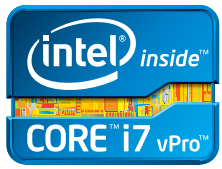
2nd Generation Intel® Core™ vPro™ Processor Family

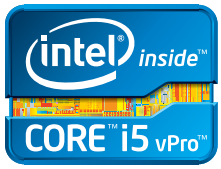
New levels of security, manageability, and responsiveness

White Paper

2nd Gen Intel® Core™ i7 vPro™ Processor

2nd Gen Intel® Core™ i5 vPro™ Processor





Business PCs powered by the 2nd generation Intel® Core™ vPro™ processor family deliver performance you can see—in maximized hardware-assisted security, easier remote PC management, and intelligent performance that adapts to user needs.[1,2] New instructions in the processor speed up encryption and decryption,[3] while new manageability features let authorized IT administrators remotely access, update, and manage systems both inside and outside the corporate firewall—including systems with encrypted hard drives. Enhanced remote monitoring tools such as KVM Remote Control[4] help technicians diagnose and repair PCs even if the PCs are shut down or the operating system (OS) is unresponsive. With 2nd gen Intel Core vPro processors inside, PCs can disable themselves via optional Intel® Anti-Theft Technology[5] if they get lost or stolen. For users, Intel® Turbo Boost Technology 2.0[6] delivers a system that responds to the way users work: The system conserves power whenever possible and accelerates the processor speed when a boost of performance is needed. These PCs deliver 4-way or 8-way multitask processing that allows a processor to do 4 to 8 tasks at the same time, thereby allowing users to move between business applications quickly and seamlessly.[7] Add in stunning built-in visuals,[8] and businesses save by eliminating the added cost burden and power requirements of an additional dedicated graphics card, yet still enjoy the performance users need for Windows* 7, with the headroom for future applications. Users can now create and work with the video-intensive presentations, digital content, and collaboration that are increasingly important in business. The smart performance, intelligent security, and improved manageability of 2nd gen Intel Core vPro processors translate into visible benefits where it counts the most: the bottom line.

Table of Contents

Executive Summary

The 2nd generation Intel® Core™ vPro™ processor family delivers visible benefits in intelligent security, greater manageability, and adaptable performance.[1,2] Intelligent security is built in, with hardware-based features that can prevent malicious attacks, automatically isolate infected systems, and respond faster when a problem occurs. Authorized IT administrators can now remotely access, manage, update, and repair even highly secured systems that have encrypted hard drives. There are also new capabilities for anti-theft protection: PCs can disable themselves if they are lost or stolen.[5] This built-in security helps businesses prove that protection remains in place for sensitive data even after a PC goes missing.

Built-in manageability features deliver secure remote access to wired and wireless PCs both on and off the corporate network virtually anytime. Upkeep is easier and more cost-effective, allowing users to experience less downtime and greater productivity. For example, KVM Remote Control[4] and other built-in capabilities let you remotely configure, diagnose, isolate, and repair an infected PC—even if the OS is unresponsive, and even for the most complex software failures. You can also quickly upgrade to Windows* 7 remotely and overnight, without losing access to legacy applications.[9] In order to enjoy the benefits of these intelligent manageability capabilities, Intel® vPro™ technology must be activated (see page 32 of this white paper).

Users get the benefit of enhanced multitasking along with superb, built-in visuals with energy-saving performance, all from one processor.[8] Adaptive technology and performance gains allow users to run business productivity applications up to 60% faster, with up to 2x faster multitasking, so users can get more accomplished in less time.[10] Intel® Turbo Boost Technology 2.0 automatically and intelligently adapts to each user's needs.[6,10] These performance gains support Windows 7 and provide headroom for future applications. As collaboration and digital content creation becomes more important to business, this performance will be increasingly critical.

2nd gen Intel Core vPro processors are energy efficient, and offer hardware-assisted virtualization capabilities for evolving compute models. The intelligent security, improved remote manageability, accelerated performance, and energy efficiency translate into benefits visible in the most important area of your business—the bottom line.

2nd Gen Intel® Core™ vPro™ Processor Family

Smart security and manageability combined with great responsiveness. A visibly smarter way to boost your business.

Business needs have changed

Business is increasingly borderless, mobility is virtually mandatory, and media has gone mainstream—user needs have evolved even as security challenges have grown. With the average organizational cost of a data breach rising to $6.75M in 2009,[11] the need to update and secure PCs is taking a front-stage position as countries around the world implement increasingly stringent data-breach regulations. Users are also running more complex applications in the foreground for collaboration, rich content creation, and conferencing—driving a demand for more adaptive performance. For example, Flash* is now used in 98.2% of enterprise PCs,[12] and with a dramatic growth in corporate presence on the Internet via social media, 10% of all corporate bandwidth is taken up watching YouTube videos.[13] According to a Gartner study, by 2013, more than 25% of the content that workers see in a day will be dominated by pictures, video or audio.[14] Businesses are reaching more customers, and video conferencing alone is saving Intel's IT group $14M per year by reducing business travel.[15] But these benefits come with costs and challenges: IT services and security for such a diverse workforce require greater access to PCs, regardless of encryption, OS state, power state, and connectivity.

Information Technology (IT) priorities for managing PCs in this environment include:

- **Migrate to Microsoft Windows 7,** and provide an increasingly rich environment to users for multitasking, media, and collaboration.
- **Mobilize the workforce without sacrificing security.** Secure sensitive data in a mobile environment, and prove compliance with increasingly strict data-breach security regulations.
- **Speed up and automate more helpdesk tasks** to reduce user downtime and improve their productivity. IT administrators must automate more tasks, make remote maintenance easier, allow off-hours servicing regardless of PC power state, improve efficiencies, and reduce costs—while still delivering the services users need.
- **Implement desktop virtualization** that is flexible enough to support multiple compute models, which can be implemented as needed for each user.

With challenges that range from security issues to performance headroom for future applications, IT organizations need technology that meets both IT and end-user needs.

Built-in intelligence and smart performance

Laptop and desktop PCs with 2nd gen Intel Core vPro processors deliver intelligent performance and unique hardware-assisted features that improve security and remote manageability, and deliver the performance needed for today's OSs and tomorrow's applications.

- 2nd generation Intel® Core™ i5 vPro™ processor-based PCs[1,2]

- 2nd generation Intel® Core™ i7 vPro™ processor-based PCs[1,2]

Access the PC virtually anytime, anywhere

The manageability capabilities of 2nd gen Intel Core vPro processors 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. Access is via a secure, protected tunnel that does not depend on the OS or security agents. 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.

Better PC security and manageability even if encrypted, wired, or wireless, and inside or outside the corporate firewall

With 2nd gen Intel Core vPro processors, businesses can improve security for both wired and wireless PCs, both inside and outside the corporate firewall. For example, 2nd gen Intel Core vPro processors deliver features that not only secure the asset, but which can help prove continued compliance even after a PC goes missing. In addition, improved manageability features can significantly cut IT service costs, reduce power bills, increase service efficiency, and improve user productivity. For example:

- For desktop PCs, reduce the need for software-related deskside visits by up to 56%.[16]
- For laptops, improve your ability to inventory previously undetected software by up to 47%, and reduce laptop asset inventory failures by up to 62%.[16]
- Run business applications up to 60% faster, experience up to 2x faster multitasking, and see visible performance gains of up to 4x faster encryption/decryption of sensitive data.[10]
- Reduce energy costs and speed up patch saturation by 56%, by powering PCs up off-hours only when service is needed, via the secure remote hardware-assisted power-up and power-down feature built into PCs with 2nd gen Intel Core vPro processors.[16]

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. Less-capable PCs also do not have the headroom for future software and applications. In addition, after 3 years, the annual support costs for a PC can exceed the purchase price for a new system.[17] On average, a 4-year-old PC can cost 59% more to support than it did in its first year.[17] Replacing that notebook in a planned refresh program can save an additional $768 per laptop per year in support and warranty cost.[17] A planned PC refresh program also eliminates expensive, enterprise-wide upgrades and helps keep your users productive. PCs that are 3 years old are also 53% more likely per year to experience a security incident.[17] 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.[18]

Laptop and desktop PCs with 2nd gen Intel Core vPro processors can handle the latest OSs, end-user applications and IT software load—including Windows 7, Office* 2010, encryption software, application streaming, and video conferencing. These PCs can also be more easily secured both inside and outside the corporate firewall. Intelligent security capabilities allow PCs themselves to help identify suspicious circumstances and respond to a "poison pill," based on IT policy. 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 deskside visits to a minimum, and help businesses significantly reduce TCO.

Refreshing wisely means keeping Total Cost of Ownership (TCO) at a minimum. Refreshing with PCs with 2nd gen Intel Core vPro processors can help you achieve a positive ROI rapidly and continuously for years to come.

New in the 2nd gen Intel Core vPro processor family

The 2nd gen Intel Core vPro processor family includes new IT intelligence and smart performance capabilities, such as:

- **Intel Turbo Boost Technology 2.0,** which automatically speeds up the processor when the user's workload requires it.[6]
- **KVM Remote Control,**[4] a hardware-based feature that works for wired and wireless PCs with 2nd gen Intel Core vPro processors that have built-in visuals. This feature helps IT remotely resolve the most complex software failures. It also eliminates the need to purchase and maintain costly hardware KVM switches in the production environment. KVM Remote Control now supports higher screen resolutions (up to 1920 x 1200 with 16-bit color) and is available on dual-core and quad-core 2nd gen Intel Core vPro processors with built-in visuals. The feature works for PCs both inside and outside the corporate firewall.
- **Optional Intel® Anti-Theft Technology (Intel® AT),** to lock down and "brick" the PC in suspicious circumstances.[5] For example, a local anti-theft trigger could be tripped if the PC 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. New features of Intel AT include:
  - **Re-authentication upon resume from S3 sleep state,** to protect data that has been decrypted. Such data has traditionally been vulnerable when users decrypt files and then put their laptop into a sleep state. This feature is available only on PCs with 2nd gen Intel Core vPro processors.
  - **Poison pill delivery over a 3G network**, which helps reduces the window of vulnerability to respond to PC loss or theft. If the PC is 3G-enabled, it can now receive a poison pill via an encrypted SMS message. 3G connections can now occur out-of-band, without dependencies on BIOS or the OS, via a direct hardware link between Intel AT and the 3G module.
  - **Remote unlock via a 3G network,** allowing IT to reactivate the laptop within minutes after it has been recovered.

  - **GPS beacon** and relay of MAC address over a 3G network. Laptops can now send out-of-band location information back to the central server when an anti-theft trigger is tripped.

- **Intel® AES-NI** (Intel® Advanced Encryption Standard New Instructions)[3] **for acceleration of encryption** are now available with both dual-core and quad-core 2nd gen Intel Core vPro processors. These instructions speed up performance for software that uses the AES algorithm for encryption and decryption. For example, performance gains in 2nd gen Intel Core i5 vPro processors accelerate encryption of sensitive data up to 4 times faster than a 3-year-old PC.[10]
- **Built-in visuals** with quick-sync video, hardware-based media acceleration for faster content creation, richer colors for multimedia and collaboration applications.
- **Next-generation Intel® Centrino® wireless products, including Intel® Centrino® Ultimate-N 6300 450 Mbps WiFi adapter on laptops,** delivering up to a 5X bandwidth/speed increase on the "2x2" adapter, and up to 8X bandwidth/speed increase on the "3x3" adapter, as compared to 802.11a/b/g's 54 Mbps.[19]
- **Intel® Management Engine firmware roll-back.** PCs with 2nd gen Intel Core vPro processors include Intel AMT 7.x firmware. IT administrators can choose the version of Intel AMT 7.x firmware to deploy. This helps businesses maintain consistency in their firmware infrastructure even as they upgrade PCs.
- **Host-based configuration**, to speed up activation of Intel vPro technology. This feature is typically used by businesses that do not have a server that is set up for certificates (for example, a small business). Host-based configuration lets a business use streamlined scripts to activate PCs with Intel vPro technology in a matter of minutes.

These and other advances in the 2nd gen Intel Core vPro processor family will help businesses respond faster, secure systems more automatically, prove compliance, support mobile users better, and grow more agile in an increasingly competitive market.

Key features of the 2nd gen Intel Core vPro processor family

The 2nd gen Intel Core vPro processor family delivers intelligent, responsive technologies that make it easier and more cost-effective to secure and manage even encrypted systems. Significant gains in energy efficiency offer visible benefits to the bottom line in conserving power and further reducing costs. And users will enjoy enhanced multitasking and better, faster, adaptive performance, making it easier to collaborate, create and manage the digital content that is increasingly important to business.

Tables 1 and 2, shown on the next page, list some of the key features of laptop and desktop PCs with 2nd gen Intel Core vPro processors.

What, exactly, is Intel® vPro™ technology?

Intel vPro technology is a set of IT capabilities—manageability, security, power management—embedded into the hardware of PCs with 2nd gen Intel Core vPro processors.[1] 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. The capabilities are available for wired and wireless PCs, and most capabilities are also available for PCs that are outside the corporate firewall.

- **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 being powered 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, responsive, 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, software applications, and hard drives. 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, responsive features resolve key challenges

The 2nd gen Intel Core vPro processor family can provide a comprehensive solution to manageability and security challenges. Table 3 on page 8 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 1. Laptop and desktop PCs with 2nd generation Intel® Core™ vPro™ processors.

