



White Paper
Intel® Centrino® 2 with
vPro™ Technology
Intel® Core™2 Processor
with vPro™ Technology

Intel® Centrino® 2 with vPro™ Technology and Intel® Core™2 Processor with vPro™ Technology

Remotely manage both wired and wireless PCs from the same IT console with hardware-assisted security and remote manageability

The latest notebook and desktop PCs with Intel® vPro™ technology build on proven capabilities to enable even greater proactive security, enhanced maintenance, and improved remote management:

- Intel® Centrino® 2 with vPro™ technology-based notebooks
- Intel® Core™2 processor with vPro™ technology-based desktop PCs

These PCs deliver down-the-wire security and manageability capabilities – even if PC power is off, the operating system (OS) is unresponsive, software agents are disabled, or hardware (such as a hard drive) has failed. Remote configuration in both notebook and desktop PCs helps information technology (IT) managers deploy thousands of systems without making a deskside visit. New wireless manageability improves remote management for notebooks even when the system is asleep or off. And now IT managers can communicate more securely with notebooks on an open LAN outside the corporate firewall. These notebook and desktop PCs are also ready to run traditional virtualization with multiple OSs, as well as support emerging uses – such as application and data virtualization – and do so faster and in a more secure, trusted environment. The latest notebook and desktop PCs with Intel vPro technology deliver significantly improved 64-bit performance for compute-intensive tasks – and includes fully integrated powerful graphics support – all in a power-efficient package that is Microsoft Windows Vista* ready.



Table of Contents

Executive Summary	3
Notebook and desktop PCs with Intel® vPro™ technology	4
Today's IT challenges	4
Security and remote manageability on the chip	4
Best for business: Remote maintenance, management, and security virtually anytime	6
Simplify maintenance, improve compliance, increase automation, and reduce service calls	7
Use an existing management console for both notebook and desktop PCs	9
Managing the wireless notebook	9
Manage notebooks regardless of power state	9
Help secure and manage notebooks outside the corporate firewall	9
Improved power-management and energy efficiency	10
Secured out-of-band PC management	11
Remote-communication channel runs outside the OS	11
More secure communication outside the corporate firewall	12
Robust security methodologies for communication	12
Best for business: Deep, built-in self-defense	13
New layers of defense	13
Out-of-band management even with 802.1x, Cisco SDN, and Microsoft NAP	13
Intel® Trusted Execution Technology (Intel® TXT)	14
Automated, continual checking for agents	14
Push updates down the wire — regardless of PC power state	15
Filter threats and isolate PCs automatically based on IT policy	15
Receive alerts even if a system is off the corporate network	16
Substantially improve efficiencies for remote maintenance and management	16
Resolve more problems remotely	16
Accurate, remote discovery and inventory for wired or wireless systems	18
Put a new tool in your security toolbox: hardware-assisted virtualization	19
Two virtualization models	20
Model 1: Traditional virtualization, with multiple, fully functional OSs	20
Model 2: Emerging uses	20
Virtualization improved by Intel® vPro™ technology	21
Reducing complexity and overhead	21
Existing security: Virtualization for memory and the CPU	21
Improved isolation and security: Virtualization for Directed I/O	21
Establishing a trusted execution environment	21
Intel® Trusted Execution Technology (Intel® TXT)	21
Building the chain of trust	21
Protection for secrets during application shutdown or power transition	22
Intel® VT compatible with other technologies	22
Roadmap for virtualization technology	22
Simplify and speed up remote configuration	23
Methods to deploy notebooks and desktops with Intel® vPro™ technology	23
Configuration process	23
Certificate-based remote configuration option	23
Key-based one-touch configuration option	24
When your business needs to respond, your PCs will be responsive	24
Best for business: Improved performance, energy efficiency and eco-smart computing	24
Ready for the future	25
Stable, standards-based, and with broad industry support	25
Wired or wireless: Security and manageability on the chip	26

Executive Summary

Proven Intel® vPro™ technology is built into notebook and desktop PCs to extend the reach and functionality of the management console and meet your critical IT challenges. This hardware-based technology delivers security and manageability on the chip through:

- Intel® Centrino® 2 with vPro™ technology-based notebooks.
- Intel® Core™2 processor with vPro™ technology-based desktop PCs.¹

IT technicians can now protect, maintain, and manage notebook and desktop PCs – even if PC power is off, the OS is unresponsive, hardware (such as a hard drive) has failed, or software agents are missing.¹ IT administrators can quickly identify and contain more security threats, remotely maintain PCs virtually anytime, take more accurate asset and hardware/software inventories, resolve more software and OS problems faster down-the-wire, and accurately diagnose hardware problems – all without leaving the service center. Technicians can even securely update, troubleshoot, repair, and receive alerts from notebooks on an open LAN outside the corporate firewall.

With Intel vPro technology, IT managers benefit from lower support costs, easier and more automated maintenance, improved security, increased compliance and more accurate inventories. In turn, companies can see significantly fewer service depot and deskside visits, and less interruption to business.

The latest Intel-based notebook and desktop PCs also deliver significantly improved performance for compute-intensive applications and multitasking – all in a power-efficient package that is Microsoft Windows Vista* ready. These PCs also include additional, hardware-based capabilities that let users run traditional and emerging virtualization applications in a faster, separate environment.

IT organizations can now spend less time on routine tasks, and can focus resources where they are most needed.

Notebook and desktop PCs with Intel® vPro™ technology

Notebook and desktop PCs with Intel vPro technology deliver down-the-wire security, enhanced maintenance, and remote management designed right into the chip.

Today's IT challenges

Information technology (IT) managers have a critical need for capabilities that make it easier to secure and manage notebook and desktop PCs. Key IT challenges today include:

- A dramatic increase in malicious attacks on PCs.
- A critical need to reduce user downtime caused by malicious attacks; problem PCs; maintenance; security updates; application upgrades; and other IT tasks.
- Financial and legal pressure to accurately inventory assets.
- Escalating demand for IT services that strain IT budgets.

Typical security and management solutions are software-based. Because of this, IT has been unable to work around a fundamental limitation: They cannot protect or manage a PC that is powered off, whose OS is unresponsive, or whose management agents are missing.

