The All New 2010 Intel® Core™ vPro™ Processor Family: Intelligence that Adapts to Your Needs

Secure your PCs. Cut your costs.
Achieve more control. Now that's smart ROI.

White Paper

Intel® Core™ i7 vPro™ Processor

Intel® Core™ i5 vPro™ Processor

PCs powered by a new 2010 Intel® Core™ vPro™ processor can adapt to the needs of your business with smart security, cost-saving manageability, and intelligent, adaptable performance.[1] The all new 2010 Intel Core vPro processor family is designed to keep downtime and desk-side visits to a minimum, helping IT reduce costs and improve services through enhanced remote monitoring, KVM Remote Control[2] (keyboard video mouse), and other tools to diagnose and repair PCs – even if the PCs are shut down or the operating system (OS) is unresponsive. Intelligent, energy-efficient performance – including Intel® Turbo Boost Technology[3] – adapts to a user's multitasking demands so the PC consumes only the power it needs. With an all new 2010 Intel Core vPro processor inside, PCs can even disable themselves via Intel® Anti-Theft Technology[4] if they get lost or stolen. With a new Intel Core vPro processor, control meets cost savings while still delivering exceptional business performance.

Table of Contents

Executive Summary

The all new 2010 Intel® Core™ vPro™ processor family can help businesses by delivering intelligent security; cost-saving remote manageability; and adaptable performance. Smart security with programmable filters can systematically guard against viruses and malicious attacks. Continuous, intelligent polling for the presence of software agents helps ensure full protection from malware and attacks. Advanced features help prevent tampering or disabling of security software. With built-in Intel® Anti-Theft Technology[4] (Intel® AT), PCs can even disable themselves if they are lost or stolen. And, because data is protected rather than erased, reactivation can be easy when the PC is recovered. Intel AT must be enabled in order to enjoy the benefits of this advanced security technology.

The all new 2010 Intel Core vPro processor family makes it easier to manage systems from a central location. KVM Remote Control[2] (keyboard video mouse) and other built-in capabilities let you remotely configure, diagnose, isolate, and repair an infected PC – even if the OS is unresponsive.[1] You can also quickly upgrade to Windows* 7 remotely and overnight – saving on average about 40 minutes per upgrade per machine.[5] This helps minimize disruptions to your users and makes it easier to retain access to your legacy applications. In order to enjoy the benefits of these intelligent remote manageability capabilities, Intel® vPro™ technology must be activated (see page 25 of this white paper).

Laptops powered by a new Intel Core vPro processor include Intel® Centrino® wireless technology (either WiFi or WiFi with optional WiMAX), and are more energy efficient. These laptop and desktop PCs also include Intel® Turbo Boost Technology[3] and Intel® Hyper-Threading Technology[6] (Intel® HT Technology), which can automatically adapt to each user's unique needs so users can move faster when multitasking and get more accomplished in less time.

Studies have shown that return on investment (ROI) can be as little as 19 months for PCs based on the a new 2010 Intel® Core™ i5 processor.[7] For businesses that implement the remote management and security capabilities of a PC with a new 2010 Intel Core i5 vPro processor, positive ROI can be achieved in as little as 9 months.[7]

Lineup of all new 2010 Intel® Core™ processor family and all new 2010 Intel® Core™ vPro™ processor family.

Choose the Intel® Core™ processor that meets your business needs		Intel® Core™ i7 vPro™	Intel® Core™ i5 vPro™	Intel® Core™ i7	Intel® Core™ i5	Intel® Core™ i3
Intelligent Performance, Security and Manageability	Hardware-assisted smart security, anti-theft technology and cost-saving manageability[a]	●	●	○	○	○
	Hardware-based KVM Remote Control[2,a,b]	●	●	○	○	○
	Hardware-assisted remote power management[a]	●	●	○	○	○
Intelligent Business Performance	Top-of-the-line performance with biggest cache	●	○	●	○	○
	Hardware-based acceleration of encryption[8]	●	●	●	●	○
	Increased processor speeds when performance is needed with Intel® Turbo Boost Technology[3]	●	●	●	●	○
	Hardware-assisted virtualization support for running multiple operating systems, such as Windows* XP with Windows* 7[9]	●	●	●	●	●
	Intelligent performance with Intel® Hyper-Threading Technology[6] and Intel® Smart Cache	●	●	●	●	●
	Energy Efficiency with Intel® Intelligent Power Technology	●	●	●	●	●

[a] IT must activate Intel® vPro™ technology in order to take advantage of these intelligent security and remote manageability technologies. For more information about activating Intel vPro technology, which includes Intel® AMT and Intel® AT, see page 25 of this white paper.

[b] Hardware-based KVM Remote Control works on all new 2010 Intel® Core™ i5 vPro™ processor-based PCs that have Intel® HD integrated graphics, and select all new 2010 Intel® Core™ i7 vPro™ processor-based PCs that have Intel® HD integrated graphics. Hardware-based KVM Remote Control will not work on PCs that use discrete graphics.

○ **Not applicable** ● **Advanced capability**

All New 2010 Intel® Core™ vPro™ Processor Family

Intelligent security, remote manageability, and adaptable performance to help businesses cut costs and improve efficiencies

The way we do business has changed

In today's global markets, business is increasingly borderless, and mobility is becoming mandatory. The amount of e-mail that corporate users manage each day has also increased dramatically. Video has become mainstream for corporate communications – the use of video conferencing alone is expected to double from 2007 to 2012.[10] At the same time, countries around the world are implementing increasingly stringent energy-compliance regulations for PCs. In addition, security threats continue to grow each year. Along with increased purchasing power in emerging markets, these shifts are driving major changes in business models worldwide.

Today's business challenges include:

- Critical need to become more efficient, reducing costs while still reaching new customers
- Increased demand for video tools for mainstream communications, both internal, such as for sales and marketing, and external, for customers
- Exponential increase in security threats, along with a shift from ego-based attacks to economically focused attacks
- Pressure from governments around the world to use PCs that are more environmentally friendly and consume less power

Information Technology (IT) managers face a corresponding set of challenges in managing PCs as strategic assets:

- Support an increasingly mobile workforce.
- Protect networks and assets both inside and outside the corporate firewall.
- Reduce operating costs for managing and securing PCs.
- Support new, compute-intensive applications and the transition to Windows* 7.

Organizations can no longer wait to capitalize on global integration and advanced technology tools. The challenge for IT is to support business goals, managing PCs as strategic assets. To do so, IT organizations need laptop and desktop PCs that are easier to configure, manage, use, and secure.

New and proven technologies pair up to deliver intelligent security, remote manageability, and adaptable performance

Control meets cost savings in laptop and desktop PCs powered by the all new Intel® Core™ vPro™ processor family.

Laptop and desktop PCs with a new Intel Core vPro processor deliver intelligent performance and unique hardware-assisted features that improve security, remote manageability, and energy management.

- New 2010 Intel® Core™ i5 vPro™ processor-based PCs[1]
- New 2010 Intel® Core™ i7 vPro™ processor-based PCs[1]

New features in this new generation of processors include intelligent security, such as Intel Anti-Theft Technology, and easier manageability – including KVM Remote Control[2] (hardware-based keyboard video mouse) and PC Alarm Clock. Additional new features for adaptable performance include Intel® Turbo Boost Technology,[3] as well as AES-NI[8] (advanced encryption standard – new instructions), to improve performance for encryption and decryption. For example, using Intel AT, you can remotely disable a PC with a "poison pill" that locks down the system after it has been reported lost or stolen.

Access the PC virtually anytime, anywhere

The hardware-based capabilities of the all new 2010 Intel Core vPro processor family are built directly into the PC's hardware. The capabilities let authorized technicians remotely access PCs that have traditionally been unavailable to the management console. Technicians can now manage the laptop or desktop PC even if PC power is off, the OS is unresponsive, hardware (such as a hard drive) has failed, or management agents are missing. Best of all, technicians can remotely maintain, update, and repair both laptop and desktop PCs that are outside the corporate firewall on an open wired or wireless connection via a secure, protected tunnel.

PCs can now be managed as strategic assets

With the new 2010 Intel Core vPro processors, businesses can significantly cut IT service costs, reduce power bills, increase efficiency, and improve productivity. For example:

- Experience up to 2x faster multitasking[11] and up to 3.5x faster encryption/decryption of sensitive data on a new Intel® Core™ i5 processor.[11]
- Cut PC maintenance costs by up to 50%.[7]
- Speed up patch saturation by 56%[12] and reduce patch deployment costs by up to 98%.[13]
- Shift more workers to laptops and gain up to 51 more minutes per user per day in user productivity.[14]
- Reduce energy costs enabled by secure remote power up/down.[15]

Spend wisely and recoup costs rapidly

Less-capable PCs can get bogged down when trying to support the latest OS, such as Windows 7, or the latest application updates. After 3 years, annual PC support costs can exceed the purchase price for a new PC.[7] On average, a 4-year-old PC can cost 59% more to support than it did in its first year.[7] In addition, 3-year-old PCs are 53% more likely per year to experience a security incident.[7] Worse, a single PC out of compliance can create an expensive security incident – up to $300,000 or more in costs – but businesses do not always budget for the full cost of a security breach.[16]

Laptop and desktop PCs with a new Intel Core vPro processor can handle the latest multi-threaded OSs, end-user applications and IT software load – including Windows 7, Office* 2007, encryption software, application streaming, and video conferencing. These PCs can also be more easily secured, via intelligent client-side capabilities, as well as through remote security features, such as PC disable via "poison pill" responses. With better remote troubleshooting and problem resolution – through secure console redirection and KVM Remote Control – IT can reduce user downtime, help improve user productivity, keep desk-side visits to a minimum, and help businesses significantly reduce TCO.

In an environment in which businesses have a critical need to spend wisely, this new generation of PCs makes it easier for organizations to manage systems as strategic assets. In fact, studies show that businesses can recoup their investment in as little as 9 months.[7]

Refreshing wisely means keeping TCO at a minimum. Refreshing with PCs with new Intel Core vPro processors can help you achieve a positive ROI rapidly and continuously for years to come.

New in the all new 2010 Intel Core vPro processor family

The new 2010 Intel Core vPro processors includes powerful new capabilities built into the hardware:

- Intel Anti-Theft Technology (Intel AT), lock down and "brick" the PC if it fails to check in to the central server, or if it fails preboot login based on local, hardware-level preboot/OS IT-defined rules. As part of the lockdown, delete or disable critical elements of encryption keys in order to prevent access to the keys and stored data. Allow rapid reactivation, integrated with existing software vendor preboot login.
- Manageability of PCs with encrypted hard drives – remotely unlock encrypted drives that require pre-boot authentication, even when the OS is inoperable or software agents are missing. Remotely manage data security settings even when PC is powered down.
- AES-NI instructions (Advanced Encryption Standard New Instructions),[8] which offload from the processor some of the performance burden of encryption, and file decryption.
- KVM Remote Control,[2] a new hardware-based feature that works for wired and wireless PCs with a new Intel Core vPro processor that have integrated Intel® HD Graphics. This feature helps IT remotely resolve the most complex software failures, and eliminates the need to purchase and maintain costly hardware KVM switches in the production environment. KVM Remote Control works for PCs both inside and outside the corporate firewall.
- Fast call for help for wired or wireless systems, even beyond the firewall.[17] Helps users avoid the costly downtime of shipping PCs back to IT to be fixed. If a PC crashes, a user can phone IT for help and, during the boot process, press a specific key to securely connect the PC to IT for troubleshooting. IT can then take over via remote console redirection or hardware-based KVM Remote Control.
- PC Alarm Clock,[1] a new hardware-based feature that lets IT schedule a PC to wake itself from any idle, powered off, or sleep state without a network connection. The PC can then perform scheduled, IT-defined tasks, such as initiate a secure call to the service center for automated, off-hour services – even if outside the corporate firewall. As with other features, PC Alarm Clock is configured via a management console. However, once the feature is implemented, businesses do not need a management console to access or use the feature in their production environment. PC Alarm Clock works even if there is no network or communication with the PC. For example, the feature allows independent software vendors (ISVs), such as McAfee, to enable IT-scheduled product updates even for businesses that don't have an IT console.

Key features of the all new 2010 Intel Core vPro processor family

The all new 2010 Intel Core vPro processor family delivers unique and powerful technologies in security, remote manageability, energy management, mobility, virtualization, and performance improvements. Tables 1 and 2 list some of the key features of laptop and desktop PCs with a new Intel Core vPro processor.

Table 1. Laptop and desktop PCs with a new Intel® Core™ vPro™ processor.

Feature	Laptop with Intel® Core™ vPro™ processor	Desktop PC with Intel® Core™ vPro™ processor
All new 2010 Intel® Core™ vPro™ processor family	Intel® Core™ i5 vPro™ processor and Intel® Core™ i7 vPro™ processor with Intel® QM57 or QS57 Express Chipsets	Intel® Core™ i5 vPro™ processor and Intel® Core™ i7 vPro™ processor with Intel® Q57 Express Chipset
Intel® Active Management Technology[1] (Intel® AMT), release 6.0	●	●
Intel® Gigabit network connection	Intel® 82567LM-3	Intel® 82566DM
Support for 802.11agn wireless protocols	●	N/A
WiFi and optional WiMAX support, with either Intel® WiMAX/WiFi 6060 2x2 agn, Intel® Centrino® Ultimate-N/Advanced-N 6000 Series 2x2 or 3x3 agn, or Intel® Centrino® Wireless-N 1000 Series 1x2 bgn	●	N/A
Support for 802.1x	●	●
Intel® Stable Image Platform Program (Intel® SIPP)[18]	●	●

Table 2. All new 2010 Intel® Core™ processor family and all new 2010 Intel® Core™ vPro™ processor family.