Feature	Laptops with Intel® Core™ vPro™ processors	Desktop PCs with Intel® Core™ vPro™ processors
2nd gen Intel® Core™ vPro™ processor family	2nd gen Intel® Core™ i5 vPro™ processor and 2nd gen Intel® Core™ i7 vPro™ processor with Intel® QM67 or QS67 Express Chipsets	2nd gen Intel® Core™ i5 vPro™ processor and 2nd gen Intel® Core™ i7 vPro™ processor with Intel® Q67 Express Chipset
Intel® Active Management Technology[2] (Intel® AMT), release 7.0	●	●
Optional Intel® Anti-Theft Technology (Intel® AT)[5]	●	●
Intel® Gigabit network connection	Intel® 82579LM	Intel® 82579LM
Support for 802.11agn wireless protocols	●	Optional
WiFi and optional WiMAX support, with either Intel® WiMAX/WiFi 6060 2x2 agn, Intel® Centrino® Ultimate-N/Advanced-N 6000 Series 2x2 or 3x3 abgn	●	Optional
Support for 802.1x, Cisco SDN*, and Microsoft NAP*	●	●
Intel® Stable Image Platform Program (Intel® SIPP)[20]	●	●

Table 2. 2nd gen Intel® Core™ processor family and 2nd gen Intel® Core™ vPro™ processor family.

		SMART PERFORMANCE			SMART PERFORMANCE, IT INTELLIGENT	
Features for...	Description	Intel® Core™ i3	Intel® Core™ i5	Intel® Core™ i7	Intel® Core™ i5 vPro™	Intel® Core™ i7 vPro™
Smart security and manageability	Reduce maintenance costs with remote configuration, diagnosis, isolation, and repair of infected PCs, even if they are unresponsive[1,2]	○	○	○	●	●
	Hardware-based KVM (keyboard video mouse) Remote Control, now with higher screen resolution (up to 1920 x 1200), allows IT to remotely see what your users see through all PC states[4]	○	○	○	●	●
	Remote unlock of encrypted drives that require pre-boot authentication, and manage data security settings even when the PC is off[2]	○	○	○	●	●
	Hardware-assisted remote shutdown, wake-up, and update of PCs during off-hours—reduces energy costs and enables up to 56% faster time to patch saturation[2,16]	○	○	○	●	●
Secure virtual environments for desktop virtualization	Take advantage of hardware-assisted secure, virtual environments to centralize management of Operating System and application images and enable the use of local computing resources for a rich end-user experience[9]	◑	◑	◑	●	●
Responsive, adaptive performance	Intel® Turbo Boost Technology 2.0 adapts performance when needed for more demanding tasks and saves energy when performance is not needed[6]	○	●	●	●	●
	Hardware-based acceleration of encryption and decryption with Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI)[3]	○	●	●	●	●
	Built-in visuals provide superb visual performance, sharper images, and richer color for multimedia, digital creation content, and collaboration[8]	●	●	●	●	●
	Multitask processing enables the PC to work on more tasks at the same time—resulting in enhanced multitasking when working among multiple office applications[7]	4-way	4-way	Up to 8-way	4-way	Up to 8-way
Safe investment	Plan PC qualification and deployment strategy with Intel® Stable Image Platform Program (Intel® SIPP)[20]	○	●	●	●	●
	Disable PCs at the hardware level in the event of loss or theft through optional Intel® Anti-Theft Technology[5]	●	●	●	●	●
	Have the performance you need for Windows* 7 when your business is ready to migrate	●	●	●	●	●
	Help PCs meet ENERGY STAR* requirements[21]	●	●	●	●	●

○ Not applicable ◑ Basic capability ● Advanced capability

Table 3. Key IT challenges and solutions addressed with 2nd gen Intel® Core™ vPro™ processor family-based PCs.

Challenge	Solution[a,b]
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 and service center calls 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**[4] to help resolve complex issues, so you can see exactly what the user sees, and repair the PC more effectively from a remote location. ▪ **Fast call for help,** which lets the user initiate secure communication with IT, even if the laptop is outside the corporate firewall.[22] ▪ **Remotely reimage systems** even if PC power is off at the start of the upgrade cycle.
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. ▪ **Intelligent agent-presence checking** for rapid notification when an application is compromised.[c] ▪ **Built-in, programmable system defense filters** for automated, hardware-based protection against viruses and attacks.
Thwart thieves—secure assets and data even if the PC is lost or stolen[5,c]	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 via a variety of methods.[c] ▪ **Built-in, programmable triggers** and responses to protect data and the PC after loss or theft of the system.[5,c] ▪ **Intelligent, local, policy-based timers** that trigger a lockdown if the user has not re-authenticated upon PC resume from sleep state before timer expiry.[c] ▪ **Delivery confirmation of a poison pill to make it easier to prove compliance with strict data-breach regulations.**[c] ▪ **3G-based and IP-based communication:** Secure, remote communication—including delivery of poison pill and remote reactivation—via an IP-based network or via SMS messages over a 3G network.[c] ▪ **GPS beacon and/or relay of MAC address over a 3G network to help locate lost or stolen laptops.**[c]
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 and discover virtually all PCs: ▪ **Accurate, remote asset inventories,** even if PCs are powered off or management agents are missing.[c] ▪ **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.[c]

[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, see page 32 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 a host OS-based VPN.

Manage PCs regardless of power state

PCs based on the 2nd gen Intel Core vPro processor family are designed to give IT technicians greater remote visibility of the PC, better remote manageability even for systems with encrypted hard drives, and "always available" access in both wired and wireless states. These PCs have built-in intelligence to deliver a more responsive, manageable machine (see Table 4).

When managing PCs with 2nd gen Intel Core vPro processors, 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 2nd gen Intel Core vPro processors for wired or wireless PCs. PCs can even perform their own local, scheduled wake from any powered-off state without a network connection. The third-party software agent on the PC can then call into a central server to initiate 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.

Use an existing management console for both laptop and desktop PCs

PCs with 2nd gen Intel Core vPro processors can use the same management console and communication mechanisms as other PCs. You can manage both laptop and desktop PCs with 2nd gen Intel Core vPro processors 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, adaptive capabilities of 2nd gen Intel Core vPro processors. For small businesses with fewer than 500 PCs, IT managed service providers can turn to management software such as N-able Technologies' N-central* to take advantage of the manageability and security features built into 2nd gen Intel Core vPro processors.

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 2nd gen Intel Core vPro processors.

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 with Intel Core vPro processors.

Table 4. Summary of key use cases for PCs with 2nd gen Intel® Core™ vPro™ processors.

Use Cases[a]	Usages[a,b]
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.
Remote software update	Power up PCs during off hours for software updates. Also client-initiated scheduled wake for update.[22]
Agent presence checking and alerting[c]	Ensure critical applications are running, and be quickly notified when they miss a check in.[c]
System isolation and recovery	Automated or manual policy-based protection against virus outbreaks.
Protection for data if a laptop is lost or stolen[c]	Identify and prevent unauthorized access to encrypted data, or disable the laptop remotely or via client-side intelligence if it is lost or stolen.[c] Upon lock-down, disable or delete access to encryption keys, and/or send a GPS beacon or relay a MAC address via a 3G network.[c] Rapid reactivation (if laptop is returned) via local reactivation or remotely via an IP-based or 3G-based network.[c]
Remote diagnosis and repair	Diagnose and repair problems remotely via an out-of-band event log, remote/redirected boot, console redirection, KVM Remote Control,[4] and preboot access to BIOS settings.
Remote hardware and/or software asset tracking[c]	Take a hardware or software inventory regardless of OS state or PC power state.[c]

[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, see page 32 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.

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 2nd gen Intel Core vPro processor family delivers both "readily available" (out-of-band) remote communication, as well as robust security technologies. These communication and security technologies are designed right into the hardware, so they are less vulnerable to tampering or removal. They help ensure that the powerful capabilities of Intel vPro technology, as well as your stored information, are better protected.

Out-of-band communication

The communication channel used by Intel vPro technology runs "under" or outside the OS (see Figure 1). Such communication is called out of band (OOB) communication because it occurs below the OS level and takes a different path through hardware. In contrast, "in-band" communication is communication with the OS or with applications at the OS level. Since the OS and software applications can be compromised in various ways (for example, if security software is not kept up to date, or if security applications or agents are removed), software-based communication can also be disabled.

The OOB channel used by Intel vPro technology is based on the TCP/IP firmware stack designed into PC hardware. This channel does not use the network 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.

Basically, once communication goes through the network adapter, it can be routed either up to the OS or down through hardware. Intel vPro technology is hardware-based, so communication with Intel vPro technology features is routed through hardware. Even if something happens "upstairs" to the OS—or a software agent is removed, or security software goes missing—the hardware "downstairs" remains in place, unaffected. Thus, you can continue to communicate with the hardware-level Intel vPro technology capabilities. This is why you can remotely reboot the PC even if the OS is not responding. Or remotely take inventory by reading the protected memory space of Intel vPro technology even if the management agent is missing.

Intel vPro technology is built into the chipset; it is not stored on the hard drive. Communications with the chipset and the protected Intel vPro technology memory do not depend on the hard drive. This means you can also still use the Intel vPro technology features even if the hard drive has failed.

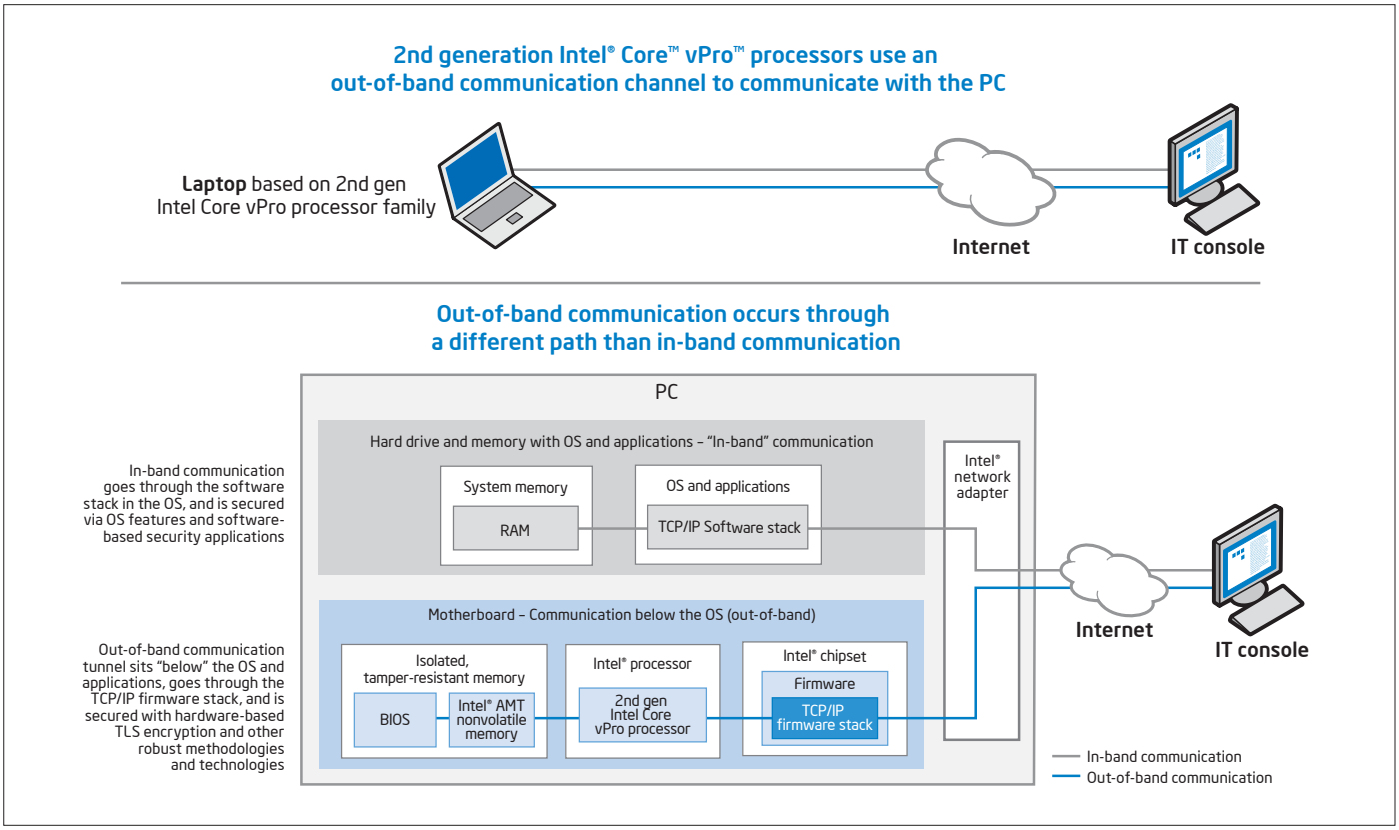


Figure 1. Out-of-band communication. Secure communication channel runs "under" or outside the OS. This channel is available regardless of the health of the operating system or the power state of the PC, even if the PC's hard drive is removed.