With today's need for increased security and for establishing well-managed environments, the cost of managing PCs has become a significant percentage of the total cost of ownership (TCO) of technology. A critical capability that would help IT do more with the resources they have is the ability to protect and remotely manage both notebook and desktop PCs, regardless of power state, wired or wireless state, or the state of the OS.

Security and remote manageability on the chip

Enter notebook and desktop PCs with Intel® vPro™ technology:

- Intel® Centrino® 2 with vPro™ technology for notebooks.
- Intel® Core™2 processor with vPro™ technology for desktop PCs.

The latest notebook and desktop PCs with Intel vPro technology are based on proven technology designed to address the top IT challenges in security and manageability.¹ With capabilities that are based in hardware, not software, these notebook and desktop PCs deliver even more powerful security, maintenance, and management capabilities to enhance management consoles. These PCs also offer full, secure remote deployment to help IT managers eliminate deskside visits during large roll-outs.

Challenge	Solution with Intel® vPro™ technology
Systems unmanageable when powered down	<p>Remotely and securely monitor and manage PCs anytime:</p> <ul style="list-style-type: none"> ▪ 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.
Unsecured communications with notebooks outside the corporate firewall	<p>More securely communicate with notebooks inside or outside the corporate firewall:</p> <ul style="list-style-type: none"> ▪ Establish a secure tunnel (for updates, diagnostics, and repair), to notebooks on an open LAN even outside the corporate firewall.
Spiraling and costly deskside visits	<p>Significantly reduce deskside visits with:</p> <ul style="list-style-type: none"> ▪ 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.
Unprotected assets	<p>Protect assets better:</p> <ul style="list-style-type: none"> ▪ Remotely power up PCs anytime to help ensure more complete saturation for patching and other updates. ▪ Built-in, programmable system defense filters and agent-presence checking for automated, hardware-based protection against viruses and attacks.
Lack of configuration compliance	<p>Ensure compliance:</p> <ul style="list-style-type: none"> ▪ Remote inventory and agent presence checking as a hardware-based, automated, policy-based service.
Costly and time-consuming manual inventories	<p>Eliminate virtually all manual inventories:</p> <ul style="list-style-type: none"> ▪ Accurate, remote asset inventories, even if PCs are powered off or management agents are missing.
Undiscoverable assets	<p>Discover virtually all PCs:</p> <ul style="list-style-type: none"> ▪ 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.

Utilizing Intel vPro technology, the hardware-based capabilities let authorized technicians remotely access PCs that have traditionally been unavailable to the management console. Technicians can now manage the wired or wireless notebook 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.

These new notebook and desktop PCs also deliver the new capabilities in an advanced, energy-efficient package with 64-bit performance and 64-bit integrated graphics support that is Microsoft Windows Vista* ready.

Notebook and desktop PCs with Intel vPro technology deliver:

- **Security** — so you can help ensure compliance down-the-wire on virtually all PCs with Intel vPro technology, ensure that third-party security software is available when needed, remotely identify viruses, worms, and other threats faster, and stop those threats more effectively, even in 802.1x and Cisco Self-Defending Network* (Cisco SDN) environments or Microsoft Network Access Protection* (Microsoft NAP) environments for notebooks.
- **Improved maintenance** — so you can streamline processes, increase automation, and dramatically improve technician efficiencies for monitoring and maintenance of all PCs with Intel vPro technology during a scheduled maintenance cycle.
- **Remote problem-resolution** — so you can accurately diagnose hardware problems and troubleshoot and resolve more software and OS problems – including OS rebuilds – without leaving the service center.
- **Remote inventory and discovery** — to help you eliminate manual inventories, improve compliance with government and industry regulations, and reduce management costs.
- **Remote configuration during deployment** – so you can remotely configure both notebook and desktop PCs without a desk-side visit, and have additional options for remote configuration using various levels of automation in an enterprise environment.

Combined with third-party management applications, the new generation of Intel vPro technology allows IT administrators to simplify maintenance, eliminate a significant number of desk-side visits, reduce overspending on existing resources, and minimize interruptions to business.

New capabilities for desktop and notebook PCs with Intel vPro technology

The key advancements in the latest PCs with Intel vPro technology include:

- Intel® Trusted Execution Technology² (Intel® TXT) is now supported for both notebook and desktop PCs with Intel vPro technology.
- Remote configuration available for wired desktop PCs and wired or wireless notebooks on a the corporate network. You can now remotely, fully, and securely configure powered-on PCs without a desk-side visit.
- Industry-standard Trusted Platform Module version 1.2 (TPM)³
- Support for 802.1x and Cisco SDN.
- Virtualization applications are now supported on both notebook and desktop PCs with Intel® Virtualization Technology⁴
- Significant performance gains for SSE4 instructions, which can significantly improve performance for compute-intensive applications.
- Performance gains of up to 4x on advanced Excel* spreadsheet calculations, over 4x on video editing, and over 2x for multitasking over previous-generation chipsets.⁵

New features in notebooks with Intel vPro technology

Along with improved remote management and security capabilities, the new notebooks based on Intel Centrino 2 with vPro technology deliver significant improvements in security, performance, energy efficiency, and battery life. Notebooks with Intel vPro technology include:

- Key capabilities are now available for wireless notebooks on AC power – *regardless of sleep state*: awake (S1), on standby (S2), hibernating (S3), suspend (S4), or off (S5). These capabilities include remote power up, remote boot, console redirection, preboot access to BIOS settings, out-of-band alerting, and access to event logs, asset information, and other critical system information.
- Notebooks can communicate securely with the management console through a secure tunnel for updates, diagnostics, and repair, when operating on an open, wired LAN outside the corporate firewall⁶
- Support for Microsoft NAP.
- Wi-Fi performance gains, with data rates of up to 450 Mbps⁷
- Smaller package size (up to 58% less package area and 60% less volume) and 25W small form factor, which enables remarkably thinner, lighter designs.⁸
- Integrated energy-saving components optimized to prolong battery life.

PCs with Intel® vPro™ technology¹

Notebook and desktop PCs with Intel® vPro™ technology deliver validated, fully integrated systems that help IT organizations improve security and remote management for both wired and wireless systems. These PCs are based on Intel® Core™2 processor to give users excellent 64-bit performance for compute-intensive applications and multitasking while delivering enhanced capabilities for IT – a unique combination of capabilities, only from Intel.