Features for...	Description	Intel® Core™ i7 vPro™	Intel® Core™ i5 vPro™	Intel® Core™ i7	Intel® Core™ i5	Intel® Core™ i3
Intelligent Performance, Security and Manageability	Hardware-assisted smart security,[1] anti-theft technology and cost-saving manageability[a]	●	●	○	○	○
	Hardware-assisted remote power management[a]	●	●	○	○	○
	Hardware-based KVM Remote Control[a,b,2]	●	●	○	○	○
	Intel® Virtualization Technology[9] (Intel® VT) including Intel® VT for Directed I/O, and support for OS and application streaming	●	●	○	○	○
	Intel® Trusted Execution Technology[19] (Intel® TXT)	●	●	○	○	○
	Support for Cisco Self-Defending Network* (Cisco SDN*), Microsoft Network Access Protection* (NAP), and PXE (preexecution environment)	●	●	○	○	○
Intelligent Business Performance	Hardware-based acceleration of encryption[8]	●	●	●	●	○
	Intel® Turbo Boost Technology[3]	●	●	●	●	○
	Intel® Smart Cache Technology and new L3 cache	Up to 8 MB L3	Up to 4 MB L3	Up to 8 MB L3	Up to 4 MB L3	Up to 4 MB L3
	Number of processor cores	2 to 4 cores	2 cores	2 to 4 cores	2 cores	2 cores
	Intel® Hyper-Threading Technology[6]	4 to 8 threads	4 threads	4 to 8 threads	4 threads	4 threads
	64-bit enabled[20]	●	●	●	●	●
Support for Operating System Requirements	Windows* 7 ready	●	●	●	●	●
	Hardware-assisted virtualization for Windows* XP in Windows* 7[c]	●	●	●	●	●
	Intel integrated graphics support of 64-bit graphics, including Windows 7 Aero interface[d]	●	●	●	●	●
	Execute Disable Bit[21]	●	●	●	●	●

[a] IT must activate Intel® vPro™ technology in order to take advantage of these intelligent security and remote manageability technologies. For more information about activating Intel vPro technology, which includes Intel® AMT and Intel® AT, see page 25 of this white paper.

[b] Hardware-based KVM Remote Control is available on Intel® Core™ i5 vPro™ and Intel® Core™ i7 vPro™ processors that have Intel integrated graphics.

[c] Hardware-assisted Intel® Virtualization Technology (Intel® VT) can significantly improve performance for users running a legacy OS (for example, Windows* XP) in Windows 7.

[d] Some new Intel Core processors do not include integrated graphics. Some allow for discrete graphic cards.

What, exactly, is Intel® vPro™ technology?

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

- **Intelligent security.** Disable a PC and/or disable access to the data even if the PC is already lost or stolen. Encrypted PCs are also fully manageable if PC power is off, the OS is unavailable, or the hard drive has failed.
- **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 policy.
- **Improved power management and rapid ROI.** Realize rapid ROI simply by implementing better power management enabled by Intel vPro technology.

Intel vPro technology takes advantage of an intelligent processor, chipset, and networking silicon features, along with protected flash memory. When combined with existing independent software vendor (ISV) consoles that support Intel vPro technology, Intel vPro technology can deliver a comprehensive, tamper-resistant solution for security and manageability.

A key benefit of being embedded in hardware is that the capabilities are less susceptible to the problems that typically affect an OS, applications or hard drive. For example, because Intel vPro technology is designed into PC hardware, it is resistant to tampering, boot issues, and other problems that can affect an OS and/or security applications.

Intelligent features to solve key challenges

The all new 2010 Intel Core vPro processor family can provide a comprehensive solution to manageability and security challenges. Table 3 provides an overview of some of the features of these new processors. New features and some of the more critical proven technologies are described in detail later in this paper.

Table 3. Key IT challenges and solutions addressed with a new 2010 Intel® Core™ vPro™ processor-based PC.

Challenge	Solution[a]
PCs unmanageable when powered down[1]	Remotely and securely monitor and manage PCs anytime: ▪ **Access the PC even if PC power is off,** the OS is unresponsive, management agents are missing, or hardware (such as a hard drive) has failed. ▪ **Access critical system information** (asset information, event logs, BIOS information, etc.) virtually anytime, even if PC power is off, to identify systems that need maintenance or service. ▪ **Remotely and securely power up PCs** for maintenance and service, initiated by the service center. ▪ **PC Alarm Clock,** in which client-side intelligence performs a scheduled wake from any powered off or sleep states, so the PC itself can call in and initiate a maintenance, security or other task off-hours.
Unsecured communications with PCs	More securely communicate with laptop and desktop PCs both inside or outside the corporate firewall: ▪ **Secure, remote communication inside the firewall.** ▪ **Secure, remote communication outside the firewall,** on an open wired or wireless LAN.
Spiraling and costly deskside visits	Significantly reduce deskside visits with: ▪ **Remote remediation,** even if management agents are missing or the OS is unresponsive. ▪ **Remote problem resolution,** even if the OS is unresponsive or hardware (such as a hard drive) has failed. ▪ **KVM Remote Control**[2] to help resolve complex issues, so you can see exactly what the user sees, and repair the PC more effectively from a remote location.
Protect assets from software-based attacks	Protect assets better: ▪ **Remotely power up PCs** anytime to help ensure more complete saturation for patching and other updates. ▪ **Built-in, programmable system defense filters and agent-presence checking** for automated, hardware-based protection against viruses and attacks.
Thwart thieves – secure assets and data even if the PC is lost or stolen[4]	Disable or "brick" a PC and/or protect its data virtually anytime: ▪ **Poison-pill** to "brick" a lost or stolen PC; data is not destroyed or lost in the process, and reactivation is rapid, simply by entering an authentication token. ▪ **Remote notification** via a 3G modem in a cell phone, to flag a system that might be in the process of being stolen. ▪ **Built-in, programmable triggers** and responses to protect data and the PC after loss or theft of the system.[4] ▪ **Intelligent, policy-based PC-side timers** that trigger a lockdown if the user has not logged in before timer expiry.
Lack of configuration compliance	Ensure compliance: ▪ **Remote inventory and agent presence checking** as a hardware-based, automated, policy-based service.
Costly and time-consuming manual inventories	Eliminate virtually all manual inventories: ▪ **Accurate, remote asset inventories,** even if PCs are powered off or management agents are missing.
Undiscoverable assets	Discover virtually all PCs: ▪ **Persistent device ID available anytime,** even if PC power is off, the OS has been rebuilt, hardware or software configuration has changed, or the hard drive has been reimaged.
Reimage systems without a deskside visit	Reduce deskside visits, speed up remote deployment, and minimize user interruptions: ▪ **Remotely reimage systems** even if PC power is off at the start of the upgrade cycle.

[a] IT must activate Intel® vPro™ technology in order to take advantage of these intelligent security and remote manageability technologies. For more information about activating Intel vPro technology, which includes Intel® AMT and Intel® AT, see page 25 of this white paper.

Manage PCs regardless of power state

PCs based on the all new 2010 Intel Core vPro processor family are designed to give IT technicians greater remote visibility into and access to the system in both wired and wireless states, as described in Table 4. When managing PCs with the all new 2010 Intel Core vPro processor family, technicians can remotely power up a PC almost anytime. (In order to prevent unexpected battery use in laptops, remote power-up is not applicable to the battery-powered, wireless sleep state.) Technicians can also reboot the PC, use secure console redirection and KVM Remote Control, and use other critical maintenance and management capabilities of a new 2010 Intel Core vPro processor for wired or wireless PCs. PCs can even perform their own local, scheduled wake from any powered-off state without a network connection. The PC can then call into a central server for updates, maintenance, and other off-hours tasks.

With the ability to remotely manage PCs regardless of power state, IT can streamline more work and implement more automation. In turn, this helps business minimize user downtime, reduce IT service costs, and realize a rapid ROI.

Table 4. Capability matrix for PCs with new 2010 Intel® Core™ vPro™ processors.

Use Cases[a]	Usages[a]	Works with wired PC-initiated secure communication outside corporate firewall[a]	AC-powered wired or wireless laptop or wired desktop			Battery-powered wired or wireless laptop		
			AWAKE, OS WORKING PROPERLY	AWAKE, BUT OS UNRESPONSIVE	ASLEEP (Sx)	AWAKE, OS WORKING PROPERLY	AWAKE, BUT OS UNRESPONSIVE	ASLEEP (Sx)
Remote power up/power cycle	IT remotely powers PC down, then up again to reset to clean state (or powers up PC for servicing). Use power management to reduce energy costs.	YES	YES	YES[b]	YES	YES	YES[b]	N/A
Remote software update	Power up PCs during off hours for software updates. Also client-initiated scheduled wake for update.	YES	YES	YES[b]	YES	YES	YES[b]	N/A
Agent presence checking and alerting	Ensure critical applications are running, and be quickly notified when they miss a check in.	YES	YES[c]	YES[b]	N/A	YES[c]	YES[b]	N/A
System isolation and recovery	Automated or manual policy-based protection against virus outbreaks.	YES	YES	YES[b]	N/A	YES	YES[b]	N/A
Protection for data if a laptop is lost or stolen	Identify and prevent unauthorized access to encrypted data, or disable the laptop remotely or via client-side intelligence if it is lost or stolen. Upon lock-down, disable or delete access to encryption keys. Rapid reactivation if laptop is returned.	N/A	YES[c] for laptops	YES for laptops	N/A	YES[c] for laptops	YES for laptops	N/A
Remote diagnosis and repair	Diagnose and repair problems remotely via out-of-band event log, remote/redirected boot, console redirection, KVM Remote Control,[2] and preboot access to BIOS settings.	YES	YES	YES[b]	YES	YES	YES[b]	N/A
Remote hardware and/or software asset tracking	Take a hardware or software inventory regardless of OS state or power state.	YES	YES[c]	YES[b]	YES	YES	YES[b]	N/A

[a] IT must activate Intel® vPro™ technology in order to take advantage of these intelligent security and remote manageability technologies. For more information about activating Intel vPro technology, which includes Intel® AMT and Intel® AT, see page 25 of this white paper.

[b] Requires WPA or WPA2/802.11i security and Controller Link 1 for wireless operation when the user OS is down.

[c] Also available when using host OS-based VPN.

Use an existing management console for both laptop and desktop PCs

PCs with a new 2010 Intel Core vPro processor can use the same management console and communication mechanisms as other PCs. You can manage both laptop and desktop PCs with a new Intel Core vPro processor from the same IT console.

Leading management software companies such as HP, LANDesk, Microsoft, and Symantec have optimized their software to take advantage of the intelligent capabilities of a new 2010 Intel Core vPro processor. For small businesses with less than 500 PCs, IT administrators can turn to management software such as N-able Technologies' N-central* to take advantage of a new 2010 Intel Core vPro processor.

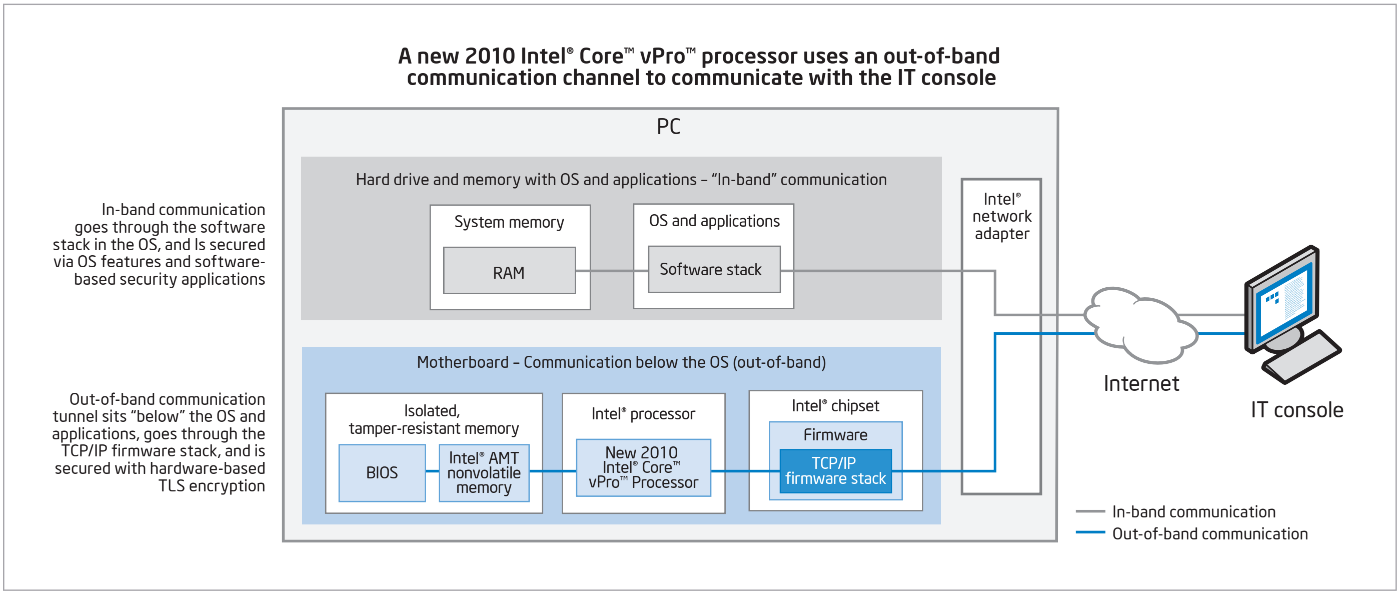
These vendors support both previous and current versions of Intel vPro technology. IT administrators who have already deployed PCs with Intel vPro technology do not have to change their management console to use PCs with a new 2010 Intel Core vPro processor. Ask your management-console vendor about specific implementation schedules and support for the new hardware-based security and remote-management capabilities for both laptop and desktop PCs.