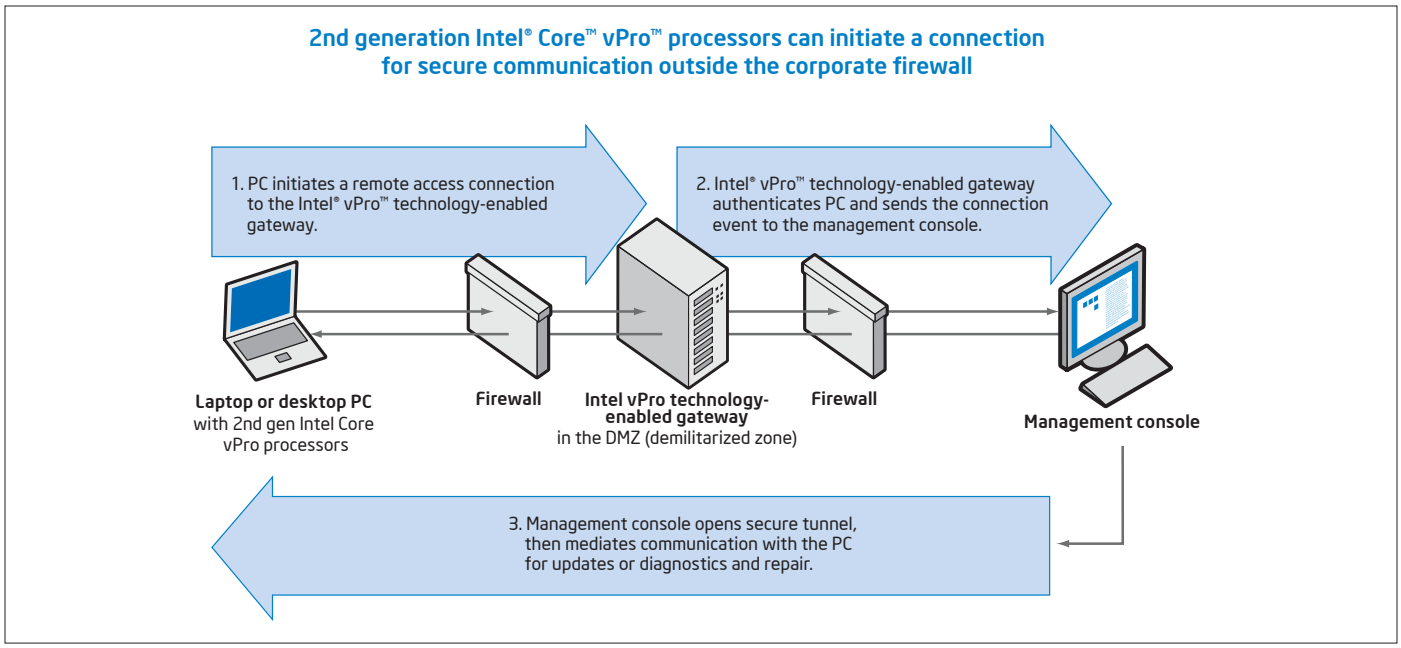


Figure 2. Communication to PCs outside the corporate firewall is secured via TLS. An Intel® vPro™ technology-enabled gateway authenticates wired and wireless PCs, opens a secure TLS tunnel between the management console and PC, and mediates communication.

Communication outside the corporate firewall

Laptops and desktop PCs with 2nd gen Intel Core vPro processors 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). The DMZ exists between the corporate and client firewalls (see Figure 2). To enable this environment, system configuration information stored 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 2nd gen Intel Core vPro processors:

- **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.[22]
- **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 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.

In order to secure the communication tunnel, authentication protocols are required for each element along the communication path, including firewalls and gateways. This communication capability relies on collaboration with the industry to establish secure gateways for client-initiated communication.

Robust security schemes for remote communication

The hardware-based communication and manageability capabilities of Intel vPro technology 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

The security measures built into laptop and desktop PCs with 2nd gen Intel Core vPro processors 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.

Respond faster to threats with intelligent, automated security

Security remains one of the highest priorities for IT. The number of security incidents has grown dramatically each year. The nature of these threats has also changed as the motivations of attackers have shifted from bragging rights to financial gain. In addition, the cost of a data breach continues to rise. A recent survey of 43 companies in 2008 found that the average cost of a lost or stolen laptop is $49,000.[23]

PCs with 2nd gen Intel Core vPro processors help IT administrators prevent more threats via automatic capabilities, and respond to threats faster through smarter security. Once Intel vPro technology is activated, IT can take advantage of intelligent 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. Agent presence checking and "always available" alerting help IT safeguard PCs from certain types of malware and malicious attacks by continually polling for the presence of software agents. This helps IT identify problems rapidly and respond automatically when an agent is compromised. When optional Intel AT is also activated, IT can use intelligent anti-theft triggers (local or remote) to help determine when a laptop is not under control of the authorized user. IT can then rapidly and remotely lock down the machine to thwart data breaches attempted by thieves. Both wired and wireless PCs can be locked down via a local, automated and policy-based approach, or through IP-based or 3G network-based communication. When a problem occurs, the user can simply press a specific key combination to call for help for repair or servicing. That key press initiates a protected communications tunnel to IT, even if the PC is outside the corporate firewall.

These flexible, policy-based and intelligent security features make it easier to protect and service your network, assets, and data, both inside and outside the corporate network. PCs with 2nd gen Intel Core vPro processors include capabilities for:

- Remote power up–push updates virtually anytime
- Agent presence checking
- Programmable filtering
- Alerting from inside and outside the corporate network
- Automated isolation of systems while still allowing OOB communication
- Manageability of PCs with encrypted hard drives
- Manageability of data security settings even if PC is powered down
- Hardware acceleration for AES encryption with Intel AES-NI
- Intel Anti-Theft technology (Intel AT), including intelligent triggers, poison pills, and reactivation features
- Out-of-band management
- Preboot access to software version information
- Preboot access to .DAT file information and other critical system information
- Preboot access to BIOS
- Intel® Trusted Execution Technology (Intel® TXT)[24]
- Intel® Virtualization Technology (Intel® VT)[9]

Keep security applications in place and up to date, regardless of PC power state

A key challenge for IT remains keeping security applications and agents in place and up to date. PCs with 2nd gen Intel Core vPro processors let authorized technicians use a combination of features to push updates down the wire, even if the PC was powered off at the start of the update cycle:

- **Full 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.
- **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 having to wake the PC.
- **Reduce power consumption** and lower energy bills by powering down PCs during off-hours, while still maintaining remote access for security updates.

Identify and respond to threats faster and more effectively

PCs with 2nd gen Intel Core vPro processors provide intelligent, policy-based tools for identifying and responding to threats, loss and theft:

- **Optional 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. For example, 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 data even if decryption credentials are known. Send poison pills via IP-based or 3G-based networks. Allow rapid reactivation, integrated with existing software vendor preboot login. (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 significantly.[25]
- **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.

Investigate and resolve security issues faster

PCs with 2nd gen Intel Core vPro processors provide a secure communication channel to the PC, even if the OS or applications have already been compromised, or PC power is off as a security measure to help prevent the spread of a threat. These PCs also include dedicated memory where critical system information is stored, and which authorized IT technicians can access—without powering up the system. This makes it easier to access PCs and identify problems without exposing the network to further problems.

- **Out-of-band management** even in secure environments, such as 802.1x, PXE, Cisco SDN,* and Microsoft NAP* environments.
- **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.

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 2nd gen Intel Core vPro processors, network security credentials can be embedded in the hardware. This includes an Intel® Active Management Technology[2] (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 of 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.

Small business: Security profile

Most small businesses do not have an in-house IT department. They rarely standardize their technology—the use of freeware and other less standardized software is common, and they typically employ PCs of different ages and from various OEMs. Small businesses often equate security with the simple use of anti-virus software and a firewall. Also, a common belief is that small businesses are too small for hackers to bother with—an attitude that can give a false sense of security. In the small-business arena, IT is often a third-party service, and when IT problems arise, the business is typically more concerned about the solution than in finding and managing the root cause.

Security solution for Managed Service Providers for small businesses without IT

2nd gen Intel Core vPro processors make it easier for a third-party IT provider to remotely secure and manage both wired and wireless PCs. This helps small businesses concentrate on their business, not their IT. Small businesses can now take advantage of the same security features as enterprises, in order to comply with strict data-breach regulations and create a more secure environment to protect assets and data.

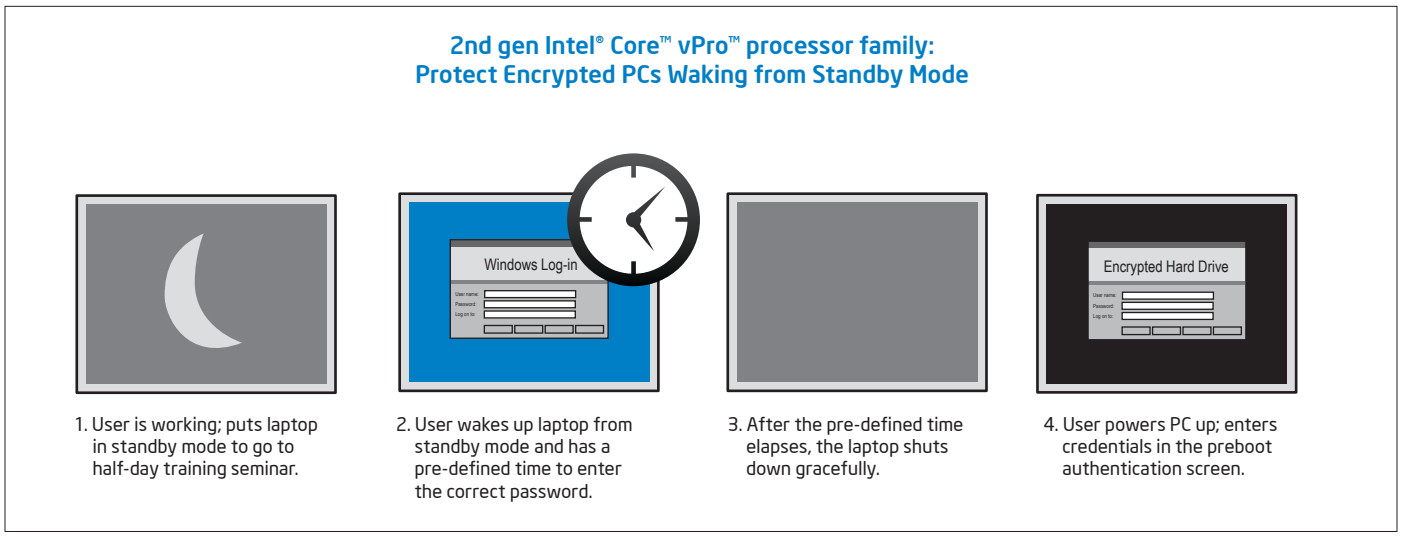


Figure 3. 2nd gen Intel® Core™ vPro™ processors with Intel® Anti-Theft Technology close a traditional vulnerability in laptops with encrypted hard drives by requiring re-authentication after resume from standby mode (S3 sleep state).

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.

Optional Intel® Anti-Theft Technology (Intel® AT)

One of the key features in PCs with 2nd gen Intel Core vPro processors is optional Intel Anti-Theft Technology (Intel AT).[5] Intel AT improves data protection and encryption solutions by protecting the encryption keys themselves, and by allowing IT to disable a laptop that is not under control of the authorized user. Intel AT must be enabled by your OEM and turned on in order for you to access this intelligent security technology.

New Intel AT features in 2nd gen Intel Core vPro processors

Some of the key Intel AT features in PCs with 2nd gen Intel Core vPro processors include:

- **Secure a laptop upon resume from the S3 sleep state,** by requiring that the user re-enter their credentials before decrypted information can be accessed. This feature closes a traditional vulnerability in laptops (see Figure 3). This feature is only available on 2nd gen Intel® Core™ i5 vPro™ processors and 2nd gen Intel® Core™ i7 vPro™ processors.
- **Specify a short delay before shutting down** a laptop that resumes from sleep state. This allows a user time to save their work even if their rendezvous timer expired while the laptop was asleep or in power-save mode.
- **Reactivate the PC via the PBA** (preboot authentication) module screen. This reduces complexity for users and makes reactivation faster and more convenient.
- **SMS messaging over a 3G network** to help reduce the window of vulnerability to respond to PC loss or theft. Send a poison pill via an encrypted SMS message over a 3G network to respond rapidly to a lost or stolen laptop even if the PC is disconnected from the IP-based network. This feature provides a direct hardware link between Intel AT and the 3G module—it does not depend on the BIOS or OS. An authorized IT administrator can also reactivate the system remotely via an SMS message to reduce user downtime when the system has been recovered. (The PC must be equipped with an Intel AT-enabled 3G module in order to take advantage of the Intel AT SMS/3G features.)
- **GPS beacon and relay of MAC address.** Intel AT can now transmit location information (latitude and longitude) if the 3G NIC provides latitude and longitude information, and/or relay a MAC address to the central server.
- **Faster enrollment,** with pre-generation of the license key in the Intel Management Engine. This feature reduces the time it takes to generate the unique license key and enroll Intel AT-enabled PCs.

Intelligent theft-detection triggers can be local or remote

Intel AT provides IT with a set of programmable hardware-based triggers to help identify a lost or stolen laptop. 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.

Local detection mechanisms include:

- Excessive login attempts
- Missed check-in with the ISV's central server
- A change in Intel Management Engine (ME) firmware
- Removal of the CMOS battery

Remote detection mechanisms include:

- User-reported theft
- Remote poison pill sent from the central server over an IP-based network
- Remote poison pill sent via an automated, encrypted SMS text message
- Remote poison pill sent via a manual, encrypted SMS text message

Flexible poison pill responses to a suspicious circumstance

Intel AT includes "poison pill" features that let IT respond rapidly to the situation, either through local, automated responses, or by a rapid remote message. Poison pill responses are policy-based and can be delivered remotely or by an automated, local mechanism:

- **Remote and administered by IT**, based on an alert, a missed rendezvous with the central server, or upon receiving a call from the user (for example, that the laptop was lost while traveling).
- **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).

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. This helps prevent access to the keys and makes data unretrievable. Even if a thief transfers the hard drive to another laptop to try to access the data, the data can still be protected.
- **Block access to (lock) cryptographic materials,** without deleting the materials.
- **Disable the PC so it cannot boot the OS,** even if the hard drive is replaced or reformatted.
- **Disable the PC's boot process** and **power down the system.**
- **Disable the PC's boot process and disable or block 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.
- **Delay the disable,** so that the system goes into stolen state, but does not immediately power down. Instead, upon the next reboot or power cycle, the boot process is blocked, and the preboot authentication screen is displayed requiring user authentication. This policy is useful for allowing a graceful shutdown and/or for creating an opportunity to collect location information.

2nd gen Intel® Core™ vPro™ processors with Intel® Anti-Theft Technology: Closes security vulnerabilities and adds convenience for users

Resume from S3 sleep state

One of the traditional vulnerabilities of encryption on laptops occurs when a laptop resumes from S3 sleep state. Files that are already decrypted remain decrypted in the sleep state, and access to these decrypted files can be as simple as opening the laptop cover. When the system comes out of sleep state, it bypasses the pre-OS encryption and instead brings up the Windows login screen, which is vulnerable to a variety of attacks.