Intel® Centrino®2 with vPro™ technology for notebooks	Intel® Core™2 processor with vPro™ technology (2007) for desktop PCs
45nm Intel® Core™2 Duo processor T, P sequence 8400, 8600, 9400, 9500, 9600, and small form factor P, L, U sequence 9300 and 9400 ^{a,9}	Intel® Core™2 Duo processor E6550, E6750, and E6850; 45nm Intel® Core™2 Duo processor E8500, E8400, E8300 and E8200 ^{a,9} ; 45nm Intel® Core™2 Quad processor Q9550, Q9450 and Q9300 ^{a,9}
Mobile 45nm Intel® GS45 Express Chipset with 1066 FSB, 6 MB L2 cache, ICH9M-enhanced	Intel® Q35 Express Chipset with ICH9DO
Intel® Active Management Technology ¹ (Intel® AMT), release 4.0	Intel® Active Management Technology ¹ (Intel® AMT), release 3.x ¹⁰
Intel® 82567LM Gigabit network connection	Intel® 82566DM Gigabit network connection
Support for 802.11a/g/n wireless protocols	
Intel® Virtualization Technology ⁴ (Intel® VT) including Intel® VT for Directed I/O	Intel® Virtualization Technology ⁴ (Intel® VT) including Intel® VT for Directed I/O
Intel® Trusted Execution Technology ² (Intel® TXT)	Intel® Trusted Execution Technology ² (Intel® TXT)
Support for Cisco Self-Defending Network* (Cisco SDN*) ¹⁰ and PXE (preexecution environment)	Support for Cisco Self-Defending Network* (Cisco SDN*) ¹⁰ 1.0 and PXE (preexecution environment)
Support for Microsoft Network Access Protection	
Support for 802.1x	Support for 802.1x
64-bit enabled ¹¹	64-bit enabled ¹¹
Execute Disable Bit ¹²	Execute Disable Bit ¹²
Industry-standard TPM 1.2	Industry-standard TPM 1.2
Intel® Stable Image Platform Program (Intel® SIPP) ^{a,13}	Intel® Stable Image Platform Program (Intel® SIPP) ^{a,13}
Windows Vista* ready	Windows Vista* ready
Integrated support for 64-bit graphics, including support for Windows Vista Aero interface	Integrated support for 64-bit graphics, including support for Windows Vista Aero interface
Windows Vista* BitLocker*-ready	Windows Vista* BitLocker*-ready

^a45nm Intel® Core™2 Duo and 45nm Intel® Core™2 Quad processors will be available to the market before they are incorporated into the Intel® Stable Image Platform Program (Intel® SIPP). The processors are expected to be included in SIPP in late 2008.

Best for business: Remote maintenance, management, and security virtually anytime

Intel vPro technology capabilities are available virtually anytime, even if PC power is off, the OS is unresponsive, hardware (such as a hard drive) has failed, or management agents are missing. Some capabilities, such as agent presence checking and access to hardware asset information, are available even for wireless notebooks in the presence of a host OS-based VPN.

IT administrators now have more control where they need it: at the remote IT console for both wired and wireless PCs. Combined with third-party management tools such as management consoles and scripting, the new capabilities make it easier to secure, maintain, and manage PCs. The results can be dramatically reduced site visits; substantially improved technician efficiencies; streamlined diagnostics, repair, and remediation; and more automation of processes. In turn, this will help IT managers free up resources for other projects.

Figure 1, on the next page, shows an example of how notebook and desktop PCs can be remotely managed regardless of PC power state or the state of the OS.¹⁴

Refer to the discussion, Managing the wireless notebook, on page 9, for a list of capabilities available in wired and wireless states, active and sleep states, and various power states.