Remote communication – virtually anytime

Software-only management applications are usually installed at the same level as the OS (see Figure 1). This leaves their management agents vulnerable to tampering. Communication privacy is also an issue in today's PCs because the in-band, software-based communication channel they use is not secure.

In contrast, the all new 2010 Intel Core vPro processor family delivers both "readily-available" (out-of-band) remote communication built into the PC, as well as robust security technologies. These security technologies help ensure that the powerful capabilities of Intel vPro technology, as well as your stored information, are better protected.

The communication channel used by Intel vPro technology runs "under" or outside the OS (see Figure 1). This out-of-band (OOB) channel is based on the TCP/IP firmware stack designed into PC hardware, and does not use the software stack in the OS. The channel allows critical system communication (such as alerting) and operations (such as agent presence checking, remote booting, and console redirection) to continue more securely virtually anytime, even if OS, applications, or hard drive have failed.



A new 2010 Intel® Core™ vPro™ processor uses an out-of-band communication channel to communicate with the IT console

In-band communication goes through the software stack in the OS, and Is secured via OS features and software-based security applications

Out-of-band communication tunnel sits "below" the OS and applications, goes through the TCP/IP firmware stack, and is secured with hardware-based TLS encryption

PC
Hard drive and memory with OS and applications – "In-band" communication
System memory
RAM
OS and applications
Software stack
Intel® network adapter
Motherboard – Communication below the OS (out-of-band)
Isolated, tamper-resistant memory
BIOS
Intel® AMT nonvolatile memory
Intel® processor
New 2010 Intel® Core™ vPro™ Processor
Intel® chipset
Firmware
TCP/IP firmware stack
Internet
IT console
In-band communication
Out-of-band communication

Figure 1. Out-of-band communication. Secure communication channel runs "under" or outside the OS regardless of the health of the operating system or the power state of the PC, even if the PC's hard drive is removed.

Communication outside the corporate firewall

Laptops and desktop PCs with a new Intel Core vPro processor support secure communication in an open wired or wireless LAN – outside the corporate firewall. This capability allows the PC to initiate communication with a remote management console through a secured tunnel for inventories, diagnostics, repair, updates, and alert reporting. IT managers now have critical maintenance and management capabilities for PCs in satellite offices, outside the corporate firewall, and in locations that don't have an onsite proxy server or management appliance, such as at a small business client's remote location. Now, IT managers can:

- Securely update and service PCs, via a prescheduled maintenance time when the PC initiates a secure connection to the IT console. This capability is available even when the system is outside the corporate firewall.
- Hotkey auto-connection to IT console, so a user can quickly connect the PC to the IT console for help or system servicing.

The PC-initiated communications capability works through the use of an Intel vPro technology-enabled gateway in the DMZ (demilitarized zone) that exists between the corporate and client firewalls (see Figure 2). System configuration information in the PC includes the name(s) of appropriate management servers for the company. The gateway uses that information to help authenticate the PC. The gateway then mediates communication between the PC and the company's management servers during the repair or update session.

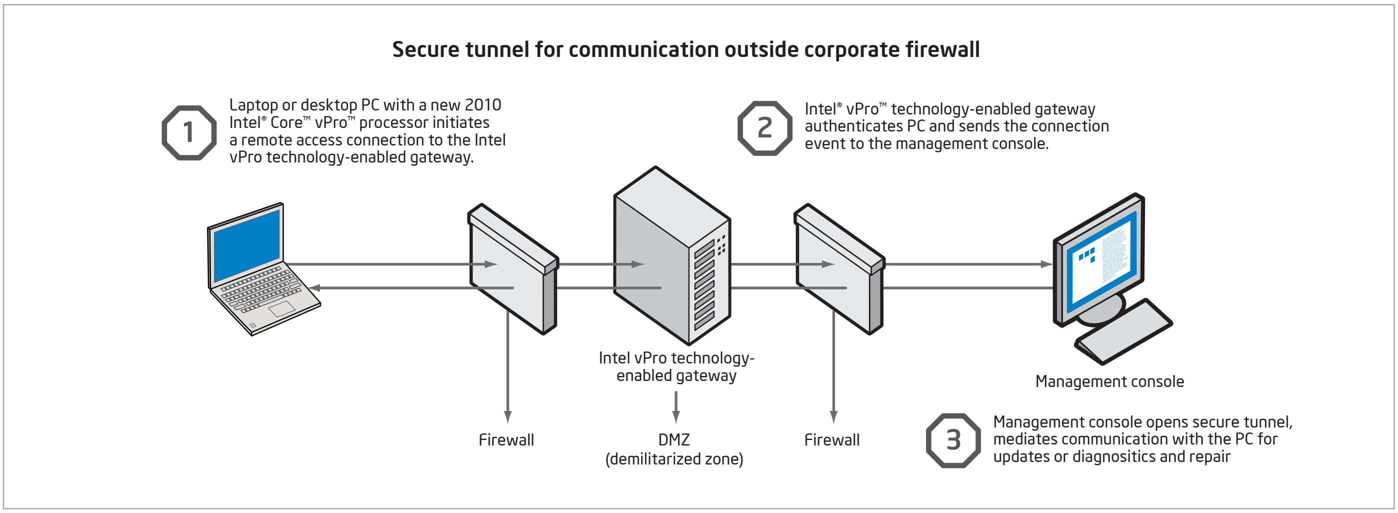
Communicate remotely with wired or wireless PCs

Once Intel vPro technology is activated, an authorized IT technician can communicate with PCs with a new 2010 Intel Core vPro processor:

- Wired AC-powered PC – anytime. Even if hardware (such as a hard drive) has failed, the OS is unresponsive, the PC is powered off, or its management agents are missing, the communication channel is still available. As long as the system is plugged into a wired LAN and connected to an AC power source, the channel is available to authorized technicians.
- Wireless laptop on battery power – anytime the system is awake and connected to the corporate network, even if the OS is unresponsive.[17]
- Wired, connected to the corporate network over a host OS-based VPN – anytime the system is awake and working properly.

PC-initiated secure communication

PC-initiated secure communication is a new capability that allows a PC to initiate its own secure communication tunnel back to an authorized server. For example, the PC Alarm Clock feature allows IT to schedule the PC to wake itself – even from a powered down state. The PC can then use other hardware-based capabilities to call "home" to look for updates or initiate other maintenance or service tasks. Because of authentication protocols, this communication capability relies on collaboration with the industry to establish secure gateways for client-initiated communication.


Secure tunnel for communication outside corporate firewall
1
2
3
Intel vPro technology-enabled gateway
Management console
Firewall
DMZ (demilitarized zone)
Firewall

1 Laptop or desktop PC with a new 2010 Intel® Core™ vPro™ processor initiates a remote access connection to the Intel vPro technology-enabled gateway.

2 Intel® vPro™ technology-enabled gateway authenticates PC and sends the connection event to the management console.

3 Management console opens secure tunnel, mediates communication with the PC for updates or diagnostics and repair

Figure 2. Communication to PCs outside the corporate firewall is secured via TLS. An Intel® vPro™ technology-enabled gateway authenticates wired and wireless PCs, opens a secure TLS tunnel between the management console and PC, and mediates communication.

Robust security schemes for remote communication

The hardware-based communication and manageability capabilities are secured through a variety of robust methodologies, technologies, and schemes. These include:

- Transport Layer Security (TLS).
- HTTP authentication.
- Enterprise-level authentication using Microsoft Active Directory* (Kerberos).
- Access control lists (ACLs).
- Digital firmware signing.
- Other advanced methodologies and technologies (refer to the Intel® vPro™ Technology Expert Center at communities.intel.com/docs/DOC-1370).

The security measures built into laptop and desktop PCs with a new Intel Core vPro processor can be active even when the PC is off, software agents have been disabled, or the OS is unresponsive. These measures help ensure the security of stored information and the confidentiality and authentication of the communication channel and hardware-based capabilities.

Better protection through smarter security

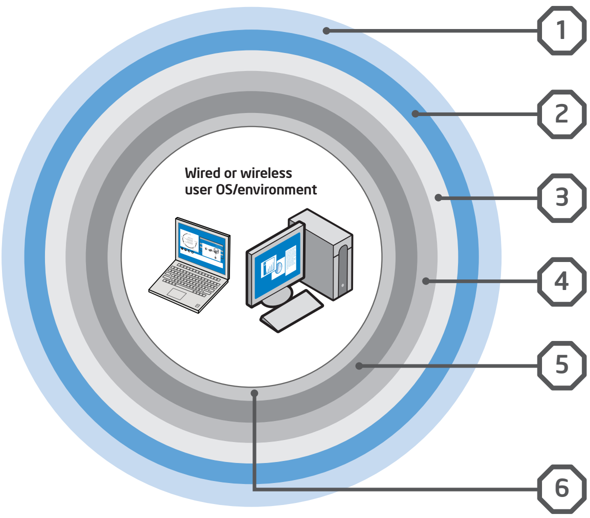
Security remains one of the highest priorities for IT. The number of security incidents has grown dramatically each year and the nature of these threats has changed as the motivations of attackers have shifted from bragging rights to financial gain. The cost of a data breach is also rising. A recent survey of 43 companies in 2008 found that the average cost of a lost or stolen laptop is $49,000.[22]

The all new 2010 Intel Core vPro processor family can make it easier to protect data and assets. Once Intel vPro technology is activated, IT can take advantage of intelligent new security features, such as hardware-based PC disable and full manageability for encrypted PCs. For example, IT can use programmable defense filters to automatically guard against viruses and malicious attacks. When Intel AT is also activated, IT can use anti-theft triggers to help determine when a laptop is in unauthorized hands, and lock down the machine to thwart data breaches attempted by thieves. These features help IT secure laptop and desktop PCs, both inside and outside the corporate network.

- **Push updates down the wire, regardless of PC power state.**
  - Remotely and securely power up PCs from the IT console to prepare them for patching.
  - Automatically deploy more updates and critical patches off-hours or when it won't interrupt the user.
  - Check a PC's software version information, .DAT file information, and other data stored in nonvolatile memory, and find out if anything needs updating without waking up a PC.
  - Reduce power consumption and lower energy bills by powering down PCs during off-hours, while still maintaining remote access for security updates.
- **Intel Anti-Theft Technology** (Intel AT), which includes programmable triggers and "poison pill" features for identifying and responding – locally or remotely – to loss or theft of the system. Intel AT allows IT to disable access to data encryption keys and the PC at a hardware-level, while still allowing rapid and remote reactivation. Intel AT must be enabled (on) in order for IT to take advantage of these intelligent security features.
- **Programmable filtering** of inbound and outbound network traffic.
- **Isolation of systems** that are suspected of being compromised – even if they are out of band or outside the corporate firewall.
- **Agent presence checking**, with continuous, intelligent polling for the presence of software agents, to help make sure security remains in place. IT can also use this capability to reduce unauthorized application usage by up to 100%.[23]
- **Alerting from inside and outside the corporate network,** such as for agent presence checking and inbound/outbound filtering of threats even if the OS is inoperable, software agents are missing, or a hard drive has failed or been removed.
- **Dedicated memory**, which better protects critical system information (such as hardware-based encryption keys) from viruses, worms, and other threats. An authorized IT technician can remotely access this protected memory to identify system ID, firmware version number, and other system information – even if PC power is off, the OS is unavailable, or hardware (such as a hard drive) has failed.
- **Manageability of PCs with encrypted hard drives,** to remotely unlock encrypted drives that require pre-boot authentication, even when the OS is unavailable (for example, if the OS is inoperable or software agents are missing). Remotely manage data security settings even when PC is powered down.
- **Out-of-band management** even in secure environments, such as 802.1x, PXE, Cisco SDN*, and Microsoft NAP* environments.
- **Hardware acceleration for AES-NI encryption,** to off-load some of the performance burden of encryption from the processor.[8]
- **Intel® Trusted Execution Technology**[19] (Intel® TXT), which uses a hardware-rooted process to establish a root of trust, allowing software to build a chain of trust from the "bare-metal" hardware to a fully functional VMM. Intel TXT also protects secrets (security credentials) during power transitions. For more information about Intel TXT, visit www.intel.com/technology/security.
- **Hardware-assisted virtualization** to help secure PCs and support emerging use models, including multiple images, shared PCs, legacy OS support (such as for Windows XP mode in Windows 7), application and OS streaming, and virtual "containers."

Note: *IT can take advantage of hardware-assisted Intel® Virtualization Technology (Intel® VT) to improve performance for users running a legacy OS (for example, Windows* XP) in Windows 7.*

Advanced layers of defense for PCs with a new Intel® Core™ vPro™ processor



1 **Support for 802.1x, Cisco NAC,* and Microsoft NAP***
to enable remote out-of-band management even in an environment with full Cisco SDN or Microsoft NAP security.

2 **Programmable filters**
examine network traffic and rate-limit-traffic, port-isolate the system, or cut off the data path when a threat is recognized.

3 **Visibility of third-party security applications**
through hardware-based agent presence checking ("heartbeats") to make sure security agents and other critical applications stay active.

4 **Persistent, protected memory**
helps prevent unauthorized access to critical system information.