This critical vulnerability affects PCs both within and outside the corporate campus. For example, users often put their laptops into a sleep state to attend a meeting, go to lunch, or simply to conserve power at remote sites. At airports, where as many as 12,000 laptops are lost or stolen each week, users often work while traveling and often put their systems into a sleep state in order to deal with the details of airline travel.[23] Overall, since 2005, more than 263 million personal records have been exposed via lost or stolen laptops.[26]

Intel® Anti-Theft Technology (Intel® AT) closes that window of vulnerability and enforces pre-OS encryption. If files have been decrypted, Intel AT requires re-authentication upon resume from sleep state after a predefined time, based on IT policy. The user must enter their credentials before regaining access to the decrypted files. This feature is available only on PCs with 2nd gen Intel® Core™ vPro™ processors.

As with other Intel AT capabilities, excessive login attempts to Windows password log-in can also trigger a local lockdown and secure the entire system.

Delay before lockdown

Intel AT is policy-based, and allows the IT administrator to specify the timeframe in which the laptop must check into the central server. If a rendezvous is missed, the system locks down. Because laptops are often put in sleep states while users are traveling or doing other lengthy tasks, a rendezvous timer could expire, even though the system is under control of the authorized user. When the system resumes from sleep state, it immediately locks down.

To help users in these circumstances, Intel AT provides IT administrators with a delay option before lockdown. Instead of locking the system immediately upon resume from sleep state, the IT administrator can allow a short delay upon resume. This notifies the user that a lockdown will be occurring within so many minutes. It allows the user to save their work before the system shuts down.

The user can then reboot the system, enter their credentials in the reactivation screen, and resume work. Or, make a fast call for help to IT, and receive a rapid reactivation message via a 3G network.

IT can also specify that, when an Intel AT trigger is tripped, Intel AT will:

- **Do nothing.** This is a special policy that, when triggered, puts the system in stolen state but does not lock the boot process or power down the system. This is useful for anti-theft service providers who specialize in PC recovery and want the PC to remain unlocked in order to collect location information.

For example, see Figure 4. IT could define a trigger for critical machines, such as a financial officer's laptop, so that the system must check in with the central server every day. 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.

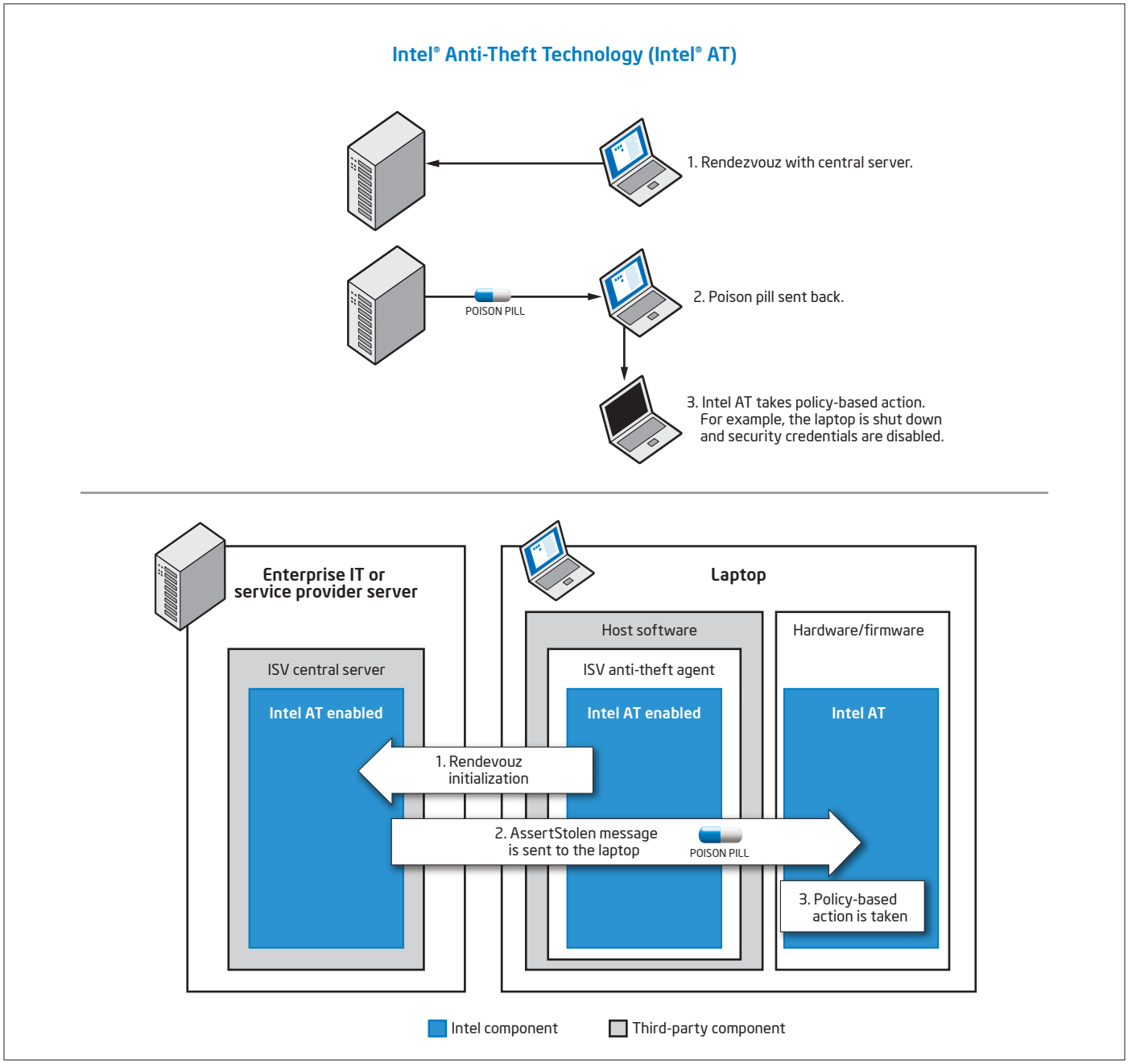


Figure 4. Lost laptop with Intel® Anti-Theft Technology rendezvous with central server and receives poison pill.

Easy reactivation and full system recovery

A key benefit of Intel AT is that it is non-destructive technology. Encrypted data is not erased; only the cryptographic materials are locked or erased. Reactivation from a lock-down can be rapid and easy, using either a local or remote mechanism. These mechanisms are policy-based.

- **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.
- **Reactivation in the preboot authentication module (PBA).** This authentication method is defined by the PBA provider, and can include passwords, PINs (personal identification numbers), biometric info, a USB token, a smart card, a secure PIN, and so on. This feature bypasses the BIOS authentication module screen and allows the laptop to be unlocked via the PBA screen. It's a convenience for users, one that simplifies their authentication process when full-disk encryption is in place.
- **Instant reactivation code sent remotely,** via an encrypted SMS message over a 3G network. (Requires a PC with a 3G modem that supports Intel AT.)

All reactivation methods return the PC to full functionality. These methods also offer a simple, inexpensive way to recover the laptop without compromising sensitive data or the system's security features.

Intel AT must be enabled 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. Vendors who support Intel AT include Absolute Software Corporation, WinMagic, and PGP, and additional security providers are planning to offer solutions in 2011.

In order to deploy an Intel AT solution, a service provider or software vendor with Intel AT capabilities is required. To help software vendors and service providers test and validate their designs for Intel AT-capable products, 2nd gen Intel Core vPro processors include a software development kit (SDK) and documentation.

Hardware-based acceleration for encryption

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

One of the more recent encryption standards adopted by the U.S. Government is AES (Advanced Encryption Standard). 2nd gen Intel Core vPro processors include hardware-based CPU instructions (Intel® AES-NI, or Intel® Advanced Encryption Standard New Instructions) for AES.[3] These instructions are designed to consolidate the AES mathematical operations, improve security by hardening cryptography software, and speed up applications that use the AES algorithm.

For example, software developers can write to these Intel 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 2nd gen Intel Core i5 vPro processor-based PC to an installed-base with a 3-year-old Intel® Core™2 Duo processor-based PC. The benchmarks showed that protection of sensitive data can be up to 4x faster on a 2nd gen Intel Core i5 processor-based PC.[10]

2nd gen Intel Core vPro processors with Intel AES-NI support can be used to improve performance for systems that use whole-disk encryption and file storage encryption. Software vendors that support Intel 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, 2nd gen Intel Core vPro processors include 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 security updates, remediation, and management.

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. In turn, this helps reduce risks to the network.

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 2nd gen Intel Core vPro processors use a regular, programmable "heartbeat" presence check. The agent presence checking capability is designed into the Intel vPro technology. The heartbeat uses a "watchdog" timer so third-party software can check in with Intel vPro technology 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. Intel vPro technology 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 can help safeguard the system from certain types of malware and malicious attacks by continually and ***intelligently*** polling for the presence of software agents. This can improve the reliability of presence checks and help reduce the window of software vulnerability.

Also, these "healthy" heartbeats are stored in the event log and are not considered "alerts." Only when there is a problem is an alert generated. Only if specified by IT policy is the alert sent across the network—so your network isn't flooded with healthy heartbeat signals, yet you can 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.

Agent presence checking is well supported by remote manageability applications. For a list of ISVs that support agent presence checking, check the software catalog on the Intel Web site: www.intelsalestraining.com/vprosoftwareguide/content.htm.

Filter threats and isolate PCs automatically based on IT policy

Laptop and desktop PCs with 2nd gen Intel Core vPro processors 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 2nd gen Intel Core vPro processors 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 5). 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 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.

Receive alerts even if a system is off the corporate network

PCs with 2nd gen Intel Core vPro processors have policy-based alerting built into the system. All alerts are logged in the persistent, protected event log. However, IT administrators can define the types of alerts they want to receive. In this way, alerts that are not as critical do not add substantially to network traffic, yet IT still has access to a full event log for diagnostics and repair.

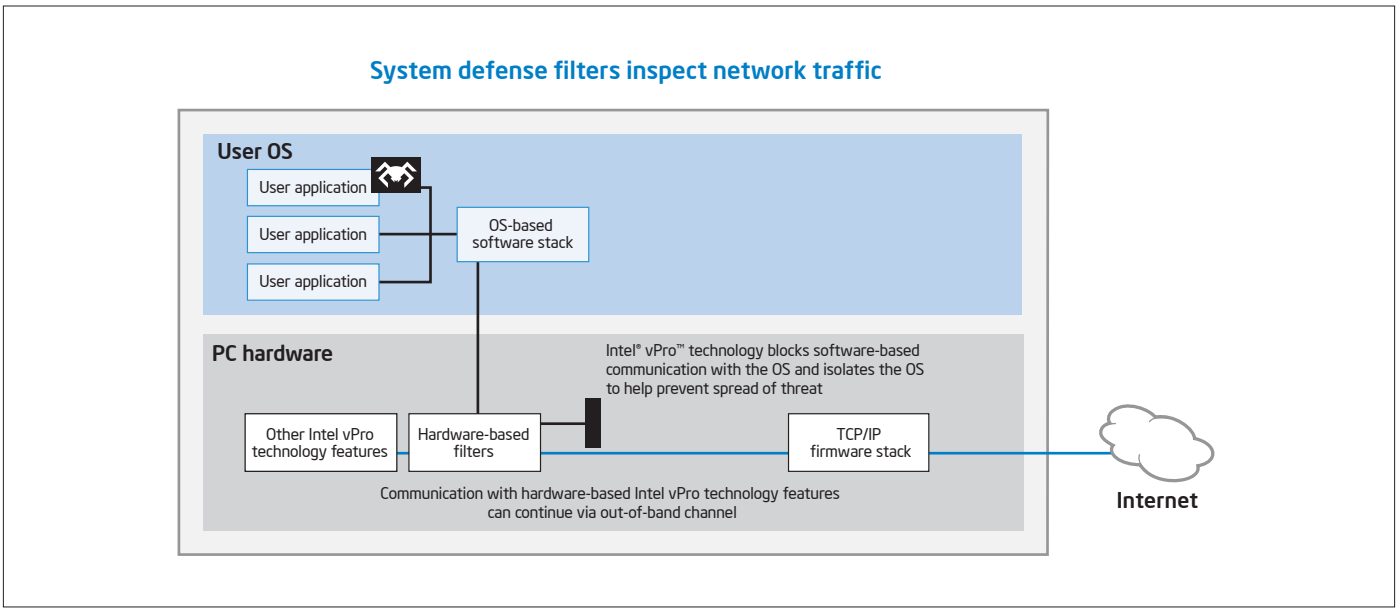


Figure 5. System defense filters inspect network traffic. PCs with 2nd gen Intel® Core™ vPro™ processors can port-isolate itself or cut off its own network data path to quarantine itself when suspicious behavior is recognized even if its OS is not available to help prevent threats from spreading to the network. Remote communication to hardware-based Intel® vPro™ technology features (such as event logs) are still available through the out-of-band communication channel.

Alerting within the corporate network

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

Alerting from outside the corporate network

IT can receive notifications from a PC (awake and OS operable) that is:

- Connected to the corporate network through a host OS-based VPN
- Connected from an open network outside the corporate firewall, via a wired or wireless LAN

IT administrators can now be notified rapidly and automatically when a system falls out of compliance. IT administrators can also be notified automatically when hardware is about to fail—sometimes even before users know they have a problem, or before applications hang.

Secure desktop virtualization for evolving compute models

PCs with 2nd gen Intel Core vPro processors include additional technologies that can improve security further:

- Intel® Trusted Execution Technology[24] (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 Virtual Machine Monitor (VMM). This helps to protect information in virtualized environments from software-based attacks. Intel TXT also protects secrets (security credentials) during power transitions. For more information about Intel TXT, visit www.intel.com/technology/malwarereduction/index.htm.
- 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." For example, Intel VT for I/O virtualization models delivers the ability to flexibly assign I/O devices to virtual machines, and extend that protection and the associated isolation properties of VMs for I/O operations. It allows IT to isolate and restrict device accesses to the resources owned by the partition that is managing the device.[9]

***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.*

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.