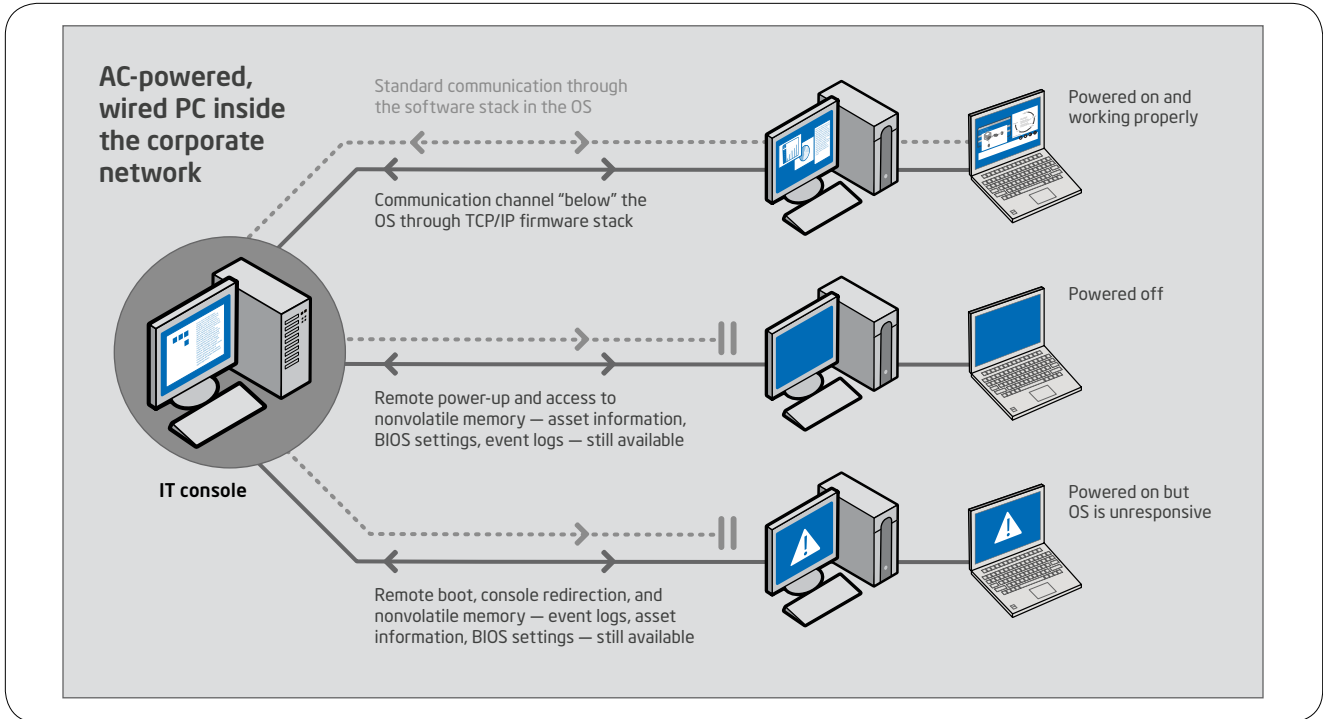


Figure 1. All capabilities are available for notebook and desktop PCs wired and on AC power. Hardware-based communication and capabilities are available virtually anytime for wired, AC-powered PCs. All key capabilities are also available for wireless notebooks within the corporate network even if the PC is powered off, its OS is inoperable, or the notebook is asleep. (Some capabilities are active only when the notebook is awake and performing a particular task.) Agent presence checking, hardware-asset tracking, and remote configuration are available even when a notebook is awake, working properly, and connected to the corporate network through a host OS-based VPN.

Simplify maintenance, improve compliance, increase automation, and reduce service calls

Intel vPro technology is designed to help IT administrators reach more PCs remotely, automate more tasks, and perform more work from a remote, centralized location. This helps business reduce user interruptions, improve work flow, and reduce the total cost of owning technology.

Tables 1 through 5 list common use cases for improved security, maintenance, and management, along with the capabilities that enable them.

Table 1. Power-management capability

Capability	What it does	Common uses
Remote power up/down/reset	Securely and remotely power up, power down, or power cycle a PC.	<ul style="list-style-type: none"> Power up PCs off-hours for updates and patches, even for PCs that don't have agents installed. Mass shut-down during malicious attacks. Power-manage the PC to reduce power consumption when the PC is not in use and save on energy costs.

Table 2. Security capability

Capability	What it does	Common uses
Agent presence checking	Third-party applications check in with hardware-based timers at IT-defined intervals. A "miss" triggers an event and can send an alert to the IT console to indicate potential problems.	<ul style="list-style-type: none"> Automated, out-of-band notification of a missing or disabled agent (in combination with policy-based out-of-band alerting)
System isolation and recovery	Programmable filters check inbound and outbound network traffic for threats before the OS and applications load and after they close down.	<ul style="list-style-type: none"> Monitor inbound/outbound network traffic for threats. Identify suspicious packet headers Identify suspicious packet behavior, including fast-moving and slow-moving worms (desktop PCs with Intel® vPro™ technology) Port-isolate or quarantine PCs even if agent or OS is disabled
Support for Cisco SDN*, Microsoft NAP*, and PXE (preexecution environment)	Lets the network verify a PC's security "posture" – even before the OS loads – before allowing the PC access to the network.	<ul style="list-style-type: none"> Enable remote, out-of-band management and PXE boot of the PC while still maintaining full network security in a Cisco SDN or Microsoft NAP (notebooks with Intel vPro technology) environment
Support for 802.1x and PXE	Lets the network authenticate a PC before allowing the PC access to the network.	<ul style="list-style-type: none"> Enable remote, out-of-band management and PXE boot the PC while still maintaining full network security
Access to critical system information ^a	Lets you access critical system information (such as software version information, .DAT file information, and machine IDs) anytime.	<ul style="list-style-type: none"> Verify a PC's posture Identify PCs that need to be updated or patched, even for PCs that do not have an agent installed

^a Access to dedicated, protected memory, including UUID, event logs, hardware asset information, and software asset information in the third-party data store is also available when the notebook is connected to the corporate network through a host OS-based VPN.

Table 3. Problem-resolution capability

Capability	What it does	Common uses
Remote/redirected boot	More securely remote boot PC to a clean state, or redirect the PC's boot to another device, such as a clean image on local storage, a CD at the help desk, or an image on another remote drive.	<ul style="list-style-type: none"> Remotely boot PC to clean state Remotely boot PC to remediation server Remotely watch as BIOS, OS, and drivers load to identify problems with boot process Remotely provision PC before agents are installed Remotely rebuild or migrate OS Remote BIOS updates
Console redirection	Secure console redirection to remotely control a PC without user participation.	<ul style="list-style-type: none"> Troubleshoot PC without user participation Remotely install missing/corrupted files Remote hard-drive service or other maintenance
Out-of-band alerting	Receive policy-based alerts anytime, even if PC power is off, the OS is unresponsive, management agents are missing, or hardware (such as a hard drive) has failed.	<ul style="list-style-type: none"> Alert on event, such as falling out of compliance (in combination with agent presence checking) Alert on thresholds, before component fails
Persistent event logs ^a	Event log stored in persistent, dedicated memory (not on the hard drive), available anytime.	<ul style="list-style-type: none"> Access list of events that occurred before a hardware or software problem was noticed, including events that occurred before a notebook connected to the network Confirm critical events
Access to BIOS settings	Allows access to BIOS settings anytime.	<ul style="list-style-type: none"> Remotely correct BIOS settings accidentally changed by user Remotely change BIOS settings to solve application conflicts Remotely change PC's primary boot device to meet user needs
Access to critical system information ^a	Lets you access critical hardware asset information (such as manufacturer and model number) anytime, even if hardware (such as a hard drive) has already failed.	<ul style="list-style-type: none"> Identify "missing" (failed) hardware components

^a Access to dedicated, protected memory, including UUID, event logs, hardware asset information, and software asset information in the third-party data store is also available when the notebook is connected to the corporate network through a host OS-based VPN.

Table 4. Asset-management capability

Capability	What it does	Common uses
Persistent universal unique identifier (UUID) ^a	Lets you identify PC 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.	<ul style="list-style-type: none"> Accurately discover and identify PCs on network Identify unauthorized devices on the network
Access to hardware asset information ^a	Access hardware asset information (such as manufacturer and model number) anytime.	<ul style="list-style-type: none"> Accurate remote hardware-asset inventory End-of-lease planning FRU inventory management Identify upgrade opportunities
Access to third-party data storage ^b	Store and access critical software asset information (such as version information) in dedicated, persistent memory.	<ul style="list-style-type: none"> Remote software-asset inventory^b Software license planning

^a Access to dedicated, protected memory, including UUID, event logs, hardware asset information, and software asset information in the third-party data store is also available when the notebook is connected to the corporate network through a host OS-based VPN.