5 **Intelligent protection from loss or theft by disabling the PC and/or data**
through local timer expiry, excessive login attempts, and/or "poison pill" responses, including through virtually instant remote notification via a 3G modem if a suspected theft is in progress.

6 **Hardware-assisted virtualization**
of memory and processor resources for PCs, and Intel® TXT helps create secure virtual environments.

Figure 3. New layers of defense. Hardware-based security capabilities offer new layers of intelligent, client-side defense to fortify the PC against critical threats, loss, or theft. Intel® vPro™ technology – including Intel® Active Management Technology (Intel® AMT) and/or Intel® Anti-Theft Technology (Intel® AT) – must be activated in order for IT to take advantage of these intelligent security features.

These new layers of defense make it easier to identify attacks faster on both wired and wireless systems, and stop them more effectively before they begin to spread.

Intel® Anti-Theft Technology (Intel® AT)

One of the new features in PCs with a new 2010 Intel Core vPro processor is Intel Anti-Theft Technology. Intel AT provides IT with a set of programmable hardware-based triggers and "poison pill" features 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.

Poison pill responses can be:

- Local and self-administered, based on an IT-defined trigger. This allows the laptop itself to deliver a local, self-initiated defense, even when it is outside the corporate firewall or disconnected from the network. For example, IT can specify policies that disable the PC based on password activation and/or time-out of a "rendezvous" timer (the timer checks in with IT's central server).
- Remote and administered by IT, based on an alert or upon receiving a call from the user (for example, that the laptop was lost while traveling).

IT can use flexible policies to specify that the poison pill:

- Disable access to encrypted data by deleting encryption key components or other cryptographic credentials required for access to data.
- Disable the PC so it cannot boot the OS, even if the hard drive is replaced or reformatted.
- Disable both the PC and access to encrypted data. IT can use the poison-pill feature to delete or disable critical security elements of encryption keys in order to help prevent access to the keys and make data unretrievable. Even if the hard drive is then transferred to another laptop, the data can still be protected.

For example, IT could define a trigger for critical machines, such as a financial officer's laptop, so that if the system does not connect to the central server every day, access to the system is disabled. If the laptop is reported lost, an IT administrator can flag the system in a central database. The next time the laptop connects to the Internet, it calls home using in-band communication and synchronizes with the central server. When Intel AT receives the server's notification that the laptop has been flagged as lost or stolen, Intel AT disables the PC and/or access to data, according to IT policy.

Easy reactivation and full system recovery

Reactivation from a lock-down can be rapid and easy, using either a local passphrase or a recovery token generated by IT.

- Local pass-phrase, which is a strong password preprovisioned in the laptop by the user. The user enters this passphrase in a special pre-OS login screen in order to reactivate the system.

- Recovery token, which is generated by IT or the user's service provider via the theft management console (upon request by the end user). The one-time recovery token is provided to the user via phone or other means. The user then enters the passcode in a special pre-OS login screen in order to reactivate the system.

Both methods return the PC to full functionality, and both offer a simple, inexpensive way to recover the laptop without compromising sensitive data or the system's security features.

Intel AT must be enabled (on) in order for IT to take advantage of these intelligent security features.

Industry support and software development

Intel AT integrates with existing theft-management solutions. ISVs who support Intel AT include Absolute Software Corporation and PGP, and additional security ISVs are planning to offer solutions in 2010.

In order to deploy an Intel AT solution, a service provider or ISV with Intel AT capabilities is required. A new 2010 Intel Core vPro processor includes an SDK and documentation for ISVs and service providers to help test and validate their designs for Intel-AT-capable products.

Hardware-based acceleration for encryption

One of the performance burdens of higher security is the encryption and decryption of the hard drive upon every access. This has become a bottleneck to performance, and many IT departments have not used encryption protection because of the performance trade-off.

One of the encryption standards adopted by the U.S. Government is AES (Advanced Encryption Standard).[24] A new Intel Core vPro processor now includes new hardware-based CPU instructions (AES-NI, or Advanced Encryption Standard New Instructions) for AES.[8] These instructions are designed to consolidate the AES mathematical operations, off-loading them from the processor to improve security (harden cryptography software) and help speed up applications that use the AES algorithm. For example, software developers can write to these AES-NI instructions to off-load encryption processing – such as AES rounds and schedules for key generation – into hardware. This not only improves performance, but improves protection against advanced forms of cryptanalysis.

- Recent benchmarks compared a new 2010 Intel Core i5 processor-based PC to an installed-base with a 3-year-old Intel® Core™2 Duo processor E6400[Δ]-based PC. The benchmarks showed that protection of sensitive data can be up to 3.5x faster on a new Intel Core i5 processor-based PC.[11]

A new 2010 Intel Core i5 vPro processor with AES-NI support can be used to improve performance for systems that use whole-disk encryption and file storage encryption. ISVs already planning support for AES-NI include PGP, McAfee, Microsoft (as part of BitLocker* in Windows 7), and WinZip.

Push updates down the wire — regardless of PC power state

There are several methods in use today to wake a PC in order to push out an update, but those methods are not usually secure or reliable, or they work only when the OS is running properly. In contrast, a new Intel Core vPro processor includes a secure, encrypted power-up capability that helps technicians ready systems for updates. This helps IT organizations substantially speed up patching and ensure greater saturation for critical updates and patches.

With Intel vPro technology, technicians can:

- Remotely power up laptop and desktop PCs from the IT console, so updates can be pushed even to machines that were powered off at the start of the maintenance cycle.
- Deploy more updates and critical patches off-hours or when it won't interrupt the user.
- Check a PC's software version information, .DAT file information, and other data stored in nonvolatile memory, and find out if anything needs updating without having to wake or power up a PC.
- Help lower power consumption for businesses, by powering PCs off when not in use, and remotely and securely powering them up off-hours only for the update or patch (or other service).

These capabilities allow IT administrators to automate more security processes. In turn, this can help IT administrators establish a more secure, better managed environment.

Greater automation for compliance with corporate policies

With the ability to remotely access PCs regardless of power state or OS state, IT administrators can automate more processes, including update, remediation, and management processes. For example, if a polling agent discovers software that is out of date, the third-party management application can automatically take a software inventory, port-isolate the system temporarily, and then update the system. The management application can then remotely return the system to its previous power state: on, off, hibernating, or sleeping. This can help administrators eliminate many of the deskside visits and service depot calls traditionally required for updates, critical patches, and remediation, and help reduce risks to the network.

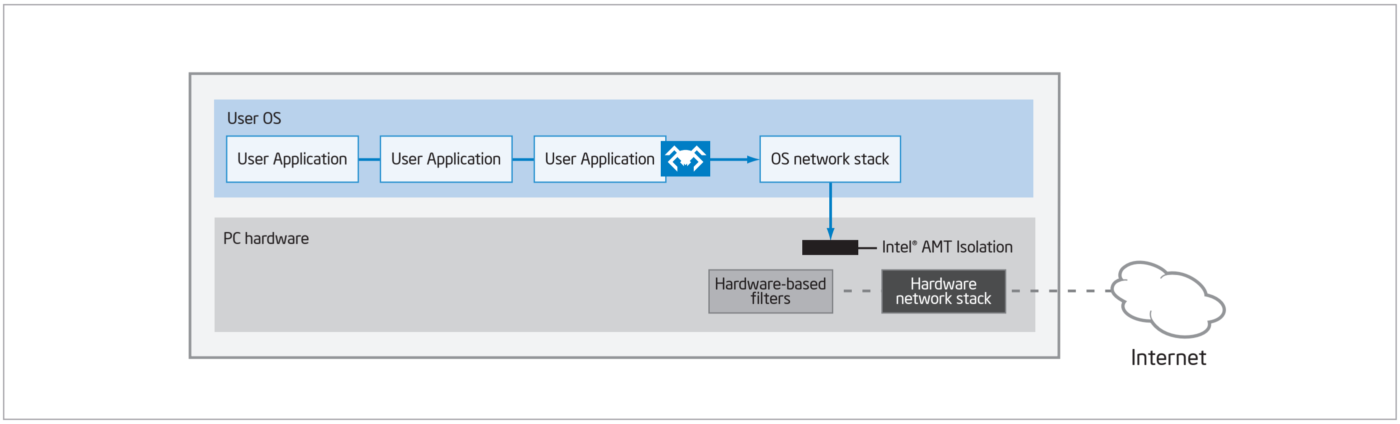


Figure 4. System defense filters inspect network traffic. A PC with a new Intel® Core™ vPro™ processor can port-isolate itself or cut off its own network data path to quarantine itself when suspicious behavior is recognized even if its OS is not available to help prevent threats from spreading to the network.

Filter threats and isolate PCs automatically based on IT policy

Laptop and desktop PCs with a new Intel Core vPro processor include programmable filters that monitor inbound and outbound network traffic for threats. IT managers can use third-party software to define the policies that will trigger hardware-based isolation of a PC.

Both laptops and desktop PCs with a new Intel Core vPro processor use programmable, hardware-based filters for examining packet headers for suspicious behavior. Desktop PCs also include additional hardware-based filters that monitor the rate of outbound traffic to help identify suspicious behavior, including both fast-moving and slow-moving worms.

Both laptop and desktop PCs also include built-in isolation circuitry (see Figure 4). When a threat is identified, a policy and hardware-based "switch" can:

- Isolate the system by specific port(s) to halt a suspicious type of traffic.
- Disconnect the network data path to the OS (the remediation port remains open) to contain threats more quickly.
- Rate-limit network traffic to give a technician more time to investigate a threat.

During a quarantine, the isolation circuitry disconnects the PC's network communication via hardware/firmware at the software stack in the OS. This is a more secure disconnect than traditional software-based isolation, which can be circumvented by hackers, viruses, worms, and user tampering.

Automated, continual checking for agents

Traditionally, IT organizations have used serial polling to verify the presence of security agents (or other business-critical applications). Because this method can saturate the network with healthy heartbeats (restricting the bandwidth available for productive traffic), IT organizations often poll for compliance only once or twice a day – if that often.

In contrast, laptop and desktop PCs with a new Intel Core vPro processor 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 can check in with the Intel Management Engine at programmable intervals, to confirm that the agent is still active. Each time an agent checks in, it resets its timer. If an agent hasn't checked in before the timer goes off, the agent is presumed removed, tampered with, or disabled. The Intel Management Engine then automatically and immediately logs the alert and notifies (if specified) the IT console.

With hardware-based heartbeats, IT administrators no longer need to wait for multiple polls to identify a potential problem. The PC itself helps improve the reliability of presence checks and reduce the window of software vulnerability. And, these "healthy" heartbeats never leave the PC. Only when there is a problem is an alert sent across the network, so your network isn't flooded with healthy heartbeat signals, and you still receive rapid notification of problems. For wireless laptops, agent presence checking is enabled even when operating outside the corporate network through a host OS-based VPN. This gives IT administrators greater visibility of these highly mobile and traditionally unsecured assets.

Combined with the remote power-up capability, the entire process of checking and reinstalling missing agents can also be automated, improving compliance further and saving additional resources.

Receive alerts even if a system is off the corporate network

PCs with a new Intel Core vPro processor have policy-based alerting built into the system. IT administrators can define the types of alerts they want to receive. Although all alerts are logged in the persistent event log, IT administrators can receive only the alerts they want. In this way, alerts that are not as critical do not add substantially to network traffic.

Alerting within the corporate network

Since alerting uses the OOB communication channel, IT administrators can receive critical notifications from PCs within the corporate network out-of-band, virtually anytime, even if the OS is inoperable, hardware has failed, or management agents are missing.

Alerting from outside the corporate network

IT can even receive notifications from a PC (awake and OS operable) that is connected to the corporate network through a host OS-based VPN or when connected via wired or wireless LAN on an open network outside the corporate firewall. IT administrators can now be notified rapidly and automatically when a system falls out of compliance, hardware is about to fail — sometimes even before users know they have a problem, or applications hang.

Out-of-band management even with 802 1x, Cisco SDN, and Microsoft NAP

In the past, IT administrators often felt they had to choose between using out-of-band management and maintaining full network security with 802.1x, Cisco SDN, or Microsoft NAP. With the latest PCs with a new Intel Core vPro processor, network security credentials can be embedded in the hardware. This includes an Intel® Active Management Technology[1] (Intel® AMT) posture plug-in, which collects security posture information (such as firmware configuration and security parameters), and the Intel AMT Embedded Trust Agent.

This capability allows the 802.1x authentication or the Cisco, or Microsoft posture profile to be stored in hardware (in protected, persistent memory), and presented to the network even if the OS is absent. The network can now authenticate a PC before the OS and applications load, and before the PC is allowed to access the network. IT administrators can now use out-of-band management for maintenance, security, management, or PXE purposes, while still maintaining full network security, including detailed, out-of-band compliance checks.

This capability also allows IT administrators to use their existing PXE infrastructure within an 802.1x, Cisco SDN, or Microsoft NAP network. The result is better security for PCs and a more reliable network, regardless of the PC's OS state, application state, or the presence of management agents.

Intel® Trusted Execution Technology (Intel® TXT)

The new generation of laptop and desktop PCs with a new Intel Core vPro processor include Intel Trusted Execution Technology (Intel TXT). Intel TXT helps build and maintain a chain of trust from hardware to a Virtual Machine Monitor (VMM). This helps to protect information in virtualized environments from software-based attacks. For more information about Intel TXT, visit www.intel.com/technology/security/.