Faster, easier remote manageability helps reduce costs

PCs with 2nd gen Intel Core vPro processors make it 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 manageability features—including hardware-based KVM Remote Control—make PC upkeep easier even for complex application and/or OS issues, and help keep service costs low. In turn, by speeding up and automating more remote service desk tasks, businesses can minimize user downtime and improve user productivity.

The 2nd gen Intel Core vPro processor family includes other important manageability features, such as PC Alarm Clock to help initiate remote servicing for PCs that are powered down and/or outside the corporate firewall. 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.

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.
- **Restore an OS** by pushing new copies of missing or corrupted files, such as .DLL files.
- **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.

Table 5. Built-in remote manageability features for wired and wireless PCs.

Manageability task	2nd gen Intel® Core™ vPro™ processor family feature[a,b]
Remote upgrades	• **Remote power up,** used with console redirection and remote reboot capabilities.
Receive alerting anytime	• **Out-of-band, policy-based alerting** that works even if the OS is not available, the hard drive has failed, or the PC is powered off.
Resolve more problems remotely for both wired and wireless PCs, even if the PC is outside the corporate firewall	• **Remote/redirected boot** through integrated drive electronics redirect (IDE-R). • **Console redirection** through Serial-over-LAN (SOL). • **KVM Remote Control,**[4] a hardware-based capability, now supporting screen resolution up to 1920 x 1200 with 16-bit color.
Minimize user involvement in repair, even if the PC is outside the corporate firewall	• **Fast call for help,** for wired or wireless systems, even outside the corporate firewall. • **PC Alarm Clock,** to schedule a PC to wake itself from any idle, powered off, or sleep state, without a network connection, even if the PC is outside the corporate firewall.
Remotely access critical system information for easier diagnostics	• **Persistent event logs,** stored in dedicated, protected memory. • **"Always available" asset information,** stored in dedicated, protected memory. • **Access to preboot BIOS** configuration information, available virtually anytime.
Accurate, remote discovery and inventory for wired or wireless systems[c]	• **UUID,** which persists even across reconfigurations, reimaging, and OS rebuilds.[c] • **Hardware-asset information,** such as manufacturer and model information for components.[c] • **Software-asset information,** such as software version information and .DAT file information, stored in dedicated, protected memory.[c]

[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, see page 32 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.

Many case studies have shown how PCs with 2nd gen Intel Core vPro processors 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).

Remote upgrades save IT and user time

PCs with 2nd gen Intel Core vPro processors make it easier to remotely and automatically upgrade operating systems and applications. For example, IT can remotely upgrade to Windows 7 at night, regardless of the initial power state of the PC.

***Note:** PCs with 2nd gen Intel Core vPro processors include Intel AMT 7.x firmware. You can choose the version of Intel AMT 7.x firmware you deploy and maintain consistency in your firmware infrastructure even as you upgrade your PCs.*

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.

As PCs age, these costs escalate until after 3 years, annual PC support costs can exceed the purchase price of a new PC.[17] On average, a PC older than 3 years can cost 59% more to support than it did in its first year.[17] It can experience up to 53% more security incidents,[17] is 4.5 times more likely to experience a hard drive failure;[27] and can cost up to 1.65 times more to repair and maintain than it did in its first year.[27]

Problem-resolution capabilities in PCs with 2nd gen Intel Core vPro processors can help IT managers reduce deskside visits by up to 56%[16] 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,** a hardware-based feature that works for wired and wireless PCs with 2nd gen Intel Core vPro processors that have built-in visuals. This capability works both inside and outside the corporate firewall, and helps IT remotely resolve the most complex software failures. KVM Remote Control now supports higher screen resolutions (up to 1920 x 1200 with 16-bit color), and is now available on quad-core 2nd gen Intel Core vPro processors with built-in visuals. Because KVM Remote Control is built into system hardware, it eliminates the need for a separate, costly data-center KVM switch.

KVM Remote Control lowers support costs

In spite of improved management tools, almost 20% of problem tickets still require that users help resolve the problem.[28] Even with the built-in remote management capabilities of Intel vPro technology, the complexity of these "corner case" or "edge" failures have traditionally meant that a technician must still make a deskside visit or ask users to help resolve the problem.

PCs with 2nd gen Intel Core vPro processors with built-in visuals deliver hardware-based KVM Remote Control.[4] KVM Remote Control allows an authorized IT technician to "get behind the user's keyboard" without leaving the help desk (see Figure 6 on the next page)—it allows the technician to remotely control the keyboard, video, and mouse of a user's PC, as if the technician were deskside at the PC itself. Unlike software-based remote desktop , hardware-based KVM Remote Control allows the technician to more securely see and control PCs reliably through all states. This helps technicians resolve software failures for both wired and wireless PCs, even for PCs outside the corporate firewall.

Typical savings from KVM Remote Control

Studies show that hardware-based KVM Remote Control[2,4] (keyboard video mouse), a feature in 2nd generation Intel® Core™ vPro™ processors can reduce problem resolution time by 20% for complex software issues.[28] These include "corner case" or "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.[28] Adding hardware-based KVM Remote Control can save such a company an additional $133,000 in IT service costs and $97,000 in user productivity.[28] That is conservatively equivalent to about 2,400 IT hours at $55 per hour, and approximately 2,400 hours in user productivity.[28]

General improvements in phone-based support can help business realize further benefits in user productivity—more than $740,000 in savings.[28] For a company with 30,000 PCs, the overall savings over 3 years from using the capabilities of 2nd gen Intel Core vPro processors with KVM Remote Control can be over $1.6 million.[28]

Technicians now have full interactivity with the PC to remotely resolve even complex issues—without leaving the help desk. Authorized technicians can use KVM Remote Control to help remotely resolve issues with BIOS, startups/shutdowns, blue screens, OS freezes, disk failures, and network software issues. Also, the KVM Remote Control session persists after a reboot of the user's PC, so the technician can fully resolve the problem without initiating a second session. IT administrators can experience visible benefits of increased efficiencies and lower manual labor costs, while improving user uptime and productivity.

With KVM Remote Control, technicians can now:

- Remotely reduce by up to 84% the IT effort typically required for manual resolution of patch deployment failures.[28]
- Remotely reduce by up to 96% the manual IT effort traditionally required for major software malfunctions.[28]

Benefits and functionality of KVM Remote Control include:

- Because KVM Remote Control is designed into the hardware of 2nd gen Intel Core vPro processors, it eliminates the need to purchase and maintain a separate, costly, data-center KVM switch in the production environment.
- To improve convenience for technicians, KVM Remote Control now supports higher screen resolutions—up to 1920 x 1200 with 16-bit color.
- KVM Remote Control works for PCs both inside and outside the corporate firewall.
- KVM Remote Control is now available on both dual-core and quad-core 2nd gen Intel Core vPro processors with built-in visuals.

Receive alerting anytime from the PC

- **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.

Minimize user involvement in maintenance and repair, even if the PC is outside the corporate firewall

Intel vPro technology includes capabilities that address the critical IT priority of supporting laptops. These capabilities allow IT to establish secure communication with the PC, even if it is outside the firewall.

- **Remote power up,** through Serial over LAN (SOL), a more secure approach than Wake on LAN (WOL). Authorized technicians can use this capability to remotely and automatically wake PCs off-hours for maintenance work or servicing.
- **Fast call for help** for wired or wireless systems, even beyond the firewall. This capability 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.

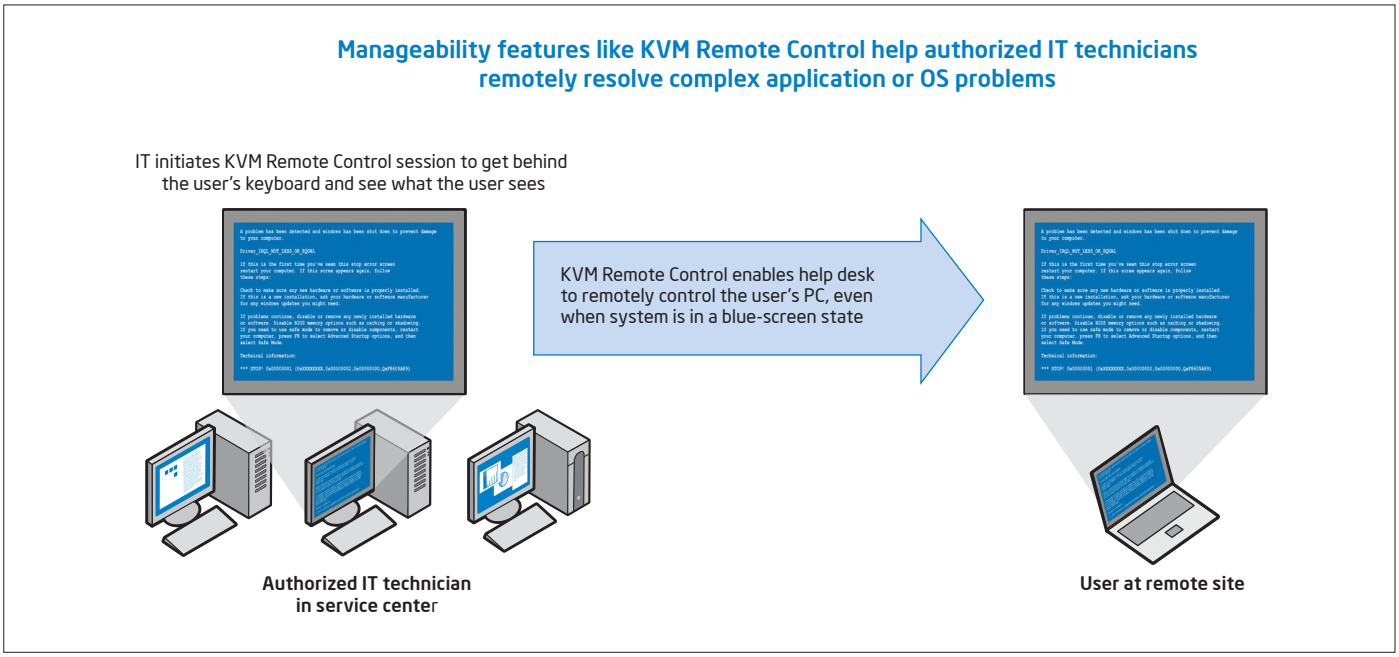


Figure 6. Improved remote manageability with KVM Remote Control allows authorized IT technicians to resolve complex PC problems, such as blue screens, without leaving the service center.

- **PC Alarm Clock,**[22] a 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 the PC is outside the corporate firewall.

PC Alarm Clock—local wake from any sleep state[2]

PCs with 2nd gen Intel Core vPro processors include the harware-based PC Alarm Clock capability. PC Alarm Clock is a secure, policy-based client-side (local) scheduled power-on.

Two forms of this feature—BIOS timers and ACPIs—exist in the market today. However, BIOS timers are not universally available or easy to configure. ACPIs allow wake only from S3 and S4.

In contrast, 2nd gen Intel Core vPro processors' alarm-clock feature allows PCs 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. The feature works even if there is no communication with the PC. This means that IT administrators can use the built-in wake-up capability to schedule tasks even for PCs that are not on the network. For example, software vendors, such as McAfee, can use the feature to enable IT-scheduled product updates even for businesses that don't have an IT console.

Potential uses for PC Alarm Clock include waking PCs:

- To ensure that virus scans run according to policy and 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.

As with other hardware-based capabilities of Intel vPro technology, 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.

Remotely access critical system information for easier diagnostics

Intel vPro technology stores critical system information in protected memory that is not on the hard drive. This allows an authorized technician to remotely access system information that can help with troubleshooting, diagnostics, and repair—even if the OS is not available, the hard drive has failed, or the PC is powered off. Critical system information available out-of-band includes:

- **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.[22]

Wake on LAN (WOL) vs. Serial over LAN (SOL) secured via Transport Layer Security (TLS)

Wake on LAN can provide IT technicians with a remote power-up ability, but it does not have strong encryption, and so has weak authentication. Because of its inherent security (and configuration) issues, many IT organizations disable or avoid using WOL. In turn, users typically have to leave their PCs and laptops powered on 24/7 so IT technicians can remotely service the systems off-hours.

2nd gen Intel® Core™ vPro™ processors use Serial over LAN (SOL), a more secure way to remotely wake the PC. These 2nd gen Intel Core vPro processors use Transport Layer Security (TLS) with Advanced Encryption Standard (AES) 128-bit encryption and RSA keys with modulus lengths of up to 2,048 bits, in order to secure the out-of-band communication tunnel between the PC and the management console. Using SOL with TLS allows a secure remote power up even in network environments that require TLS-based security, such as IEEE 802.1x, Cisco Self Defending Network (SDN)*, and Microsoft Network Access Protection (NAP)* environments.

Users can now power down at the end of the work shift—or IT can establish an automated policy to shut down systems to save power. When off-hours service is needed, an authorized IT technician can wake the PCs via the Intel® vPro™ technology SOL power-up feature. This helps businesses conserve power, reduce energy bills, and still improve remote services.

Accurate, remote discovery and inventory for wired or wireless systems

On average, a significant percentage of a business's PCs are not in compliance at any given time. Adding to this problem is the difficulty in getting accurate software inventories. For example, software inventories for laptops fail up to 62% of the time.[16] 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 2nd gen 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 2nd gen Intel Core vPro processors, IT technicians can now remotely, securely, and automatically:

- 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.[16]
- 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.
- Identify noncompliant PCs even if management agents have been disabled.