^b You can perform a remote software-asset inventory by accessing software information stored in the third-party data store; or by powering up an AC-powered, wired PC, and then performing the remote software inventory through the software inventory agent.

Table 5. Secure communication and remote configuration capabilities

Capability	What it does	Common uses
Secure tunnel for communication outside corporate firewall ^a	Allows a notebook to communicate with a remote management console through a secured tunnel for updates, diagnostics, repair, and alert reporting.	<ul style="list-style-type: none"> Remotely and securely service notebooks at 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
Certificate-based remote setup and configuration ^a	Allows for self-initiated, remote configuration using SSL certificate on a setup-and-configuration server (SCS) and root certificates on the Intel vPro technology-based client.	<ul style="list-style-type: none"> Simplify and speed up PC deployment without a desk-side visit
Key-based "one-touch" setup and configuration	Allows enterprise IT administrators to enter the security credentials for Intel AMT in-house.	<ul style="list-style-type: none"> Control the level of security needed for PC deployments

^aRemote set-up and configuration is also available when the notebook is connected to the corporate network through a host OS-based VPN.

Use an existing management console for both notebook and desktop PCs

The management capabilities built into Intel vPro technology allow for a phased-in or integrated implementation of systems. To help simplify the transition to a remotely managed environment, the new notebook and desktop PCs not only offer full remote configuration, but also use the same management console and communication mechanisms as other PCs.

Leading management software companies such as HP, LANDesk, Microsoft, and Symantec have already optimized their software to take advantage of the advanced capabilities of Intel vPro technology. These vendors support both previous and current versions of Intel vPro technology. IT administrators who have already deployed notebook and desktop PCs with Intel vPro technology do not have to change their management console to use PCs with the current version of Intel vPro technology. Ask your management-console vendor about specific implementation schedules and support for the new hardware-based security and remote-management capabilities for both desktop and notebook PCs.

Managing the wireless notebook

The new notebooks based on Intel Centrino 2 with vPro technology deliver significant improvements in performance, connectivity, security, management, battery life, and form factor. They are designed to make it easier for IT technicians to manage notebooks in both wired and wireless states:

- Identify notebook power state remotely.
- Maintain and manage the notebook in both wired and wireless states.
- Communicate more securely with notebooks in an open LAN – even outside the corporate firewall.
- Secure, manage, and maintain notebooks remotely – without user participation.

Manage notebooks regardless of power state

Notebooks with Intel vPro technology are designed to give IT technicians greater remote visibility into the system in both wired and wireless states (refer to Table 6 on the next page). Technicians can now remotely power up an AC-powered wireless notebook anytime, reboot the system, use secure console redirection, and use other critical maintenance and management capabilities of Intel vPro technology.

With the ability to remotely wake, power up, maintain, and manage a notebook anytime, technicians can ensure that IT tasks are performed when needed for security, and also performed at an advantageous times for the mobile user – without requiring user participation.

Help secure and manage notebooks outside the corporate firewall

Intel vPro technology now delivers new capabilities to secure and maintain notebooks even when they are outside the corporate firewall. These notebooks support a secure tunnel for communication outside the corporate firewall for:

- Out-of-band remote diagnostics and repair, to reduce service-depot calls and help-desk costs.
- Remote scheduled system maintenance, including patching, System Defense filter updates, audits/event logs, and inventory reporting.
- Alerting, so IT technicians can maintain and service notebooks before an OS or application becomes inoperable.

Table 6, on the next page, shows how the capabilities are enabled for wired and wireless notebooks and for desktop PCs, both inside and outside the corporate network.

Table 6. Capability matrix for notebooks and desktop PCs

Use Cases	Usages	AC-powered wired or wireless notebook or wired desktop			Battery-powered wired or wireless notebook ^a		
		Awake, OS working properly	Awake, but OS unresponsive	Asleep (Sx)	Awake, OS working properly	Awake, but OS unresponsive	Asleep (Sx)
Remote power up/power cycle	IT resets PC to clean state (or powers up PC for servicing). Use power management to reduce energy costs.	Yes	Yes ^a	Yes	Yes	Yes ^a	N/A
Remote diagnosis and repair	IT diagnoses remotely via out-of-band event log, remote/redirected boot, and console redirection.	Yes	Yes ^a	Yes	Yes	Yes ^a	
Remote hardware and/or software asset tracking	Take a hardware and software inventory regardless of OS or power state.	Yes Also available in presence of host OS-based VPN	Yes ^a	Yes	Yes Also available in presence of host OS-based VPN	Yes ^a	
Encrypted, remote software update	Third-party application discovers/updates antivirus engines and signatures.	Yes	Yes ^a	Yes	Yes	Yes ^a	
Agent presence checking and alerting	Ensure critical applications are running.	Yes Also available in presence of host OS-based VPN	Yes ^a	N/A	Yes Also available in presence of host OS-based VPN	Yes ^a	
System isolation and recovery	Automated or manual policy-based protection against virus outbreaks.	Yes	Yes ^a	NA	Yes	Yes ^a	
Remote configuration	Configure and provision PCs without a desk-side visit	Yes Also available in presence of host OS-based VPN	N/A	N/A	Yes Also available in presence of host OS-based VPN	N/A	
Secure tunnel for communication outside corporate firewall	Remote repair and maintenance support for systems outside the firewall	Yes ^b	Yes ^b	N/A	Yes ^b	Yes ^b	

^aRequires WPA or WPA2/802.11i security and Controller Link 1 for wireless operation when user OS is down.

^bRequires wired connectivity over an open network outside the corporate firewall. Not supported in “click to connect” environments.

Improved power-management and energy efficiency

Notebooks with Intel vPro technology are designed to help conserve energy and enable extended battery life for users. For example, these systems include a power-optimized chipset, ultra-low wattage electronics, and a new sleep state (C6) which allows the system to power down one processor core when it is not needed.

Intel Centrino 2 with Intel vPro technology-based notebooks deliver:

- Variety of power-management options to extend battery life.
- Integrated energy-saving components that are optimized to extend battery life.
- DDR3 memory, which reduces total device power, but still allows data to flow faster.
- Energy Star* Ready.

Secured out-of-band PC management

Software-only management applications are usually installed at the same level as the OS. 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, Intel vPro technology delivers both "readily-available" (out-of-band) remote communication built into the PC, as well as robust security technologies. The security technologies help ensure that the powerful capabilities of Intel vPro technology, as well as your stored information, are well protected.