Faster, easier remote manageability helps reduce costs

PCs with a new Intel Core vPro processor make it even easier to reduce maintenance costs. Built-in capabilities in these PCs include remote configuration, diagnosis, isolation, and repair of PCs, even if systems are unresponsive. Remote, automated manageability features – including new, hardware-based KVM Remote Control[2] in PCs with a new Intel Core i5 vPro processor (and select Intel Core i7 vPro processor-based PCs) – make PC upkeep easier even for complex issues, and help keep service costs low while improving user productivity. The all new 2010 Intel Core vPro processor family includes other new features, such as PC Alarm Clock. IT managers can also quickly upgrade to Windows 7 remotely and overnight, minimizing disruptions to users and without losing access to legacy applications. Once Intel vPro technology is activated, IT administrators can take advantage of these built-in remote manageability capabilities.

Remote upgrades save IT and user time

PCs with a new Intel Core vPro processor make it easier to upgrade OSs and applications remotely and automatically. For example, IT can remotely upgrade to Windows 7 at night, regardless of the initial power state of the PC, and save users up to 40 minutes or more by performing the process off-hours.[5]

Resolve more problems remotely

One of the most critical IT needs is a greater ability to remotely resolve PC problems, especially when a laptop or desktop PC's OS is down or hardware has failed. According to industry studies, deskside and service-center calls make up only a small percent of PC problems in a typical business, but they take up the majority of the budget. In fact, the cost of a deskside visit is seven times the cost of a remote problem resolution.[25]

Problem-resolution capabilities in PCs with a new Intel Core vPro processor can help IT managers reduce deskside visits by up to 56%[12] through features such as:

- **Remote/redirected boot,** through integrated drive electronics redirect (IDE-R). IDE-R allows authorized IT technicians to remotely boot a PC to a clean state, or redirect the boot device for a problem PC to a clean image on local storage, on a CD at the help desk, or to an image on another remote drive. There is no need for a deskside visit or service depot call to resolve many boot, OS, and software remediation problems.
- **Console redirection,** through Serial-Over-LAN (SOL). Technicians now have remote keyboard control of a PC outside of standard OS control, allowing them to perform tasks such as editing BIOS settings from the service center – without user participation.
- **KVM Remote Control,**[2] a new hardware-based feature that works for wired and wireless PCs (that have integrated Intel HD Graphics) both inside and outside the corporate firewall. KVM allows an authorized IT technician to remotely control the keyboard, video, and mouse of a remote PC, as if they were deskside, at the PC itself. This feature helps IT remotely resolve the most complex software failures and eliminates the need for a separate, costly data-center KVM switch.
- **PC Alarm Clock,** a new hardware-based feature that lets IT schedule a PC to wake itself from any powered down or sleep state. The PC can then perform tasks based on IT policy, such as initiate a secure call to the service center for automated, off-hour services – even if outside the corporate firewall. The feature allows independent software vendors (ISVs), such as McAfee, to enable IT-scheduled product updates even for businesses that don't have an IT console.
- **Out-of-band, policy-based alerting,** so the PC can send alerts and Simple Network Management Protocol (SNMP) traps to the management console anytime, based on IT policies.
- **Fast call for help** for wired or wireless systems, even beyond the firewall. Helps users avoid the costly downtime of shipping PCs back to IT to be fixed. If a PC crashes, a user can phone IT for help and, during the boot process, press a specific key to securely connect the PC to IT for troubleshooting. IT can then take over via remote console redirection or through hardware-based KVM Remote Control.
- **Persistent event logs,** stored in dedicated memory (not on the hard drive) so the information is available anytime. IT technicians can now access the list of events that occurred even before a hardware or software problem was noticed, including events that occurred before a PC connected to the network.
- **Always-available asset information,** stored in dedicated, protected memory. This information is updated every time the system goes through power-on self test (POST).
- **Access to preboot BIOS** configuration information anytime. Diagnostics and repair processes can also be securely performed on wired and wireless PCs – even outside the corporate firewall.[17]

IT technicians can now remotely:

- Access asset information anytime, to identify "missing" or failed hardware components, and verify software version information.
- Guide a PC through a troubleshooting session without requiring user participation – even for complex issues such as BIOS issues, blue-screens, freezes, patch failures, and other "edge" software issues.
- Reboot a system to a clean state, or redirect the PC's boot device to a diagnostics or remediation server (or other device).
- Watch as BIOS, drivers, and the OS attempt to load, to identify problems with the boot process.
- Update BIOS settings, identify BIOS versions, or push a new BIOS version to the PC to resolve a particular problem.
- Upload the persistent event log to identify the sequence of events (such as temperature spikes or an unauthorized software download) that occurred before the system failed.
- Push new copies of missing or corrupted files, such as .DLL files, to restore an OS.
- Rebuild the OS or fully reimage the hard drive remotely.
- Perform OS migrations and application upgrades, and troubleshoot upgrade problems remotely.
- Power-manage PCs more effectively to lower power consumption and reduce energy costs.
- Schedule a local wake from a full power down, to prepare systems for incoming workers.

If a system becomes inoperable, a technician can use secure remote and/or redirected boot or a secure PXE boot to change the system's boot device to a CD or to an image located on a remote network drive – without leaving the service center. The technician can then use secure console redirection to remotely guide the PC through a troubleshooting session. If a user application has become corrupted, the technician can remotely reimage the user's hard drive and restore user data from known-good files, overwriting corrupt or problem files. The user is back up and running as quickly and efficiently as possible without a service depot call or deskside visit.

Many case studies have shown how PCs with a new Intel Core vPro processor can help substantially reduce IT service costs for problem resolution and software updates (refer to the Intel Web site, www.intel.com/references/ecm/index.htm, for case studies in various industries).

Accurate, remote discovery and inventory for wired or wireless systems

On average, up to 20% of a business's PCs are not in compliance at any given time.[12] Adding to this problem is the difficulty in getting accurate software inventories. For example, software inventories for laptops are often up to 11% inaccurate.[12] One problem with inaccuracies caused by underreporting is that it may also expose corporate officers to liabilities, such as noncompliance with Sarbanes-Oxley and other government regulations. There is a critical need for accurate system inventories, especially for PCs that are powered off or whose OS is inoperative.

PCs with a new Intel Core vPro processors give IT "always-available" access to system information. This makes it easier for IT to perform accurate, remote discovery and inventory of wired and wireless PCs both inside and outside the corporate firewall:

- UUID, which persists even across reconfigurations, reimaging, and OS rebuilds.
- Hardware-asset information, such as manufacturer and model information for components. This information is automatically updated each time the system goes through POST.
- Software-asset information, such as software version information, .DAT file information, pointers to database information, and other data stored by third-party vendors in the persistent memory space provided by Intel vPro technology.

When managing PCs with a new Intel Core vPro processor, IT technicians can:

- Write asset and other information (or pointers to asset information) into protected memory.
- Poll both wired and wireless systems in any power state for hardware- and software-asset information stored in protected memory – an out-of-band (outside the OS) process that is up to 94% faster than performing a manual inventory.[12]
- Identify noncompliant PCs even if management agents have been disabled.
- Power up PCs that are off to perform inventory tasks, push replacement management agents to the system, and remotely power the PC back to the state in which the user left it.
- Push replacement agents to a wired or wireless PC, to bring it back into compliance before further network access is allowed even if management agents are missing.

The capabilities help reduce time-consuming manual inventories, saving significant costs in labor. Unused software licenses can also be appropriately reallocated to other resources, while hardware assets can be better utilized and warranties better managed. At the same time, businesses can be more confident that their audits are in compliance with government regulations.

KVM Remote Control lowers support costs

In spite of improved remote management tools, almost 20% of problem tickets still require that users help resolve the problem.[26] Even with the use of the remote management capabilities of Intel vPro technology, the complexity these "edge" failures have traditionally meant that a technician must still make a deskside visit or ask users to help resolve the problem.

A PC with a new Intel Core i5 vPro processor with Intel integrated graphics delivers hardware-based KVM Remote Control.[2] Unlike software-based KVM, hardware-based KVM Remote Control allows an authorized IT technician to more securely see and control PCs reliably through all states to resolve software failures – even beyond the corporate firewall. With KVM Remote Control, technicians have full interactivity with the PC to remotely resolve complex issues with BIOS, startups/shutdowns, blue screens, OS freezes, disk failures and network software issues.

With KVM Remote Control, technicians can now:

- Remotely reduce the IT effort required for manual failure resolution of patch deployment failures by up to 84%.[26]
- Remotely reduce manual IT effort required for major software malfunctions by up to 96%.[26]

Typical savings from KVM Remote Control

Studies show that PCs with a new Intel® Core™ vPro™ processor with KVM Remote Control[2] (keyboard video mouse) can reduce problem resolution time by 20% for complex software issues.[26] These include "edge" issues, such as major software failures and patch deployment failures.

For example, a model company with approximately 30,000 PCs can realize savings of up to $1.4 million in IT service costs over 3 years, by implementing the remote management capabilities of Intel® vPro™ technology for problem resolution.[26] Adding hardware-based KVM Remote Control[1] can save such a company an additional $133,000 in IT service costs and $97,000 in user productivity.[26] That is conservatively equivalent to about 2,400 IT hours at $55 per hour, and approximately 2,400 hours in user productivity.[26]

General improvements in phone-based support can help business realize further benefits in user productivity – more than $740,000 in savings.[26] For a company with 30,000 PCs, the overall savings over 3 years from using the capabilities of a new Intel Core vPro processor with KVM Remote Control can be over $1.6 million.[26]

Now that IT administrators have KVM Remote Control built into the PC's hardware, they also have the built-in ability to remotely resolve even complex edge problems. IT administrators can now increase efficiencies and lower manual labor costs, without increasing service costs in their IT environment.

PC Alarm Clock – local wake from any sleep state

A new feature in PCs with a new Intel Core vPro processor is PC Alarm Clock. PC Alarm Clock is a secure, policy-based client-side (local) scheduled power-on.

Two forms of this feature – BIOS timers and ACPI interfaces – exist in the market today. However, BIOS timers are not universally available or easy to configure, and ACPI interfaces allow wake only from S3 and S4. In contrast, a new Intel Core vPro processor's alarm-clock feature allows a PC to wake from any powered-off state or sleep state, including from a full power down. Also, because this is client-side intelligence, no network is required. IT can use this capability to schedule tasks even for PCs that are not on the network.

Potential uses for PC Alarm Clock include waking PCs:

- To ensure that virus scans run according to policy
- To ensure PCs pull and apply scheduled updates from the central server
- To execute periodic backups
- In anticipation of start of work
- To run periodic disk defragmentation

IT administrators can now be more confident that maintenance and key security tasks are performed regularly, even for laptop PC users who are not always on the corporate network.

Power down at night and save on power bills[15]

Businesses are increasingly concerned about power consumption. Battery life in laptops is one consideration. Just as important are on-site energy costs – a significant operating expense. In addition, with a global presence, businesses are faced with increasingly stringent energy regulations around the world, and an ever-increasing corporate focus on environmental responsibility.

ROI studies, such as from the University of Plymouth, have shown that companies can reduce power bills by up to 50% by powering down PCs during off-hours.[15] IT technicians simply use the built-in remote power up/down capability of a new Intel Core vPro processor to remotely power systems down during off-hours. They can use the same secure capability to remotely power systems back up from the service center. This lets technicians minimize power consumption, but still maintain access to the PC to perform off-hours work – or simply ready the PC for the next work shift.

Positive ROI in 9 months – just from reducing power consumption[15]

Unmanaged PCs waste energy. Simply by using the secure remote power up/down capability, some companies have recouped their investment in a PC with a new Intel® Core™ vPro™ processor in as little as 9 months.[15] By implementing other capabilities of a new 2010 Intel Core vPro processor, businesses can realize further savings.

Actual customer savings from moving to a PC with a new Intel® Core™ vPro™ processor

When managing PCs with a new Intel Core vPro processor, businesses can experience exceptional performance while lowering power consumption and power bills.

- **Calgary Health Region:** Total projected savings of $276,800[27]
- **Cleveland Clinic:** Power savings 66% over 4 years[28]
- **EDS Call Center:** Power-efficiency improvement of 25%[29]
- **CSK (Japan):** Saved approximately $61,000 in energy costs[30]
- **State of Indiana:** Projected savings of over $1.4 million in 4 years[31]

Virtualization enables flexible computing models

Virtualization partitions a PC so that it can run separate operating systems and software in each partition. This allows one PC to act as many, and takes advantage of the multi-core processing power available in PCs with a new 2010 Intel Core vPro processor. Virtualized applications, streamed OSs, and virtual user environments are especially useful in data centers, where users share PCs, and where IT must support different builds based on user IDs (see Figures 5 and 6).

To enable virtualization for alternate computing models, the all new 2010 Intel Core vPro processor family includes Intel® Virtualization Technology[9] (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.

Usage models

Virtualization can be used to support next-generation, emerging, and traditional usage models for OSs and applications:

- Delivery of managed applications on-demand
- Delivery of managed desktop images
- Isolation of execution environments
- Traditional, multi-OS usage model

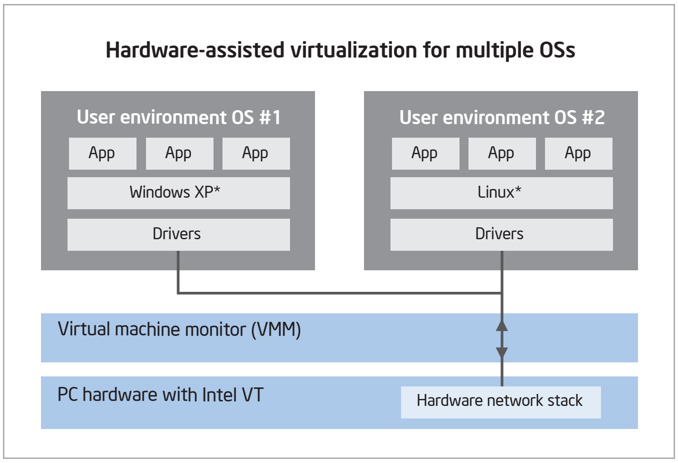


Figure 5. Hardware-assisted virtualization. Virtualization provides IT with isolated, secure spaces in which to abstract or stream OSs and applications Both next-generation and traditional virtualization is supported on laptop and desktop PCs with a new Intel® Core™ vPro™ processor.