These capabilities provide visible benefits that not only help IT speed up and automate services, but save substantially on inventory costs:

- Reduce laptop inventory failures by up to 62%.[16]
- Improve accuracy of inventory for previously undetected software by up to 47%.[16]
- Improve accuracy of automatic hardware asset inventory by up to 22%.[16]
- Improve the overall success rate of automated inventories by up to 16%.[16]

The asset management capabilities of 2nd gen Intel Core vPro processors help reduce time-consuming manual inventories and help save 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.

Power down at night and save on energy bills

Businesses are increasingly concerned about power consumption. Battery life in laptops is just one consideration. Equally as important are on-site energy costs—a significant operating expense. In addition, 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 via Intel vPro technology. IT technicians simply use the built-in remote power up/down capability in the 2nd gen Intel Core vPro processor family 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[29]

Unmanaged PCs waste energy. Simply by using the secure remote power up/down capability, some companies have recouped their investment in a PC with Intel® vPro™ technology in as little as 9 months.[29] By implementing other capabilities of a PC with Intel vPro technology, businesses can realize further savings.

Actual customer savings from moving to a PC with a Intel® vPro™ technology

When managing PCs with Intel vPro technology, businesses can experience exceptional performance while lowering power consumption and power bills.

- **Calgary Health Region:** Total projected savings of $276,800[30]
- **Cleveland Clinic:** Power savings 66% over 4 years[31]
- **EDS Call Center:** Power-efficiency improvement of 25%[32]
- **CSK (Japan):** Saved approximately $61,000 in energy costs[33]
- **State of Indiana:** Projected savings of over $1.4 million in 4 years[34]

Desktop virtualization models deliver more manageable, responsive computing

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 operating systems, and takes advantage of the smart performance available in PCs with 2nd gen Intel Core vPro processors. Virtualized applications, streamed OSs, and virtual user environments are especially useful for alternative computing models. For example, in a data center, users share PCs, and IT must support different builds based on user IDs (see Figure 7). Virtualization is also useful when users need separate environments for personal versus work areas, or when they need a highly secured environment versus a low security environment.

To enable virtualization for alternate computing models, the 2nd gen Intel Core vPro processor family includes Intel® Virtualization Technology (Intel® VT).[9] Intel VT is the technology of choice for hardware-based virtualization. Intel VT enables a flexible computing foundation with built-in security and with various alternative virtualization models enabled, so you are ready for the compute models of today and in the future.

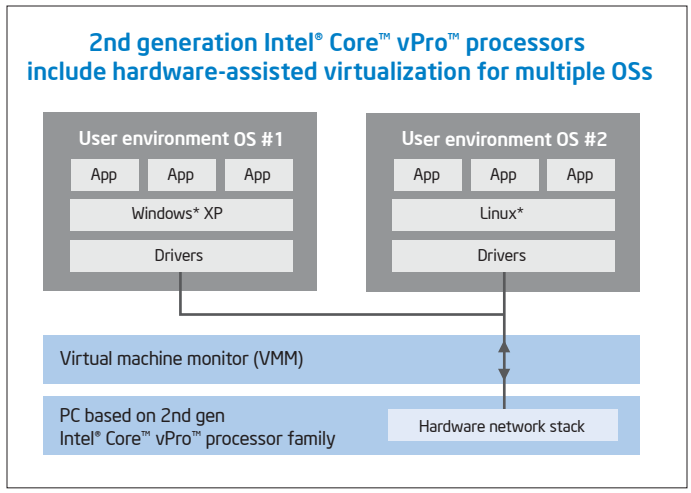


Figure 7. Virtualization provides IT with isolated, secure spaces in which to abstract or stream OSs and applications. Both next-generation and traditional virtualization is supported on laptop and desktop PCs with 2nd generation Intel® Core™ vPro™ processors.

Usage models

Virtualization can be used to support next-generation, emerging, and traditional usage models for OSs and applications. By centralizing OSs and applications, IT can minimize the burden of maintaining multiple builds, reimaging, and upgrading systems. At the same time, IT can improve security, since the primary build is secured in the data center and less exposed to threats.

2nd gen Intel Core vPro processors enable several alternate computing models:

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

Virtualization: Streaming

Streaming refers to sending software (an OS or applications) over the network for execution on the PC (see Figure 8). 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 PC, IT does not have to absorb the large data center build-out required by server-side compute models. Also, users enjoy the more responsive application experience of local software execution.

- **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 data center 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 2nd gen Intel Core vPro processors support both OS streaming and application streaming. Application streaming products are available from several software vendors.

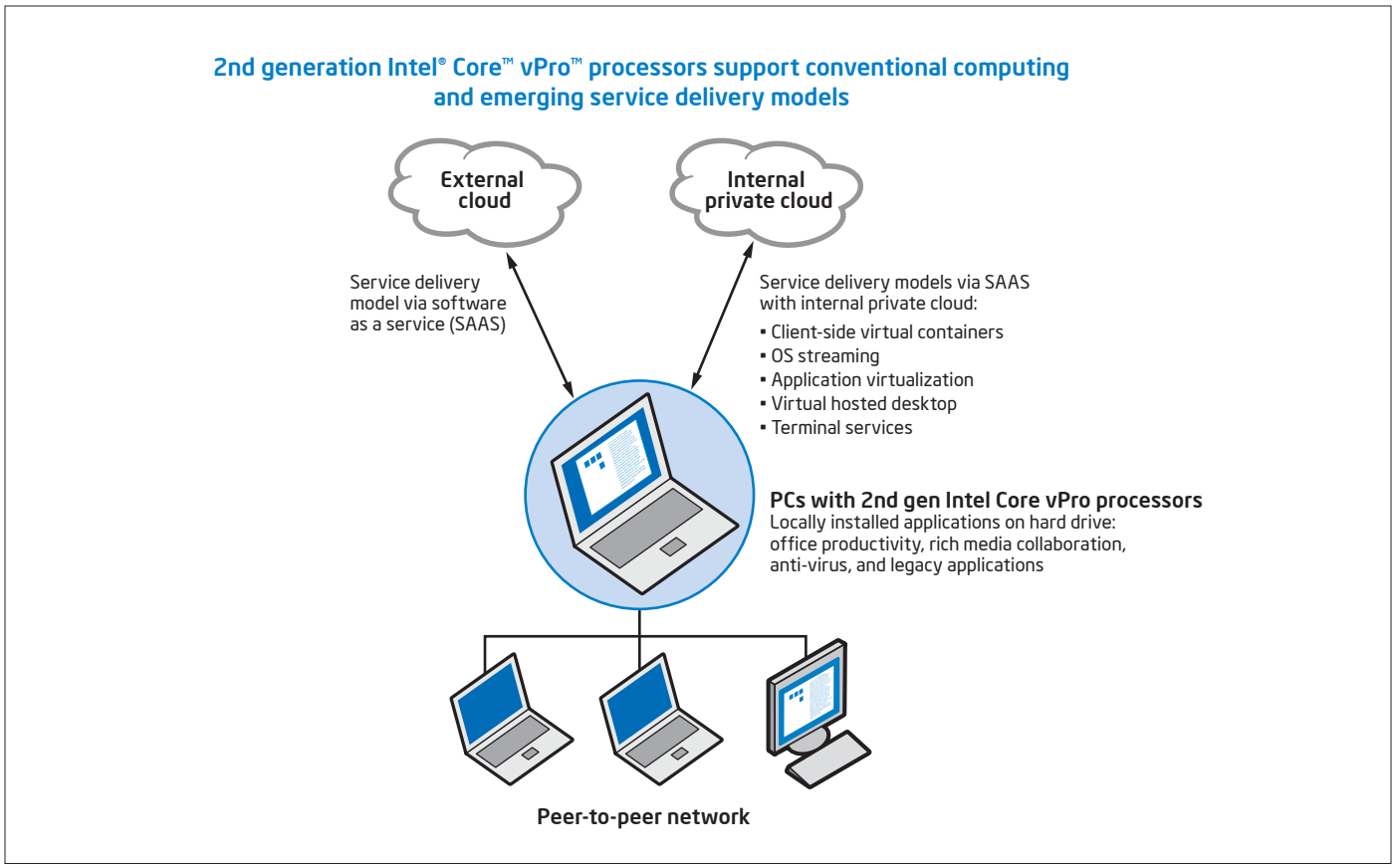


Figure 8. PCs with 2nd generation Intel® Core™ vPro™ processors support conventional computing and emerging service delivery models. Emerging service delivery models include software as a service, in which the software application is delivered from an external vendor or from an internal source.

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.

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.[24] 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 2nd gen Intel Core vPro processors.

Intel's Cloud 2015 Vision: Client-aware computing

As the workforce becomes more mobile, users become more versatile, working from multiple locations on a variety of devices. Unfortunately, when it comes to the ability to access, display, manipulate, or secure data, some devices are more capable than others. One of the issues with delivering services to such devices is that most Internet services simply "dumb down" delivery to the most basic definition of the device. Services might recognize the device's screen size or display type, but typically have only a limited ability to take advantage of other capabilities.

Because mobile users are creating, manipulating, and collaborating on more complex digital content, it's no longer enough to know only the screen size in order to determine how to deliver the service. Applications must know how much memory is in the device; what kind of performance capabilities the device has for video, graphics, and encryption/decryption; how much battery life is remaining; and what kind of security and communications technologies are built in. For example, applications must be able to verify security before allowing applications to execute on the end point.

Three elements to cloud vision 2015

Intel's cloud vision addresses key issues of delivering content to devices in an appropriate format. This vision has three main elements:

- Communications, data, and services should move easily within and across cloud computing infrastructures.
- Cloud computing services and resources can be specified, located, and securely provisioned with little or no human interaction.
- Cloud computing solutions adapt seamlessly to the end user's device and usage model, regardless of the type of client system in use—desktop PC, laptop, tablet, PDA, smart phone, etc.—and irrespective of how the users are moving their work between devices.

Intel's vision for cloud computing addresses these issues from the perspective of both the data center and the end user, and is expected to change the way IT services are created, delivered, and consumed. At a time when data centers face increasingly rapid growth and a staggering volume of data, cloud computing promises large gains in efficiency and flexibility. End users also benefit significantly from a better experience across a range of devices, and from devices that are interoperable, rather than those that support only a single, standalone functionality.

Intel is already investing in the development of application programming interfaces (APIs) that will enable cloud-based applications to be aware of client capabilities. For an initial set of APIs that will help you add new, competitive functionality to your applications, visit the Intel Web site at http://software.intel.com/sites/whatif/webapis.

Table 5. Virtualization support in laptop and desktop PCs.

Advanced technology	Offers	2nd gen 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 to create separate virtual machines (VMs) and provide near-native graphics performance for those VMs	Yes
Support for virtual containers	Temporary virtual machines ("containers") that support virtual user environments and isolate streamed OS and applications	Yes
Intel® TXT[24]	Trusted launch of the VMM and protection of secrets during proper or improper shutdown	Yes

Intel® VT is compatible with other technologies

Standard memory, storage, and graphics cards work with Intel VT.[9] The latest laptop and desktop PCs with 2nd gen Intel Core vPro processors 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 with the 2nd gen Intel Core vPro processor family, 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 that are off the network, while streaming applications or OSs to users on other systems that are still in the network.
- **Performance.** Great user experience with local, hardware-level acceleration for local processing and video.
- **Leading ISV support** from Citrix, Symantec, and Microsoft.

Managing laptops—cut costs and improve productivity

Employees are increasingly required to access enterprise applications while away from the office. Now that more powerful, seamless software tools are available—such as video conferencing, streaming OS virtualization, and real-time application streaming—working off-site has become easier than ever, and more important to business. In fact, up to 82% of employees require access to enterprise applications and data while away from their desks.[35]

Wireless mobility

2nd gen Intel Core vPro processors include many capabilities to support an increasingly mobile workforce, including virtual location workforces and remote office LAN replacements. For example, laptops with 2nd gen Intel Core vPro processors include proven Intel® Centrino® wireless products, such as the new, uniquely powerful Intel Centrino 6000 wireless adapter. The adapter is Intel's second-generation 450 Mbps Wi-Fi adapter.

The Intel Centrino 6000 wireless adapter comes in 2 SKUs:

- 450 Mbps Premium SKU, which is sometimes called 3x3 or Multi-Stream. The 3x3 adapter provides up to 8X bandwidth/speed increase compared to 802.11a/b/g's 54 Mbps.[19]
- 300 Mbps Mainstream SKU, which is sometimes called 2x2 or Dual-Stream. The 2x2 adapter provides up to a 5X bandwidth/speed increase compared to 802.11a/b/g's 54 Mbps.[19]

Improved reception and fewer drop-offs for wireless users

Many laptops include only 1 antenna for wireless connectivity. This has traditionally meant that moving the laptop a few inches or changing the viewing angle could cause a drop in performance.

In contrast, PCs with 2nd gen Intel Core vPro processors include up to 3 WiFi antennas and provides better and more consistent business-class WiFi performance. This is definitely a case of "more is better." With more antennas, signals can be received from more angles with greater integrity and fewer dropoffs, regardless of the laptop's position.

Intelligent, responsive, energy-efficient performance

One of the key pain points in using older PCs is lack of performance—newer applications are not always responsive on older hardware. In contrast, 2nd gen Intel Core i5 vPro processors can run business productivity applications up to 60% faster than a 3-year-old PC.[10] Also, with strict new data-breach regulations in effect, compliance is becoming more important. Performance gains that speed up encryption and decryption can make a visible difference, not only in greater user productivity on secure systems, but also in reducing user frustration, which in turn can help motivate users to leave encryption in place.

Some of the performance and efficiency features of 2nd gen Intel Core i5 vPro processors include:

- Protection of confidential data up to 4x faster.[10]
- Adaptable performance through new Intel Turbo Boost Technology 2.0, which can accelerate the processor speed when higher performance is needed.[10]
- Up to 2x faster multitasking.[10]
- Up to 60% faster on business productivity applications.[10]

The new processors provide enough performance not just for today's applications, but also for future, heavily threaded OSs and applications. In addition, 2nd gen Intel Core vPro processors can help improve productivity by automatically and intelligently adjusting to each user's needs.