Remote-communication channel runs outside the OS

The communication channel used by Intel vPro technology runs outside the OS (see figures 2 and 3 on the next page). This out-of-band (OOB) channel is based on the TCP/IP firmware

stack designed into system hardware, not on the software stack in the OS. The channel allows critical system communication (such as alerting) and operations (such as agent presence checking, remote booting, and console redirection) to continue more securely virtually anytime.

Because the channel is independent of the state of the OS, authorized IT technicians can communicate with an AC-powered wired 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,¹ 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, even if PC power is off.

For wireless notebooks on battery power, the communication channel is available anytime the system is awake and connected to the corporate network, even if the OS is unresponsive. The communication channel is also available for wireless or wired notebooks connected to the corporate network over a host OS-based VPN when notebooks are awake and working properly.

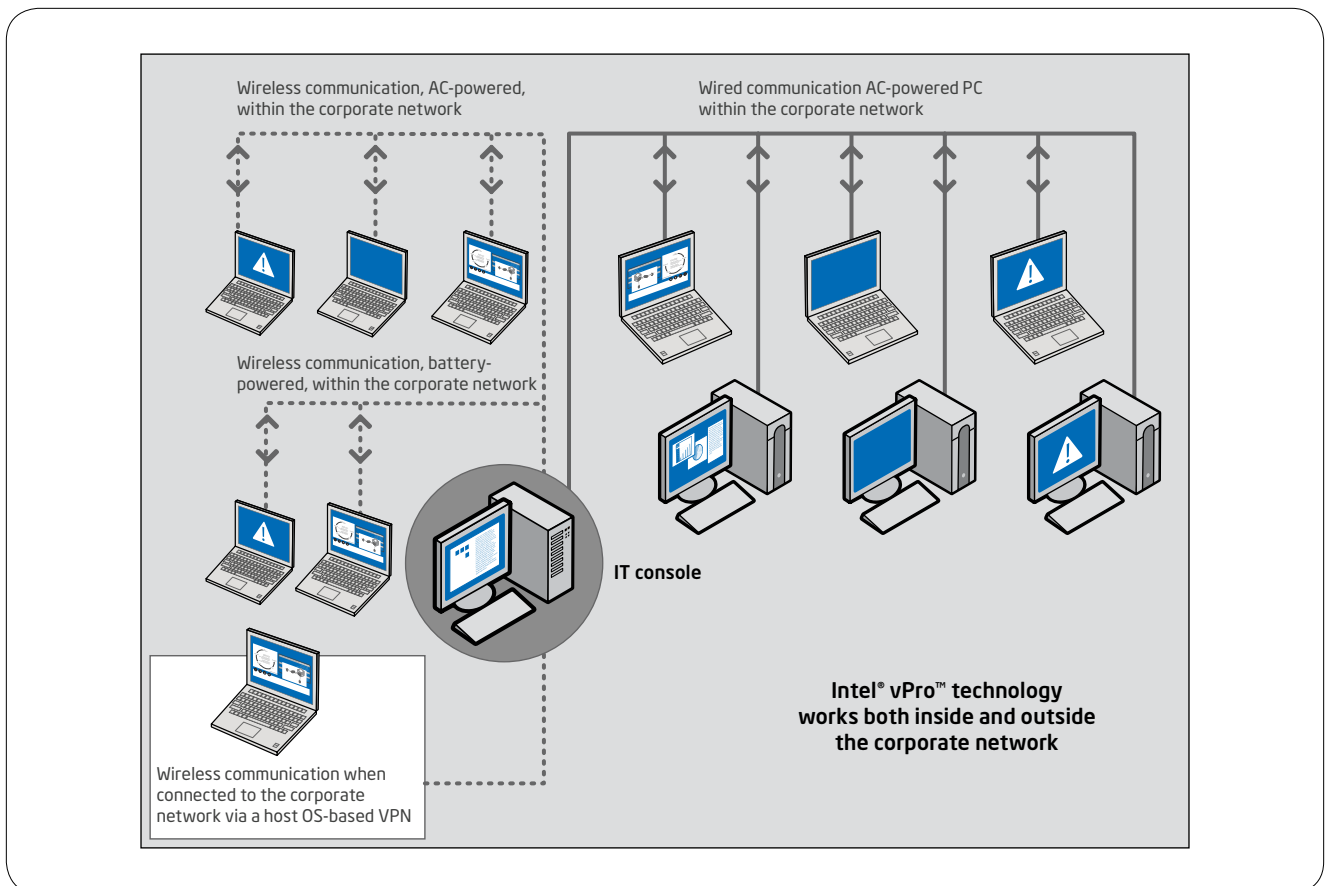


Figure 2. Remote communication. Capabilities are available for both notebook and desktop PCs with Intel® vPro™ technology. Some remote service capabilities for wireless notebooks with Intel vPro technology are also available when the notebook is connected to the corporate network through a host OS-based VPN.

