intel Active Technology Management (AMT)  
   http://www.intel.com/technology/platform-technology/intel-amt/
7. Intel Anti-Theft  
   http://www.intel.com/technology/anti-theft/

About RingCube Technologies, Inc.

RingCube is the leading provider of workspace virtualization. The company's innovative virtualization solution, vDesk, enables users to securely access their complete desktop computing experience from any Windows PC anywhere in the world. With vDesk, organizations can increase user productivity, lower desktop management and support costs, and eliminate the performance and resource overhead commonly found with legacy virtualization approaches. The company is privately held and based in Mountain View, CA. For more information, please visit: www.ringcube.com