Intel® Turbo Boost Technology 2.0

Intel Turbo Boost Technology 2.0 is exciting performance technology embedded in the 2nd gen Intel Core vPro processor family. Intel Turbo Boost Technology 2.0 manages power and thermal headroom to optimize performance. Basically, it is an intelligent allocation of extra processing power to match the workload of the applications that need it most.

For example, see Figure 9 (shown on the next page). If the processor is operating below its maximum power, current, and temperature specifications, Intel Turbo Boost Technology 2.0 can accelerate the processor speed[10] to provide additional performance for an application that needs more compute power.

In essence, Intel Turbo Boost Technology 2.0 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 Technology 2.0 is dependent on the number of active cores in the processor. The amount of time the processor spends in the Intel Turbo Boost Technology 2.0 state depends on the workload and operating environment. With today's compute-intensive applications and increased demand for encryption applications, this is a key technology that can improve productivity for both existing and future applications.

4-way or 8-way multitask processing

Multitask processing enables 2nd gen Intel Core vPro processors to execute 4 or 8 tasks at the same time. 2nd gen Intel® Core™ i3 processors and 2nd gen Intel Core i5 processors deliver 4-way multitask processing (see Figure 10). All desktop PCs with 2nd gen Intel Core i7 processors and some laptops with 2nd gen Intel Core i7 processors enable 8-way multitask processing.

This 4-way or greater multitask processing reduces computational latency: Every clock cycle can be 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. This also

Significant performance gains for SATA/SSD

SATA solid state drives (SSDs) are becoming a standard feature in today's PCs. These drives reduce the performance bottleneck that currently exists between the I/O and hard drive. SSDs can speed up access to I/O and substantially reduce hard drive failures.

PCs with 2nd generation Intel® Core™ vPro™ processors deliver substantial I/O performance gains for SATA 6 Gbps/next-generation SSDs. This increases the PC's responsiveness, with noticeably faster booting and application loads, higher reliability, and longer battery life in laptops. Businesses that choose to use a SATA 6 GB/s SSD can lower the PC's energy use further via SATA Link Power Management.

SATA 6 Gbps SSDs use the same cabling and connectors and are backwards compatible with SATA 1.5 Gbps and SATA 3 Gbps. Intel® SSDs based on innovative, industry-leading 34 nm Intel® Flash technology offer:

- No moving parts for high reliability.
- The quality and reliability you expect from Intel, the leading manufacturer of PC processor technology.
- Lower power consumption than a traditional hard drive.

helps processors use only the power needed for the task at hand. Multiple threads execute simultaneously only when there are multiple tasks to be processed at the same time.

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.

ENERGY STAR* compliance and energy efficiency

The 2nd gen Intel Core vPro processor family is ENERGY STAR compliant.[21]

These systems also take advantage of deeper processor sleep states and lower idle power. With intelligent power management, idle cores can reduce their power consumption so that the system consumes only the power it needs based on actual user workload.

Stunning visual performance with built-in visuals

2nd gen Intel Core vPro processors include built-in visuals and are now available on dual-core and quad-core processors. These integrated graphics provide the capability that a corporate PC needs, to support collaboration and digital content creation. These built-in visuals eliminate the need for a dedicated graphics card, as well as the cost burden and power requirements associated with an additional card.

The built-in visuals of 2nd gen Intel Core vPro processors deliver dynamic frequency, quick-sync video, and scaled performance that accelerates graphics performance when users need it. The graphics power-sharing algorithm works in concert with Intel Turbo Boost Technology 2.0 to deliver performance when and where it's needed.

The built-in visuals are on the silicon, next to the processor core, and are tightly integrated with the processor. They share the same cache as the processor—there is no memory controller hub between them. This means faster access to memory and better performance in general for graphics-intensive applications. Also, because the graphics are built in, they consume less power than a dedicated graphics card, providing an even more energy-efficient PC.

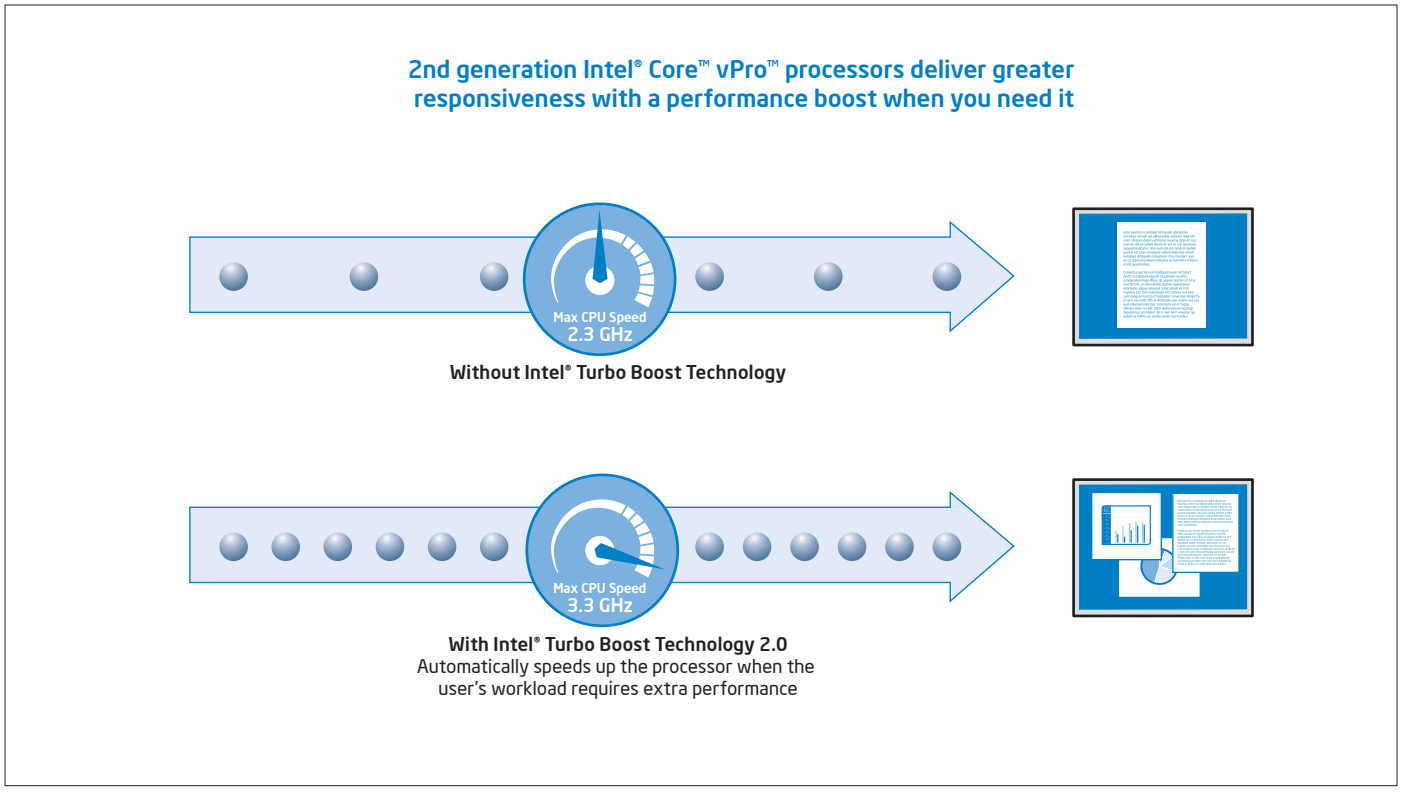


Figure 9. Intel® Turbo Boost Technology 2.0 accelerates the processor speed to provide additional performance for compute-intensive applications.[9] When accelerated performance is no longer needed, the processor drops back to deliver only the power required for the current application(s). (Speeds shown are based on a 2nd generation Intel® Core™ i5-2500T processor.)

No more front-side bus (FSB)

The 2nd generation 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™2 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 2nd gen 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. 2nd gen Intel Core vPro processors include:

- 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 2nd gen 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 2.0[6]	Dynamically accelerates processor speed (if processor load allows) when faced with a demanding task.	Faster (higher number)
Multitask processing	The ability for the processor to process multiple tasks simultaneously. Greater multitask processing enables faster multitasking and improved performance with multi-threaded applications.	More (higher number)

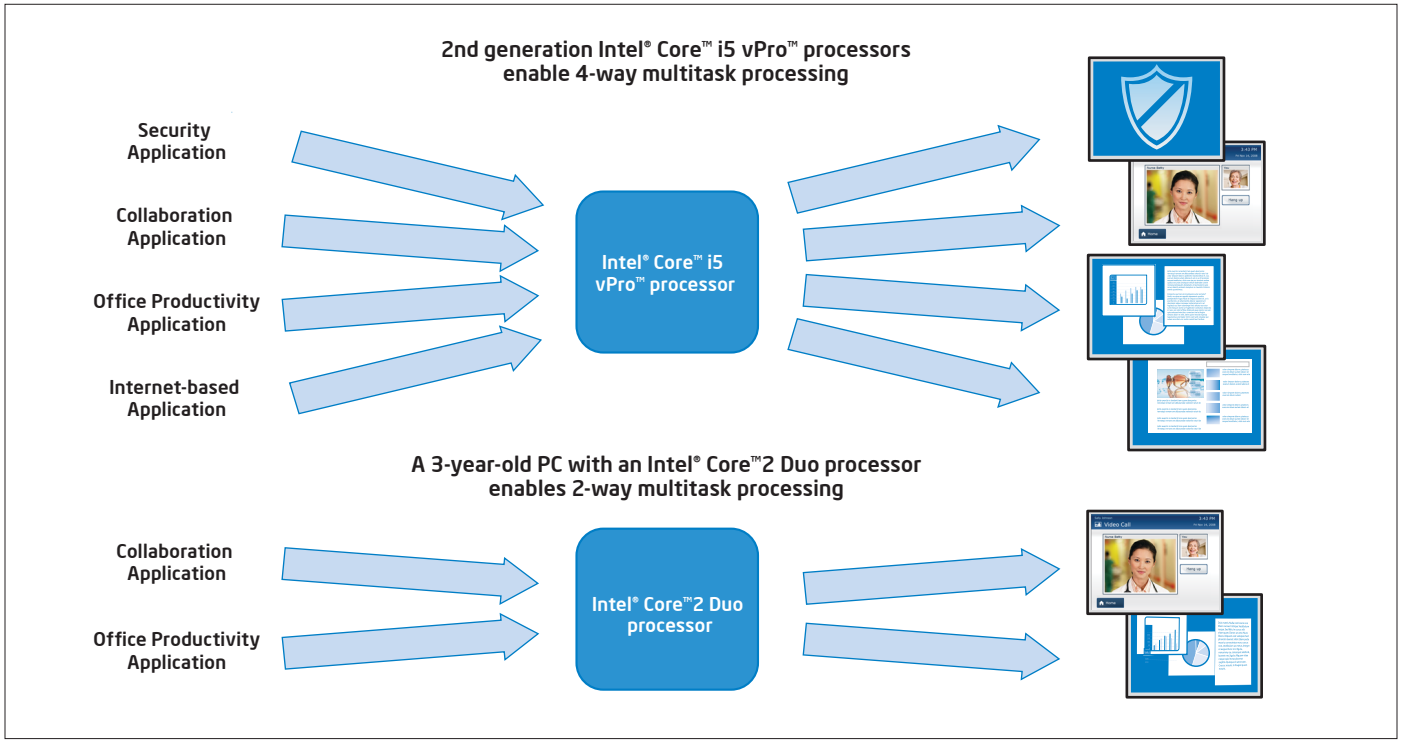


Figure 10. Enhanced multitasking. 2nd gen Intel® Core™ vPro™ processors enable 4-way or 8-way multitask processing. This can dramatically increase performance and help users move seamlessly between office applications.

Simplify and speed up activation

The 2nd gen 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. Security credentials for activation in the service environment must be established before you configure Intel vPro technology for remote management. This includes activating Intel® Active Management Technology (Intel® AMT), a critical component of Intel vPro technology.

IT administrators can choose the level of security and automation appropriate for their network environments.

General activation process for Intel® AMT

Activating Intel AMT in PCs with 2nd gen Intel Core vPro processors 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 on the target PC. 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 2nd gen Intel Core vPro processor family-based PCs into the management application. Once these steps are complete, Intel AMT is activated, and IT administrators can start taking advantage of the built-in intelligent security and remote manageability capabilities.

Methods to establish security credentials for Intel AMT

2nd gen Intel Core vPro processors support different processes for setting up security credentials on the PC and management console for Intel AMT. 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 for Intel AMT

2nd gen Intel Core vPro processors support four configuration models to allow for flexible activation:

- **Host-based configuration** to speed up activation of Intel AMT and allow activation in a method similar to a software update. This method is typically used by very small businesses that do not have security certificates. This method allows an in-house IT administrator to remotely configure Intel AMT using a software-based agent on the PC. This activation method uses in-band communication, and depends on the integrity of the software agent already established between the IT console and the PC, and between the software agent and Microsoft Windows. This method does not use HTTP Digest for authentication. There is no encryption applied to management traffic. Security is the responsibility of the user. For example, if another machine (such as the IT administrator's machine) tries to initiate a KVM Remote Control session, remote reboot, or other IT task on the user's PC, the system displays a pop-up message asking permission. The user must opt-in to allow remote control of their machine. If the business later establishes a manageability console or server that can handle certificates, the business can reconfigure Intel AMT to increase security to a higher level.

***Note:** For companies that have only a few machines and do have the ability to set up a server that can handle certificates, it is better to do one-touch configuration to provide better security and minimize user involvement.*

- **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 2nd gen Intel Core vPro processors allow IT to remotely configure these security options. Note that not all management console vendors provide support to configure all security options.

Migrating to a new firmware version

PCs with 2nd gen Intel Core vPro processors include Intel AMT 7.x firmware. IT administrators can choose the version of Intel AMT 7.x firmware to deploy. This helps businesses maintain consistency in their firmware infrastructure even as they upgrade PCs.