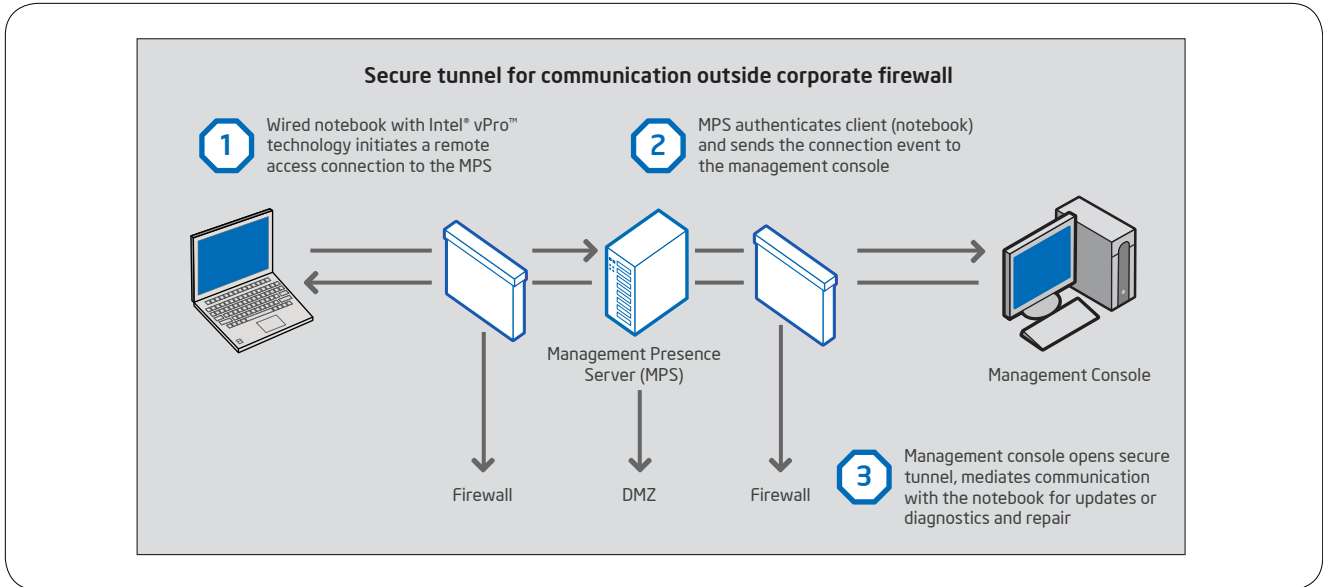


Figure 3. More secure communication to wired notebooks outside the corporate firewall. A management presence server authenticates wired notebooks, opens a secure TLS tunnel between the management console and notebook, and mediates communication.

Further, notebook and desktop PCs with Intel vPro technology support pre-OS authentication in 802.1x and Cisco Self-Defending Network (SDN) environments, and notebooks with Intel vPro technology support pre-OS authentication in Microsoft Network Access Protection (NAP) environments as well. Authorized technicians can now have out-of-band communication and management capabilities even in an environment with full Cisco SDN or Microsoft NAP network security.

More secure communication outside the corporate firewall

The new notebooks based on Intel Centrino 2 with vPro technology support secure communication in an open LAN – even outside the corporate firewall.⁵ This capability allows a wired notebook to communicate with a remote management console through a secured tunnel for diagnostics, repair, updates, and alert reporting. IT managers can now securely update and service notebooks at 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.

This capability works through the use of a management presence server (MPS) in the "DMZ" or "demilitarized zone" that exists between the corporate and client (notebook) firewalls. In the notebook, system configuration information includes the name(s) of appropriate management servers for the company. The MPS uses that information to help authenticate the wired notebook, then mediates communication between the notebook and the company's management servers during the repair or update session (see Figure 3).

Intel is working with leading independent software vendors (ISVs) to enable this capability in management consoles and firewalls. To help developers implement this important security technology, Intel is also including a reference design for the MPS in the software development kit (SDK) for Intel vPro technology.

Robust security methodologies for communication

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

- Transport layer security (TLS)
- HTTP authentication
- Enterprise-level authentication using Microsoft Active Directory* (Kerberos)
- Access control lists (ACLs)
- Digital firmware signing
- Other advanced methodologies and technologies

The security measures built into notebook and desktop PCs with Intel vPro technology 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.

PCs with Intel vPro technology also include built-in security capabilities to help protect themselves. Refer to the next discussion for information about built-in security capabilities such as System Defense filters, agent presence checking, and Intel TXT.

Best for business: Deep, built-in self-defense

IT administrators typically identify their most critical challenge as securing PCs from malicious attacks. The traditional problem is that even the best software-only solution can't manage systems that are powered off or whose OS is unavailable.

The solution? The proven hardware-assisted security capabilities of Intel vPro technology. These capabilities enable proactive protection that helps guard your business from data loss and interruptions:

- Eliminate virtually all deskside visits traditionally required to update or patch PCs.¹⁵
- Remotely power on PCs for off-hours updates, patching, or other work.
- Remotely identify PCs that are out of compliance.
- Rely on programmable, automated hardware-based filters to check network traffic – even when PCs are in the traditionally vulnerable state before the OS and applications load, and after they shut down.

New layers of defense

Intel vPro technology gives IT organizations new, proactive, hardware-based defenses to deal with malicious attacks (see Figure 4 on the next page). There are now several distinct layers of hardware-based protection for both notebook and desktop PCs:

- Programmable filtering of network traffic and out-of-band isolation capabilities.
- Remote visibility of software agents.
- Dedicated memory to better protect critical system information from viruses, worms, and other threats.
- Out-of-band management even with 802.1x and Cisco SDN or Microsoft NAP for notebooks.
- Intel Trusted Execution Technology (Intel® TXT).
- Industry standard TPM 1.2.
- Hardware-assisted virtualization.

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

Operate wirelessly with greater link reliability and predictability

Notebooks with Intel® Centrino® 2 with vPro™ technology support wireless technologies, including:

- 802.11a/b/g protocols for more secure, flexible wireless connectivity.¹⁶
- Draft 802.11n, the new standard expected to deliver up to 5x improvement in data throughput on a wireless-n network.¹⁷
- Current Cisco*-compatible extensions and features for improved network performance and Voice over WLAN, by optimal access-point selection technology.

Draft 802.11n – delivering performance gains of up to 5x.

Notebooks with Intel® vPro™ technology and Intel® Next-Gen Wireless-N¹⁸ on a new wireless 802.11n network deliver better reliability by reducing dead spots and dropped connections to improve productivity with fewer wireless interruptions. These notebooks also provide improved wireless connectivity for mobile users at the office. Among its many benefits, Intel Next-Gen Wireless-N technology can deliver up to five times the performance of existing 802.11g networks,¹⁷ with faster and more reliable wireless coverage.

Intel is committed to the adoption of the draft 802.11n standard. Intel has worked closely with leading wireless access-point (AP) vendors and has conducted extensive testing to verify the implementation of the technology. IT administrators can be assured that notebooks with Intel vPro technology and Intel Next-Gen Wireless-N work well with existing 802.11a/b/g access points and also provide great benefits with new wireless-n networks.