Virtualization: Streaming

Streaming refers to sending software (an OS or applications) over the network for execution on the PC (see Figure 7 on the next page). During streaming, the software is sequenced, then divided into blocks and prioritized, and then placed in specific order for streaming. This allows the software to launch and begin operations on the PC even before all the code is streamed, so that users still have the responsiveness and performance of local execution. For IT, the advantage is that the OS and/or applications can be managed centrally, and standardized policies can be set to govern data storage. Since streamed software executes on the client, IT does not have to absorb the large datacenter build-out required by server-side compute models. Also, users enjoy the more responsive application experience of local software execution.

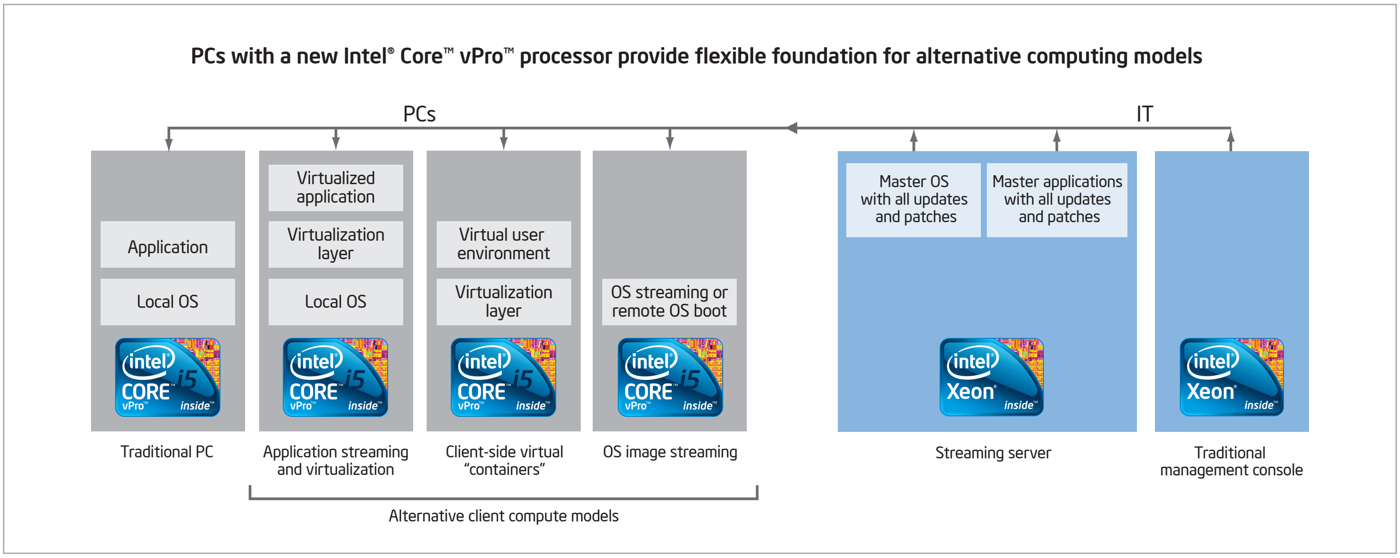

PCs with a new Intel® Core™ vPro™ processor provide flexible foundation for alternative computing models
PCs
IT
Application
Local OS
Virtualized application
Virtualization layer
Local OS
Virtual user environment
Virtualization layer
OS streaming or remote OS boot
Master OS with all updates and patches
Master applications with all updates and patches
intel CORE i5 vPro inside
intel Xeon inside
Traditional PC
Application streaming and virtualization
Client-side virtual "containers"
OS image streaming
Streaming server
Traditional management console
Alternative client compute models

Figure 6. The all new 2010 Intel® Core™ vPro™ processor family enables alternate computing models that support different user needs. By centralizing OSs and applications, IT can minimize the burden of maintaining multiple builds, reimaging, and upgrading systems, and improve security at the same time.

- **OS and application streaming:** the OS and applications are not installed locally. Instead, the OS and applications are streamed to the PC across the network. Critical application data can be stored at the data center, traditional problems with OS and/or application corruption are remediated by simply re-streaming the "gold" software image. Security, patching, and other IT services are also simplified, since they are performed only on the software image at the data center.
- **Application streaming:** the OS is installed locally, but the applications are streamed from the datacenter to the user on-demand. Data can be stored locally or at the data center, based on IT policy. Streaming only the applications reduces the network load, as opposed to streaming both the OS and applications. Also, applications can be cached for off-network use on laptops. The terms "application streaming" and "application virtualization" are sometimes used interchangeably, but they are different. Streaming is the technique to deliver applications over the network.

Application virtualization is a technology that abstracts the application from the OS. Virtualized applications have full access to OS resources, but do not install themselves in the OS registry or system files. This can reduce many of the management issues and application conflicts that result from traditional installation. PCs with a new Intel Core vPro processor support both OS streaming and application streaming. Application streaming products are available from several software vendors.

Virtualization: Virtual containers

Virtual containers are self-contained virtual machines on the local PC. Virtual containers let you create individual, isolated work environments for a variety of scenarios. You can also use a managed virtual container to fully isolate and protect corporate data from personal data. This would allow you to increase security as necessary for sensitive information without frustrating users in their personal use of the system.

With virtual containers, the PC has at least one fully featured OS, and one or more additional, environments that are self-contained and used for specific purposes. For example, you could:

- Use virtual containers to separate locked-down corporate applications from more loosely-governed personal applications.
- Deploy a highly managed, limited-access image to a contractor or temporary employee.
- Allow employees to bring their own laptops into the office and use a managed virtual container to provide their applications. The virtualization software would abstract differences in the hardware, reducing the burden of validating the corporate image against the myriad of hardware combinations employees might be using.

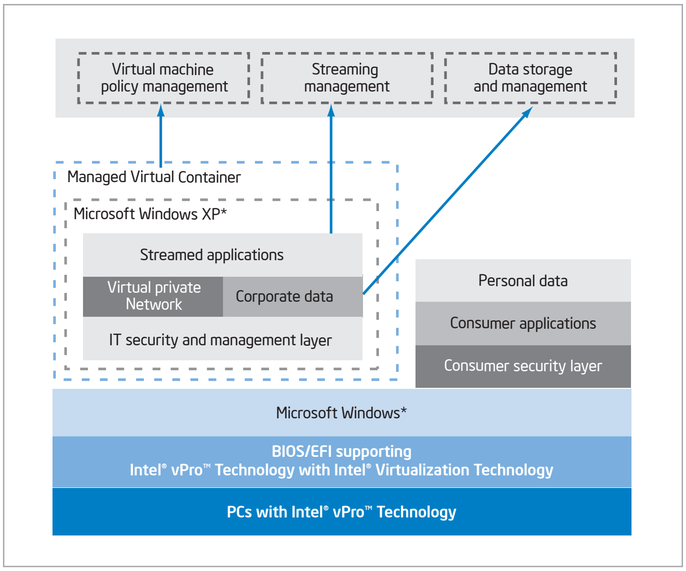

Virtual machine policy management
Streaming management
Data storage and management
Managed Virtual Container
Microsoft Windows XP*
Streamed applications
Virtual private Network
Corporate data
IT security and management layer
Personal data
Consumer applications
Consumer security layer
Microsoft Windows*
BIOS/EFI supporting Intel® vPro™ Technology with Intel® Virtualization Technology
PCs with Intel® vPro™ Technology

Figure 7. Application streaming. Intel® Virtualization Technology supports OS and application streaming, a next-generation standard practice for managing, securing, and delivering applications to users.

Virtualization: Multiple OSs (traditional model)

The traditional model of virtualization gives the user access to multiple fully functional OS environments running in separate virtual machines. For example, the PC could have Microsoft Windows XP* and Linux* running side-by-side. This type of virtualization is also seeing significantly improved performance from the recent advances in Intel VT.

Traditional virtualization has typically been used:

- By software developers and support staff who need to work in more than one OS environment but do not want more than one PC on their desk.
- For OS migration, by keeping unportable legacy applications running in an earlier OS, while moving the rest of their applications over to Windows 7.

Traditional virtualization usually requires that you install a VMM software package from a vendor like VMware or Parallels, then build OS and applications images on top of the VMM software. Intel VT is enabled today in VMM packages from vendors such as VMware and Parallels.

Intel® Virtualization Technology (Intel® VT) features

Virtualization can be achieved entirely with software – but this approach has traditionally had several challenges, including too much overhead, poor performance, and unenforced isolation (a security issue).

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 third-party vendors to build lightweight VMMs. It also helps make virtualization more efficient and secure in general, and significantly improves performance – to near native levels or better, depending on the virtualization model.

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 VMM's 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 VMM. Intel 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 a fully functional VMM.[19] Using hash-based measurements protected by hardware, Intel TXT can detect changes to the VMM during its launch, which helps ensure that virtual machines will run as expected. The process allows the VMM 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, removes the secrets, then allows a normal boot process. (Secrets are not removed by Intel TXT after a normal protected partition tear-down. Removal of secrets under normal shutdown is handled by the VMM.) With Intel TXT, secrets that have not traditionally been protected before the OS and security applications are launched, are now protected even after improper shut-downs and in the traditionally vulnerable state before the OS and applications load once again.

Intel TXT is available in the latest laptop and desktop PCs with a new Intel Core vPro processor.

Intel® VT is compatible with other technologies

Standard memory, storage, and graphics cards work with Intel VT.[5] The latest laptop and desktop PCs with a new Intel Core vPro processor can also run most off-the-shelf OSs and applications without IT administrators having to perform special installation steps. The hardware-based virtualization technology is also designed to work with and complement other advanced security and management technologies from Intel, such as Intel AMT.

Key benefits of virtualization

PCs with hardware-based virtualization offer IT benefits in:

- **Flexibility.** Support both traditional and alternative compute models on a single standardized PC build.
- **Legacy support.** Run legacy applications seamlessly in a user environment, and still maintain high security in a separate virtual environment through the use of Intel VT and Intel TXT.
- **Hardware-based security.** Take advantage of hardware VM isolation, VMM launch verification, and memory protection for secrets (via Intel TXT) provide a robust, isolated, tamper-resistant environment for streaming an OS and/or applications into virtual containers on the PC from a centralized management server.
- **Productivity.** Provide local execution for laptop PCs who are off the network, while streaming applications or OSs to other users who are network connected.
- **Performance.** Great user experience with local, hardware-level acceleration for local processing and video.
- **Leading ISV support** from Citrix, VMWare, Microsoft, and Symantec.

Table 5. Virtualization support in laptop and desktop PCs.

Advanced technology	Offers	All new 2010 Intel® Core™ vPro™ processor family
Intel® VT[9]	Traditional client virtualization, which isolates and supports multiple OSs on a single PC	Yes
Intel® VT for Directed I/O	Virtualization of I/O hardware	Yes
Support for virtual containers	Temporary virtual machines ("containers") that support virtual user environments and isolate streamed OS and applications	Yes
Intel® TXT[19]	Trusted launch of the VMM and protection of secrets during proper or improper shutdown	Yes

Go mobile – cut costs and improve productivity

Employees are increasingly required to access enterprise applications while away from the office. Now that more powerful, seamless tools are available – such as video conferencing, streaming OS virtualization, and real-time application streaming – working off-site has become easier than ever.

Businesses are realizing significant benefits in going mobile:

- Improved productivity while working outside the office – on average, mobile users are more productive by 51 minutes a day, or up to 15% to 20%.[14]
- Ability to view and respond to critical or urgent issues in real-time.
- Reduce workforce support costs by 40% or more.[14,32,33]
- Realize up to 98% positive ROI in 14 months simply by increasing adoption of laptops.[34]
- Reestablish operations and reconnect 60% faster to your company's intranet or the Internet via wireless laptops in the event of a disaster.[35]

In addition, mobile workers find it easier to balance work and life, eliminate commutes, and save fuel. The challenge for IT is to manage and secure those systems without a deskside or service center visit.

Wireless mobility

A new Intel Core vPro processor includes many features and capabilities to support a mobile workforce, including virtual location workforces and remote office LAN replacements. For example, laptops with a new Intel Core vPro processor include proven Intel® Centrino® wireless products. Users can choose between support for WiFi or support for WiFI with optional WiMAX.

- Reliable and predictable coverage – less likely to drop off in wireless speed.
- Access metro-wide networks beyond hot spots with Intel® Centrino® Advanced–N + WiMAX 6250.
- Intel® Centrino® Ultimate-N 6300 offers premium Wi-Fi, with up to 8x greater speed.[36]

Virtual location workforce

PCs with a new 2010 Intel Core vPro processor let businesses provide connectivity to employees working from home or in remote locations in covered areas. By implementing Mobile WiMAX, businesses can improve worker productivity and begin reducing employee support costs. (Mobile WiMAX must be supported by your service provider.)