Easier migration to Windows* 7

PCs with 2nd gen Intel Core vPro processors help manufacturers deliver stable, standardized PCs. These laptop and desktop PCs have broad industry support and are ready for OSs, such as Windows* 7, and applications of the future.

- **Easier maintenance:** Upgrade to Windows 7 quickly, remotely, and overnight without losing access to your legacy applications (see Figure 11).
- **Strong security:** Protect data from unauthorized viewing with faster encryption with Intel Core vPro processors, such as for Windows 7 BitLocker Drive Encryption.
- **Greater productivity:** 2nd gen Intel Core vPro processors help the system start up and shut down fast, and deliver faster multitasking, faster information search, and easier connections (see Figure 12).
- **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.

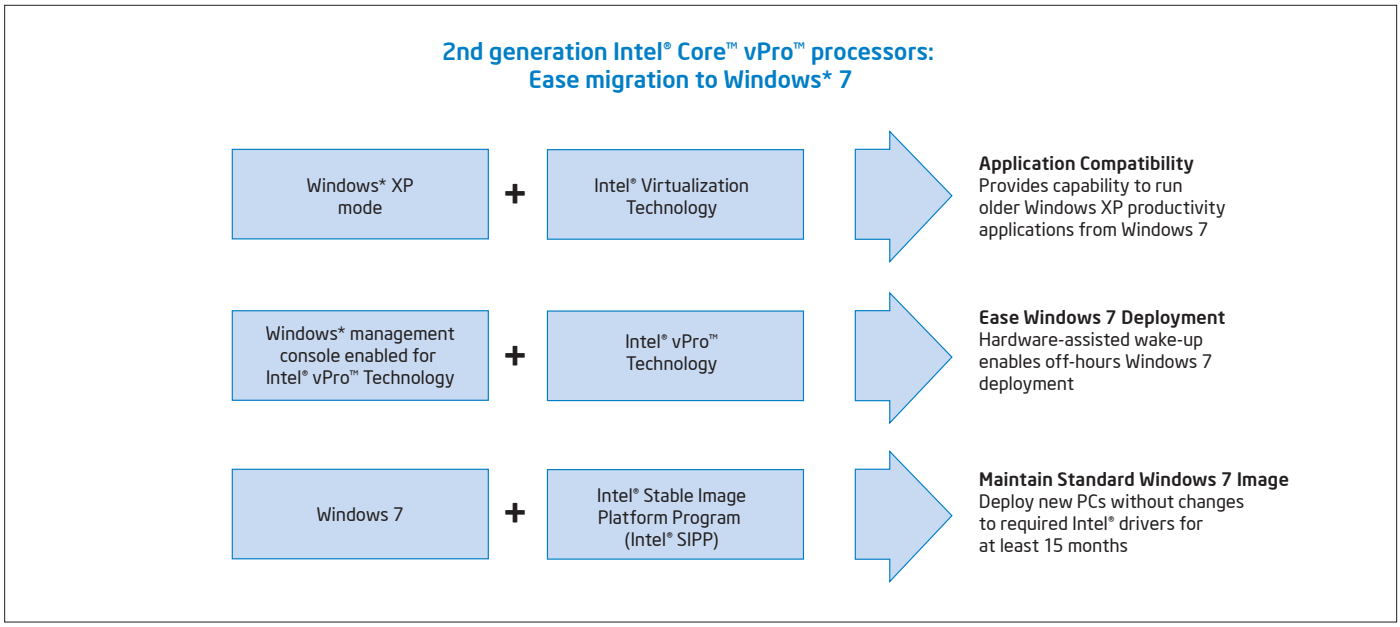


Figure 11. PCs with 2nd gen Intel® Core™ vPro™ processors make it easier to migrate to Windows* 7.

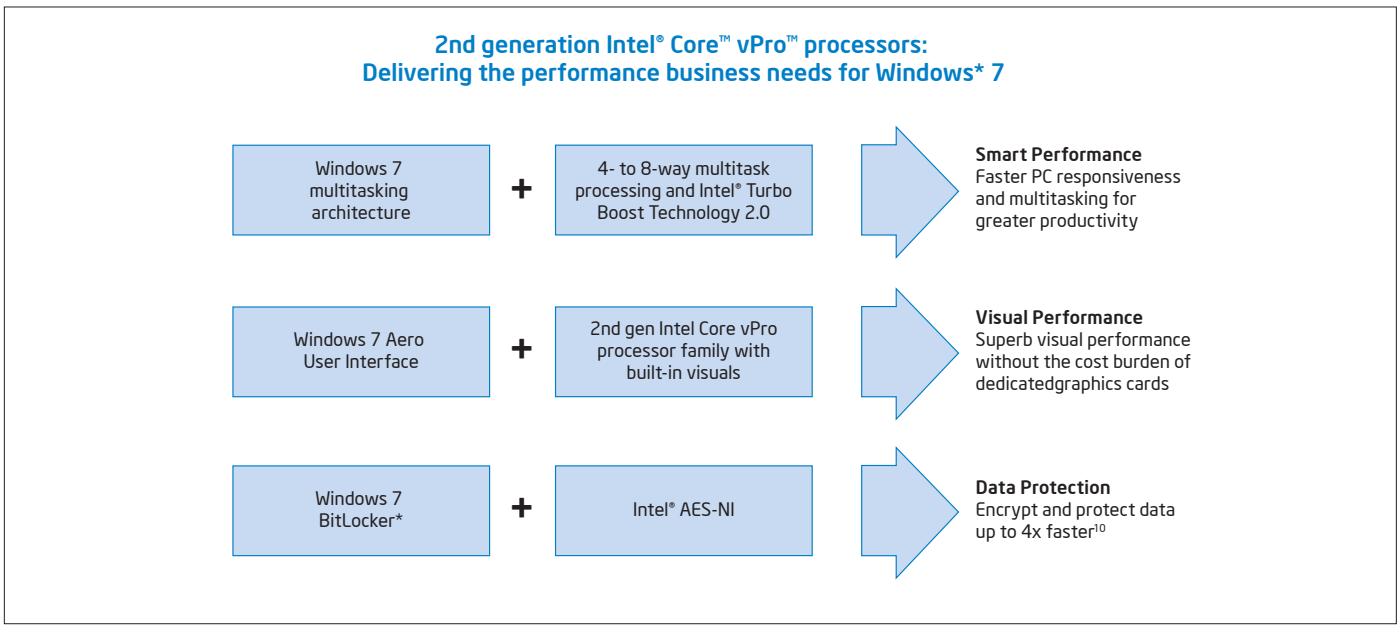


Figure 12. PCs with 2nd gen Intel® Core™ vPro™ processors deliver the performance needed for Windows* 7.

Stable, standards-based, and with broad industry support

To help industry get the most from its technology investments, PCs with 2nd gen Intel Core vPro processors are:

- **Built on standards.** The 2nd gen 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 2nd gen Intel Core vPro processor family is built include XML, SOAP, TLS, HTTP authentication, Kerberos, DASH, and WS-MAN.
- **Broadly supported by the industry.** The 2nd gen Intel Core vPro processor family is supported by major software vendors in security software, management applications, and business software. PCs with 2nd gen Intel Core vPro processors 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 2nd gen Intel Core vPro processors are available under the Intel® Stable Image Platform Program (Intel® SIPP), so businesses can avoid unexpected changes that might force software image revisions or hardware requalifications.[20] Intel SIPP for 2nd gen Intel Core vPro processors begins in February 2011, 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.

The ultimate in visibly smart performance for business

The 2nd generation Intel Core vPro processor family delivers top-of-the-line benefits in security, manageability, and cost effectiveness. This processor family delivers "always available" access to the PC both inside and outside the corporate firewall, intelligent security that proves compliance even after a PC is stolen, improved remote manageability, and remote control to resolve even the most complex issues without leaving the help desk. The robust features built in these PCs allow IT to automate more processes, improve efficiencies, and reduce service costs. With responsive, up to 8-way multitask processing and support for Windows 7, your users will also enjoy enhanced multitasking and better adaptive performance, along with the stunning speed of these latest-generation processors. See the benefits of built-in IT intelligence and smart performance. That's what visibly smart is all about.

To learn more about the built-in intelligence of security and remote manageability in laptop and desktop PCs with 2nd gen Intel Core vPro processors, visit www.intel.com/go/vpro101.

To blog with the pros who have deployed PCs with 2nd gen Intel Core vPro processors, visit www.intel.com/go/vproexpert.

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

[2] Intel® Active Management Technology (Intel® AMT) requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup & configuration. For more information, visit http://www.intel.com/technology/platform-technology/intel-amt.

[3] Intel® Advanced Encryption Standard-New Instructions (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. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

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

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

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

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

[8] Available on the 2nd gen Intel® Core™ processor family. Includes Intel® HD Graphics, Intel® Quick Sync Video, Intel® Clear Video HD Technology, Intel® InTru™ 3D Technology, and Intel® Advanced Vector Extensions. Also optionally includes Intel® Wireless Display depending on whether enabled on a given system or not. Whether you will receive the benefits of built-in visuals depends upon the particular design of the PC you choose. Consult your PC manufacturer whether built-in visuals are enabled on your system. Learn more about built-in visuals at http://www.intel.com/technology/visualtechnology/index.htm.

[9] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

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

(Mobile) Comparing pre-production Intel® Core™ i5-2410M Processor (2C4T, 2.3GHz, 3MB cache), Intel Emerald Lake CRB, 4GB (2x2GB) PC3-10700 (DDR3-1333)-CL9, Hitachi* Travelstar 320GB hard-disk drive, Intel® HD Graphics 3000, Driver: 2185 (BIOS:v.34, Intel v.9.2.0.1009) , Microsoft* Windows* 7 Ultimate 64-bit RTM Intel® Core™2 Duo Processor T7250 (2M Cache, 2.00 GHz, 800 MHz FSB), Intel Silver Cascade Fab2 CRB, Micron* 4 GB (2x2GB) PC3-8500F (DDR3-1066)-400, Hitachi* 320GB hard-disk drive, Mobile Intel 4 Series Express Chipset Family w/ 8.15.10.2182 (BIOS: American Megatrends AMVACRB1®6C.0104.B00.0907270557, 9.1.2.1008).

(Desktop) Pre-production Intel® Core™ i5-2400 Processor (4C4T, 3.1GHz, 6MB cache), Intel Los Lunas CRB, Micron* 4GB (2x2GB) PC3-10700 (DDR3-1333)-CL9, Seagate* 1 TB, Intel® HD Graphics 2000, Driver: 2185 (BIOS:v.35, Intel v.9.2.0.1009) , Microsoft* Windows* 7 Ultimate 64-bit RTM Intel® Core™ 2 Duo E6550 (2C2T, 2.33GHz, 4MB cache), Intel DG945GCL Motherboard, Micron 2GB (2x1GB) DDR2 667MHz, Seagate320 GB hard-disk drive, Intel® GMA 950, Driver: 7.14.10.1329, (BIOS:CL94510J.86A.0034, INF: 9.0.0.1011), Microsoft* Windows* 7 Ultimate 64-bit RTM.

Business productivity claims based on SYSmark* 2007, which is the 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 PCMark Vantage, a hardware performance benchmark for PCs running Windows 7 or Windows Vista, includes a collection of various single and multi-threaded CPU, Graphics, and HDD test sets with a focus on Windows* application tests. Security workload consists of SiSoftware Sandra* 2010 - AES256 CPU Cryptographic subtest measures CPU performance while executing AES (Advanced Encryption Standard) encryption and decryption algorithm. For more information go to http://www.intel.com/performance.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.]. For more information go to http://www.intel.com/performance.

[11] Source: 2009 Annual Study: Cost of a Data Breach, Ponemon Institute, January 2010.

[12] Source: Adobe Flash Player Enterprise Penetration, Adobe, last retrieved August 16, 2010, - http://www.adobe.com/products/player_census/flashplayer/enterprise_penetration.html.

[13] Source: Business Internet traffic increases to Facebook and YouTube, Kate Hartley Carrot Communications, 15 April 2010, http://www.network-box.com/node/533.

[14] Source: "Gartner Identifies the Top 10 Strategic Technologies for 2011" Gartner, Oct 19, 2010. http://www.gartner.com/it/page.jsp?id=1454221.

[15] Source: Increasing productivity with Mobile Business PCs, IT@Intel, May 2010, http://download.intel.com/it/pdf/Increasing_Productivity_with_Mobile_PCs.pdf.

[16] 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.

[17] Using Total Cost of Ownership to Determine Optimal PC Refresh Lifecycles", Wipro Technologies, March 2009 (www.wipro.com/industryresearch). Based on an Intel Corporation-sponsored 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/docs/DOC-3144.

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

[19] 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.

[20] Check with your PC vendor for availability of computer systems that meet Intel® Stable Image Platform Program (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.

[21] ENERGY STAR is a system-level energy specification, defined by the Environmental Protection Agency, that relies on all system components, such as processor, chipset, power supply, etc.) For more information, visit http://www.intel.com/technology/epa/index.htm.

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

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

[24] 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.

[25] 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.

[26] Source: Ponemon Institute, 2008.

[27] "A White Paper—The cost of maintaining a PC" TechAisle March 2009 http://www.techaisle.com/White%20Paper%20-%20Cost%20of%20Maintaining%20a%20PC.pdf.

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

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

[30] 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.

[31] 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.

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

[33] 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.

[34] Source: Reducing 856,000 Pounds of CO_2 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.

[35] Source: "Increase Productivity by Providing Notebooks Beyond Road Warriors," Forrester Consulting, October 2008 http://ipip.intel.com/go/wpcontent/uploads/2009/06/increase-productivity-byproviding-notebooks-beyond-the-road-warriors.pdf.

Printed in USA 0411/GK/OCG/XX/PDF Please Recycle 324823-002US