Go mobile and take your savings to a new level

Cisco generated an estimated annual savings of $277 million in productivity after deploying more laptops, taking the company to new levels of efficiency and effectiveness.[37]

According to Information Week, "If everyone who could telecommute did twice weekly, the US could save 9.7 billions gallons of gas and $38.2 billion per year..."[38]

Remote office LAN replacement

Mobile WiMAX is the single, primary connectivity model in remote offices that do not have a LAN. Laptops with a new Intel Core vPro processor can eliminate the need for a LAN by allowing connectivity through WiMAX service. This can help businesses reduce infrastructure costs and employee support costs. (Mobile WiMAX must be supported by your service provider.)

Mobile metropolitan worker connectivity

PCs with a new Intel Core vPro processor also allow businesses to take advantage of Internet Service Provider (ISP) Mobile WiMAX services. In the ISP model, mobile employees connect at broadband speeds from remote locations. This can help businesses realize key benefits:

- Extend the manageability and security reach of IT for PCs with a new Intel Core vPro processor for mobile metropolitan workers and specialized devices, including tracking of assets.
- Improve sales-force access to real-time information for better customer support.
- Improve time-to-decision by providing real-time content access to decision makers when they are mobile.
- Improve time-to-support by providing support personnel with real-time access to experts anytime, anywhere.

When using PCs with a new Intel Core vPro processor, businesses can evaluate WiMAX as a mainstream solution and start taking advantage of the growing number of metros that offer WiMAX.

Responsive, energy-efficient intelligent performance

One of the key pain points in using older PCs is lack of performance – newer applications are not always responsive on older hardware. A new 2010 Intel Core i5 vPro processor can run business productivity applications up to 80% faster than a 3-year-old PC.[11] The new processors provide enough performance not just for today's applications, but also for future, heavily-threaded OSs and applications (see Table 6). In addition, the all new Intel Core vPro processor family can help improve productivity by automatically and intelligently adjusting to each user's needs. PC technology now adapts to your business – not the other way around.

Some of the performance and efficiency features of a new 2010 Intel Core i5 vPro processor include:

- Protect confidential data up to 3.5x faster.[11]
- Adaptable performance through new Intel Turbo Boost Technology.
- Up to 2x faster multitasking.[11]
- Up to 80 percent faster on business productivity applications.[11]

Energy Star compliance and energy efficient

The all new 2010 Intel Core vPro processor family is Energy Star complaint.[39]

These systems also take advantage of deeper processor sleep states and lower idle power. Intelligent power management allows idle cores to reduce their power consumption so that the system consumes only the power it needs based on actual user workload. For example, compared to a 3-year-old PC based on an Intel Core 2 Duo E6400$^{\Delta}$ processor, desktop PCs based on a new 2010 Intel Core i5 vPro processor are 30% more energy efficient.[11]

Intel® Turbo Boost Technology

Intel Turbo Boost Technology is an exciting new technology embedded in the all new 2010 Intel Core vPro processor family. This is an intelligent allocation of extra processing power to match the workload of the applications that need it most. If the processor is operating below its maximum power, current, and temperature specifications, Intel Turbo Boost can accelerate the processor – up to 20% faster – to provide additional performance for an application that needs more compute power.

In essence, Intel Turbo Boost identifies work load versus processor specification levels, and automatically allows processor cores to run faster than the base operating frequency. The maximum frequency of Intel Turbo Boost is dependent on the number of active cores in the processor. The amount of time the processor spends in the Intel Turbo Boost state depends on the workload and operating environment. With today's compute-intensive applications, this is a key technology to helps improve productivity for both existing and future applications.

Table 6. Intelligent, energy-efficient performance.

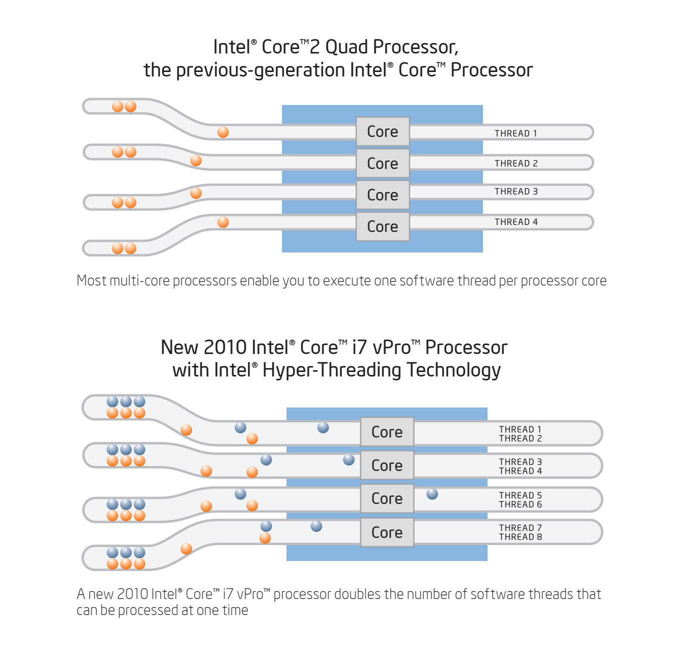
Select the right processor for the job	Processor delivers	Cores	Cache	Encryption support with AES-NI[8]	Intel® Turbo Boost[3]	Advanced multi-tasking via Intel® Hyper-Threading[6]	Intel® vPro™ Technology[1,4]
Intel® Core™ i7 vPro™ Processor	Intelligent security, remote manageability, and adaptive performance	4 Cores	Up to 8 MB	●	●	4 to 8 Threads	●
Intel® Core™ i5 vPro™ Processor		2 Cores	Up to 4 MB	●	●	4 Threads	●
Intel® Core™ i7 Processor	Performance for everyday business applications	2-4 Cores	Up to 8 MB	●	●	4 to 8 Threads	○
Intel® Core™ i5 Processor		2 Cores	Up to 4 MB	●	●	4 Threads	○
Intel® Core™ i3 Processor		2 Cores	Up to 4 MB	○	○	4 Threads	○

Intel® Hyper-Threading Technology

Intel HT Technology allows each processor core to work on two tasks at the same time. This typically doubles the number of threads being executed (see Figure 8). With Intel HT Technology, computational latency is reduced, and every clock cycle is used to its optimum potential. For example, while one thread is waiting for a result or event, another thread can execute in that core, minimizing down cycles.

With faster performance, users can get more accomplished in less time. This results in a more efficient use of processor resources – higher processing throughput – and improved performance on the multi-threaded applications of today and tomorrow. Businesses can now:

- Run demanding desktop applications simultaneously without slowing down.
- Reduce the burden of security applications that process in the background, minimizing their impact on productivity, yet still keep systems more secure, efficient, and manageable.
- Provide headroom for future business growth.


Intel® Core™2 Quad Processor,
the previous-generation Intel® Core™ Processor
Core
Core
Core
Core
THREAD 1
THREAD 2
THREAD 3
THREAD 4
New 2010 Intel® Core™ i7 vPro™ Processor
with Intel® Hyper-Threading Technology
Core
Core
Core
Core
THREAD 1
THREAD 2
THREAD 3
THREAD 4
THREAD 5
THREAD 6
THREAD 7
THREAD 8

Most multi-core processors enable you to execute one software thread per processor core

A new 2010 Intel® Core™ i7 vPro™ processor doubles the number of software threads that can be processed at one time

Figure 8. Intel® Hyper-Threading Technology allows each core to execute two threads at the same time. This can dramatically increase performance for heavily threaded OSs and applications, such as Microsoft Windows* 7 and Microsoft Office* 2007.

No more front-side-bus (FSB)

The all new 2010 Intel® Core™ vPro™ processor family no longer has a front-side bus (FSB). Instead, these processors enhance Intel® Smart Cache with a shared L3 (last level) cache that can be up to 8 MB in size.

In previous generations of Intel® Core™ processors, an external bi-directional data bus (the FSB) was used to keep instructions and traffic flowing quickly to the processor. However, as processors have grown more powerful and as the number of processing cores has increased, the FSB has become a limiting factor for the speed at which a microprocessor and its execution cores can access system memory.

The all new 2010 Intel Core vPro processor family eliminates this bottleneck by adding a new high-speed interconnect, and embedding an L3 cache into the microarchitecture. L3 cache is shared across all processor cores. Key benefits of L3 cache include more opportunities to take advantage of hyper-threading, and an increase in overall performance while reducing traffic to the cores. A new 2010 Intel Core vPro processor includes:

- New fully inclusive, fully shared up to 8 MB L3 cache – all applications can use the entire cache
- New L2 cache per core, for very low latency: 256 KB per core for handling data and instructions
- Same L1 cache as previous Intel® Core™ microarchitecture: 32 KB instruction cache, 32 KB data cache

For new 2010 Intel Core vPro processors, look for an L3 designation instead of an FSB number.

Specification	What it means	For best performance in the new generation of processors, look for:
Clock speed	Measures how fast a processor processes data.	Faster (higher number)
Intel® Smart Cache Technology	Level 3 cache, which is shared between the cores, speeds up data accesses and reduces data bottlenecks.	More (higher number)
FSB	An interconnect used in previous-generation Intel® Core™ processor-based PCs.	None (the FSB has been replaced with a new higher speed interconnect and shared L3 cache)
Intel® Turbo Boost Technology[3]	Dynamically accelerates performance up to 20% faster (if processor load allows) when faced with a demanding task.	Faster (higher number)
Multicore designation	The number of cores available for processing data. Multiple cores allows for faster multitasking and improved performance with multi-threaded applications.	More (higher number)
Intel® Hyper-Threading Technology[6]	The number of tasks that can be executed simultaneously.	More (higher number)

Simplify and speed up activation

The all new 2010 Intel Core vPro processor family allows secure, remote access and management of PCs even if the OS is inoperable, PC power is off, a hard drive has failed, or the PC is outside the corporate firewall. To maintain the proper level of security for these capabilities, it is important that IT administrators establish the security credentials for Intel vPro technology appropriately for activation in their service environment before configuring Intel vPro technology for remote management. IT administrators can choose the level of security and automation appropriate for their network environments.

General activation process

Activating Intel vPro technology in a PC with a new Intel Core vPro processor generally follows three steps: setup, configuration, and integration. Setup establishes the initial security credentials required for secure communication between the setup-and-configuration application (SCA) and Intel Active Management Technology (Intel AMT) on the target PC. (Intel AMT is part of Intel vPro technology.) Setup also establishes the initial network and operational parameters required to begin configuration.

Configuration is a self-initiated, automated step that depends on security credentials being in place. Integration means discovering and integrating a new Intel Core vPro processor-based PC into the management application. Once these steps are complete, Intel vPro technology is activated, and IT administrators can start taking advantage of the built-in intelligent security and remote manageability capabilities.

Methods to establish security credentials

A new Intel Core vPro processor supports different processes for setting up security credentials on the PC and management console. These processes allow IT to select the security level appropriate for their environment:

- One-touch manual: Manually enter key pairs into the PC and the management console.
- One-touch USB key: Keys can be generated on the management console and stored on a USB key. The USB key is then used to install the keys onto the PCs.
- Remote configuration: Setup of initial security credentials occurs automatically (the PC must be configured by the original equipment manufacturer (OEM) for remote configuration). Remote configuration requires a provisioning service, typically called a setup and configuration application (SCA). An SCA is required for both standard and advanced provisioning.

Activation models

A new Intel Core vPro processor supports three configuration models to allow for flexible activation:

- Basic configuration refers to a manual provisioning method useful for small businesses. This configuration method uses HTTP Digest for user authentication. There is no encryption applied to management traffic.
- Standard configuration provides enough security for most corporations. Client authentication is based on HTTP Digest, which requires a username and password. There is no encryption applied to management traffic.
- Advanced configuration provides the highest level of security features. This model allows IT to configure the PCs to use network access control standards such as 802.1x, Cisco SDN, and Microsoft NAP. This model also allows IT to configure the management traffic to be encrypted with TLS or mutual TLS. In addition, authentication can be managed by the Microsoft Active Directory* via Kerberos. PCs with a new Intel Core vPro processor allow IT to remotely configure these security options. Note that not all management console vendors provide support to configure all security options.

Ready for the future

Laptop and desktop PCs with a new Intel Core vPro processor help manufacturers deliver stable, standardized PCs. These PCs have with broad industry support and are ready for the heavily multithreaded OSs and applications of the future.

- 64-bit multi-core processor: PCs with a new 2010 Intel Core vPro processor handle today's OSs, and are ready for Windows 7, a heavily threaded architecture. Get the intelligent performance you need for Windows 7 when your business is ready to migrate.
- Performance for multi-threaded Office applications: New 2010 Intel Core vPro processors provide the performance needed for Microsoft Office 2007, including the adaptable performance for intense, always-on (by default) text-based search indexing, which is heavily multithreaded.
- 64-bit graphics support: PCs with a new 2010 Intel Core vPro processor have built-in 64-bit graphics for an outstanding Windows 7 Aero* experience. There is no need for a discrete graphics card with these laptop or desktop PCs.
- Upgrade to Windows 7 quickly, remotely, and overnight without losing access to your legacy applications, and save up to 40 minutes of end-user productivity per user with a new 2010 Intel Core vPro processor-based PC.[5]
- Support for legacy applications via Windows 7: IT can take advantage of hardware-assisted virtualization through Intel VT, to improve performance for users running a legacy OS (such as Windows XP) in Windows 7.

Stable, standards-based, and with broad industry support

To help the industry get the most from its technology investments, PCs with a new 2010 Intel Core vPro processor are:

- **Built on standards.** The all new 2010 Intel Core vPro processor family is built on industry standards to give you many choices in selecting OEMs and software vendors. Some of the standards upon which the new Intel Core vPro processor is built include ASF, XML, SOAP, TLS, HTTP authentication, Kerberos, DASH,* and WS-MAN.
- **Broadly supported by the industry.** The all new 2010 Intel Core vPro processor family is supported by major software vendors in security software, management applications, and business software. PCs with a new Intel Core vPro processor are available from leading, worldwide desktop and laptop PC manufacturers and are supported by major IT managed service providers.
- **Stable and simple.** The latest PCs with a new Intel Core vPro processor are available under the Intel® Stable Image Platform Program[18] (Intel® SIPP), so businesses can avoid unexpected changes that might force software image revisions or hardware requalifications. Intel SIPP for the new 2010 Intel Core vPro processors begins in February 2010, and extends for 15 months after that month. With Intel SIPP-compliant laptop and desktop PCs, IT can be more assured of having a stable platform that simplifies the deployment of new computing systems.

Wired or wireless: The intelligence of security and manageability on every chip

The all new 2010 Intel Core vPro processor family delivers cost-cutting efficiency and maximum productivity with the intelligence of hardware-assisted security and manageability.

For IT organizations, the result is a professional-grade system designed from hardware to software with proven, built-in capabilities that resolve the most critical challenges of business and IT: proactive and intelligent security, powerful remote manageability, and energy-efficient performance. With PCs based on a new 2010 Intel Core vPro processor, IT organizations can improve security, reduce operating costs, improve efficiencies and increase productivity, while realizing a return on their investment for years to come.

To learn more about the built-in intelligence of security and remote manageability in laptop and desktop PCs with a new Intel Core vPro processor, visit www.intel.com/vpro.

Blog with the pros who have deployed a new Intel Core vPro processor, visit www.intel.com/go/vproexpert.

[Δ] Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

[1] Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to laptops, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see http://www.intel.com/technology/platform-technology/intel-amt/.

[2] KVM Remote Control (Keyboard Video Mouse) is only available with dual-core Intel® Core™ i5 vPro™ processors and i7 vPro™ processors with active integrated graphics. Discrete graphics are not supported.

[3] Intel® Turbo Boost Technology available on the Intel® Core™ i7 processor and the Intel® Core™ i5 processor only. Intel® Turbo Boost Technology requires a PC with a processor with Intel Turbo Boost Technology capability. Intel Turbo Boost Technology performance varies depending on hardware, software and overall system configuration. Check with your PC manufacturer on whether your system delivers Intel Turbo Boost Technology. For more information, see http://www.intel.com/technology/turboboost.

[4] Intel® Anti-Theft Technology – PC Protection (Intel® AT-p). No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT-p) requires the computer system to h ave an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[5] Source: Intel. Actual time saved depends on network traffic conditions, the amount of user data migrated, and applications, drivers, or policies downloaded during the migration process. Data collected by Intel on various desktop and laptop PCs migrated to Windows 7 under various conditions. MMS demo showing remote, wireless Windows 7 upgrade on Win XP laptops: http://www.vimeo.com/4430604.

[6] Intel® Hyper-Threading Technology (Intel® HT Technology) requires a computer system with an Intel® processor supporting Intel HT Technology and an Intel HT Technology enabled chipset, BIOS, and operating system. Performance will vary depending on the specific hardware and software you use. See www.intel.com/products/ht/hyperthreading_more.htm for more information including details on which processors support Intel HT Technology.

[7] Source: "Using Total Cost of Ownership to Determine Optimal PC Refresh Lifecycles", Wipro Technologies, March 2009 (www.wipro.com/industryresearch). Based on a survey of 106 firms in North America and representing 15 different industries and projections based on a Model Company developed by Wipro Technologies. Computer system price data updated November 2009. Actual results may vary based on the number of use-cases implemented and may not be representative of results that individual businesses may realize. For additional implementation examples refer to Intel Case Studies available at http://communities.intel.com/openport/docs/DOC-1494. Study commissioned by Intel.

[8] AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling AES-NI requires a computer system with an AES-NI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For further availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer. For more information, see http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf.

[9] Intel® Virtualization 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.

[10] Source: Business World – IT Matters - http://www.itmatters.com.ph/ovum.php?id=111108a.

[11] Cross client claim based on lowest performance data number when comparing desktop and laptop benchmarks. Configurations and performance test as follows:

(Laptop) Comparing pre-production Intel® Core™ i5-520M processor based laptops to theoretical installed base of Intel® Core™2 Duo processor T5500. Laptop system configurations: Intel® Core™ i5-520M (3 MB Cache, 2.4 GHz), with Intel® Turbo Boost Technology and Intel® Hyper-Threading Technology on pre-production Intel® Ibex Peak HM55, Dual-channel Micron* 4 GB (2x2 GB) DDR3-1066 7-7-7-20 with Intel® Graphics Media Accelerator HD graphics, Hitachi* 320 GB HDD, Intel® Matrix Storage Manager 8.9.0.1023 (BIOS, Intel® INF and Graphics: pre-production, Imoncompliant with VRD 11.1 requirements), Microsoft* Windows* 7 Ultimate 64-bit RTM. Intel® Core™2 Duo processor T5500 (2 MB Cache, 1.66 GHz, 667 MHz FSB) in Lenovo* Thinkpad* T60 laptop, Laptop Intel® 945GM Express Chipset, Micron* PC5300 DDR2 667 2x1 GB 5-5-5-15 memory, Intel® GMA 950 graphics 224 MB Dynamic video memory technology, Hitachi* Travelstar* HTS721010G9SA00 SATA 100 GB 7200RPM HDD, BIOS Lenovo* 79ETD7WW 2.17 with default settings, Microsoft* Windows* Vista Ultimate. Business productivity claims based on SYSmark* 2007 preview is BAPCo's latest version of the mainstream office productivity and Internet content creation benchmark tool used to characterize the performance of the business client. SYSmark 2007 preview features user-driven workloads and usage models developed by application experts. Multitasking claims based on financial calculations workload consisting of advanced spreadsheet calculation measured using Microsoft* Excel* Monte Carlo Simulation plus Virus Scan. Security workload consists of Winzip*12 decompressing an encrypted archive containing 200 photos, 125 of which are 10MP photos and 75 which are 6MP photos. The photos are in jpeg format. The total size of all the photos is about 830 MB.

(Desktop) Comparing pre-production Intel® Core™ i5-650 processor based desktops to theoretical installed base of Intel® Core™2 Duo Processor E6400 with comparable frequency. Desktop configurations: pre-production Intel® Core™ i5-650 processor (4MB Cache, 3.20 GHz) on pre-production Intel® Ibex Peak P55, Dual-channel DS Micron* 4 GB (2x2 GB) DDR3-1333 9-9-9-24 with Intel® Graphics Media Accelerator HD graphics @ 900 MHz, Seagate* 1TB HDD, Intel® Matrix Storage Manager 8.9.1023 (BIOS, Intel® INF and Graphics: pre-production, Imon compliant with VRD 11.1 requirements), Microsoft* Windows* 7 Ultimate 64-bit RTM Intel® Core™2 Duo Processor E6400 (2M Cache, 2.13 GHz, 1066 MHz FSB) on Intel® DQ45CB, Dual channel DS Micron* 2 GB (2x1 GB) DDR2-800 5-5-5-18 with Integrated Intel® GMA 3000 onboard graphics subsystem, Seagate* 320 GB HDD, (BIOS:0059, Intel® Chipset INF: 8.4.0.1016, Graphics: 7.14.10.1329), Microsoft* Windows* 7 Ultimate 64-bit RTM, Microsoft* Windows* Vista Ultimate 32-bit. Business productivity and energy claims based on SYSmark* 2007 preview is BAPCo's latest version of the mainstream office productivity and Internet content creation benchmark tool used to characterize the performance of the business client. SYSmark 2007 preview features user-driven workloads and usage models developed by application experts. Multitasking claims based on financial calculations workload consists of advanced spreadsheet calculation measured using Microsoft* Excel* Monte Carlo Simulation plus Virus Scan. Security workload consists of Winzip*14 decompressing an encrypted archive containing 200 photos, 125 of which are 10 MP photos and 75 which are 6 MP photos. The photos are in jpeg format. The total size of all the photos is about 830 MB.

[12] Results shown are from the 2007 EDS Case Studies with Intel® Centrino® Pro and the 2007 EDS case studies with Intel® vPro™ processor technology, by LeGrand and Salamasick., 3rd party audit commissioned by Intel, of various enterprise IT environments and the 2007 Benefits of Intel® Centrino® Pro Processor Technology in the Enterprise, Wipro Technologies study commissioned by Intel. The EDS studies compare test environments of Intel® Centrino® Pro and Intel® vPro™ processor technology equipped PCs vs. non-Intel® vPro™ processor technology environments. Tested PCs were in multiple OS and power states to mirror a typical working environment. The Wipro study models projected ROI of deploying Intel® Centrino® Pro processor technology. Actual results may vary and may not be representative of the results that can be expected for smaller businesses. The study is available at www.intel.com/vpro, www.eds.com and www.wipro.com. Studies commissioned by Intel.

[13] Source: Major Utility District ROI case study, http://communities.intel.com/docs/DOC-1494. Study commissioned by Intel.

[14] Source: Increase Productivity by Providing Laptops Beyond Road Warriors, Forrester Consulting, October, 2008 (www.Forrester.com). Study commissioned by Intel.

[15] Source: University of Plymouth ROI Analysis http://communities.intel.com/docs/DOC-2020. Study commissioned by Intel.

[16] Source: CSI Computer Crime & Security Survey, 2008, http://www.pgp.com/insight/newsroom/press_releases/2008_annual_study_cost_of_data_breach.html.

[17] Systems using Client Initiated Remote Access (CIRA) require wired or wirelss LAN connectivity and may not be available in public hot spots or "click to accept" locations.

[18] Check with your PC vendor for availability of computer systems that meet Intel SIPP guidelines. A stable image computer system is a standardized hardware configuration that IT departments can deploy into the enterprise for a set period of time, which is usually 12 months. Intel SIPP is a client program only and does not apply to servers or Intel-based handhelds and/or handsets.

[19] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security.

[20] 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel® 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

[21] Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.

[22] Source: The Cost of a Lost Laptop, The Ponemon Institute, LLC. April 2009. Study commissioned by Intel.

[23] Source: ROI Analysis: Taibei High School uses Intel® vPro™ technology to achieve ROI of 115% and virtually eliminate student IM usage during classes, March 2009, Intel. See http://communities.intel.com/docs/DOC-2989. Study commissioned by Intel.

[24] FIPS PUBS 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[25] Source: http://www.microsoft.com/presspass/exec/bradand/mms2008.mspx.

[26] Source: Quantifying the Benefits of Intel KVM. Wipro, November 2009. Study commissioned by Intel and available at: http://communities.intel.com/docs/DOC-3144.

[27] Source: ROI Analysis: Transforming IT Support with Intel® vPro™ Technology, July 2008, Intel. See http://communities.intel.com/docs/DOC-1755. Study commissioned by Intel.

[28] Source: ROI Analysis: Improving Productivity and Reducing Energy Costs and Consumption with Intel® vPro™ Technology, September 2008, Intel. See http://communities.intel.com/docs/DOC-1915. Study commissioned by Intel.

[29] Source: ROI Analysis: Increasing Call Center Productivity, March 2008, Intel. See http://communities.intel.com/docs/DOC-1915. Study commissioned by Intel.

[30] Source: ROI Analysis: Positive ROI of 100% with Reduced Carbon Emissions and Better Patching Using PCs with Intel® vPro™ Technology, October, 2008, Intel. See http://communities.intel.com/docs/DOC-2141. Study commissioned by Intel.

[31] Source: Reducing 856,000 Pounds of CO2 Emissions through Remote Services and Off-Hours Power Management, 2008, Intel. See http://communities.intel.com/servlet/JiveServlet/previewBody/1703-102-2-2745/320101-002US.PDF. Study commissioned by Intel.

[32] Source: How Come Distributed Work is Still the Next Big Thing? http://www.thefutureofwork.net/assets/WP-20061-Distributed_Work_Next_Big_Thing.pdf.

[33] Source: Telework in Montana State Government, http://www.leg.mt.gov/content/Publications/Audit/Report/06SP-05.pdf.

[34] "Intel Insights and Market Research," Techaisle, March 2009 (www.Techaisle.com). Study commissioned by Intel.

[35] Source: Forrester: The Total Economic Impact™ of Increasing Enterprise Laptop Adoption, http://www.ciscointelalliance.com/_files/pdf/Intel%20Workplace%20Mobility%20Study%20-%20TEI%20Report.pdf. Study commissioned by Intel.

[36] Up to 8X Bandwidth increase based on the theoretical maximum bandwidth enabled by 3x3 Draft-N implementations with 3 spatial streams in combination with a 3 spatial stream Access Point. Actual wireless throughput and/or range will vary depending on your specific operating system, hardware and software configurations. Check with your PC manufacturer for details.

[37] Source: http://newsroom.cisco.com/dlls/2009/prod_062609.html.

[38] Source: Telecommuting Could Save Gas And U.S. $38 Billion Annually – InformationWeek, http://www.informationweek.com/news/management/trends/showArticle.jhtml?articleID=208700405.

[39] ENERGY STAR denotes a system level energy specification, defined by the US Environmental Protection Agency, that relies upon all of the system's components, including processor, chipset, power supply, HDD, graphics controller and memory to meet the specification. For more information, see http://www.energystar.gov/index.cfm?fuseaction=find_a_product.showProductGroup&pgw_code=CO.

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.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Printed in USA 0110/GK/OCG/XX/PDF ♻ Please Recycle 311710-010US