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 and Cisco SDN on desktop and notebook PCs or Microsoft NAP on notebook PCs. With the latest PCs with Intel vPro technology, network security credentials can be embedded in the hardware. This includes an Intel® Active Management Technology¹ (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, 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,

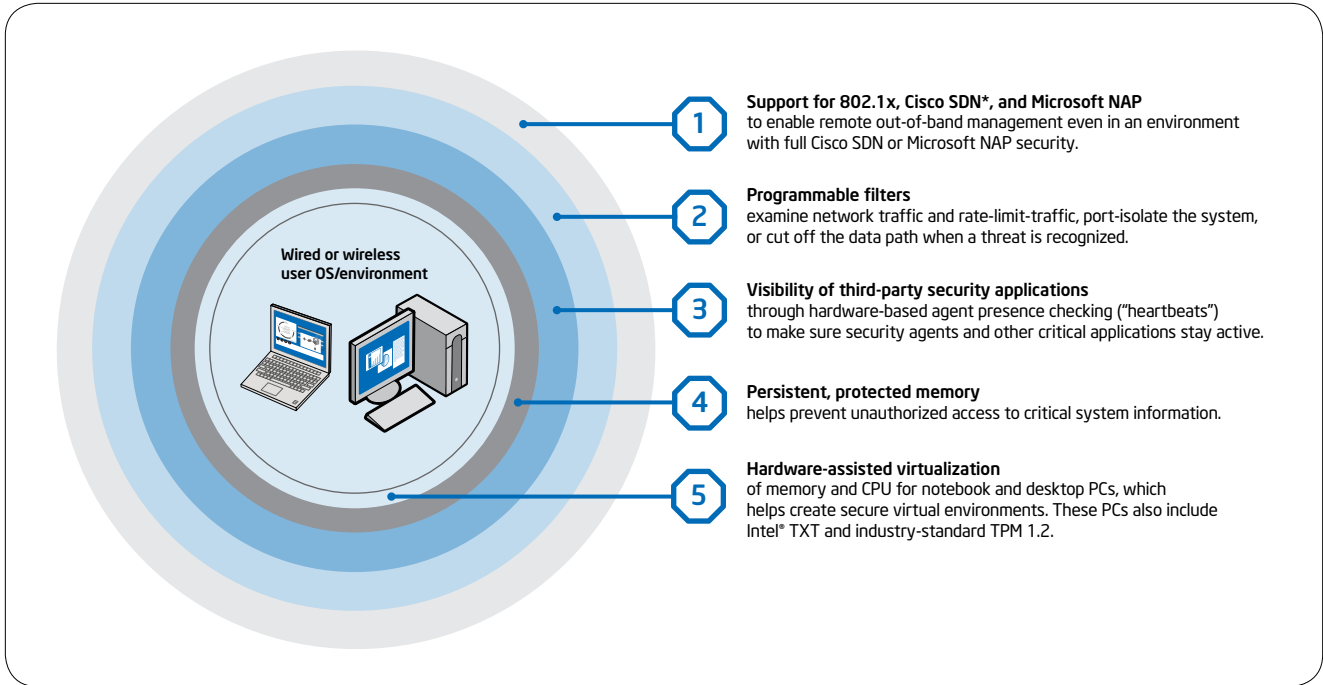


Figure 4. New layers of defense. Hardware-based security capabilities offer new layers of defense to fortify the PC against many critical threats.

and before the PC is allowed to access the network. IT administrators can now use out-of-band management for maintenance, security, management, or PXE purposes, while still maintaining full network security, including detailed, out-of-band compliance checks.

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

Notebooks require Intel AMT 4.0 for 802.1x, Cisco SDN and Microsoft NAP. Desktop PCs require Intel AMT release 3.2 or higher for Cisco SDN and 802.1x.

Intel® Trusted Execution Technology (Intel® TXT)

The new generation of notebook and desktop PCs with Intel vPro technology include Intel TXT, as well as industry-standard TPM 1.2. Intel TXT helps build and maintain a chain of trust from hardware to an Intel TXT-enabled OS or application. For example, Intel TXT can build and maintain a chain of trust from hardware to a virtual machine monitor (VMM) to protect information in virtualized environments from software-based attacks.

PCs with Intel vPro technology also include industry standard TPM 1.2, which stores keys in hardware, so security measures such as hard-drive encryption (for example, via Windows BitLocker full

drive encryption) are more effective. IT managers can now be more assured that data is more secure even when notebooks are lost or stolen. TPM 1.2 is compatible with both Windows Vista TPM driver and TPM base service.

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, notebook and desktop PCs with Intel vPro technology use a regular, programmable "heartbeat" presence check, which is built into the Intel® Management Engine. The heartbeat uses a "watchdog" timer so third-party software can check in with the Intel Management Engine at programmable intervals, to confirm that the agent is still active. Each time an agent checks in, it resets its timer. If an agent hasn't checked in before the timer goes off, the agent is presumed removed, tampered with, or disabled. The Intel Management Engine then automatically and immediately logs the alert and notifies (if specified) the IT console.

With hardware-based heartbeats, IT administrators no longer need to wait for multiple polls to identify a potential problem. The PC itself helps improve the reliability of presence checks and reduce the window of software vulnerability. And, these “healthy” heartbeats never leave the PC. Only when there is a problem is data sent across the network, so your network isn’t flooded with healthy heartbeat signals, and you still receive rapid notification of problems.

For wireless notebooks, 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.

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 secure, or they work only when the OS is running properly. When a PC is inoperable or powered down, technicians have traditionally had to update those systems later, when the machines were powered up and working properly – a process that allowed many systems to remain vulnerable to attack for dangerous lengths of time.

Intel vPro technology helps reduce security risks by allowing authorized technicians to remotely power up notebook and desktop PCs. This will help IT organizations substantially speed up critical updates and patches. Technicians can now:

- Remotely power up notebook and desktop PCs from the IT console, so updates can be pushed even to machines that were originally 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 waking 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).

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

Filter threats and isolate PCs automatically based on IT policy

Notebook and desktop PCs with Intel vPro technology include programmable filters for network traffic. IT managers can now use third-party software to define the policies that will trigger isolation of a PC.

Notebooks with Intel vPro technology additionally use programmable, hardware-based filters for monitoring the rate of inbound and outbound traffic, and for examining packet headers for threats. Desktop PCs with Intel vPro technology use programmable time-based (heuristics-based) filters built into the hardware to help identify suspicious behavior including both fast-moving and slow-moving worms.

Both notebook and desktop PCs also include built-in isolation circuitry (see Figure 5 on the next page). When a threat is identified, a policy and hardware-based “switch” can:

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

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

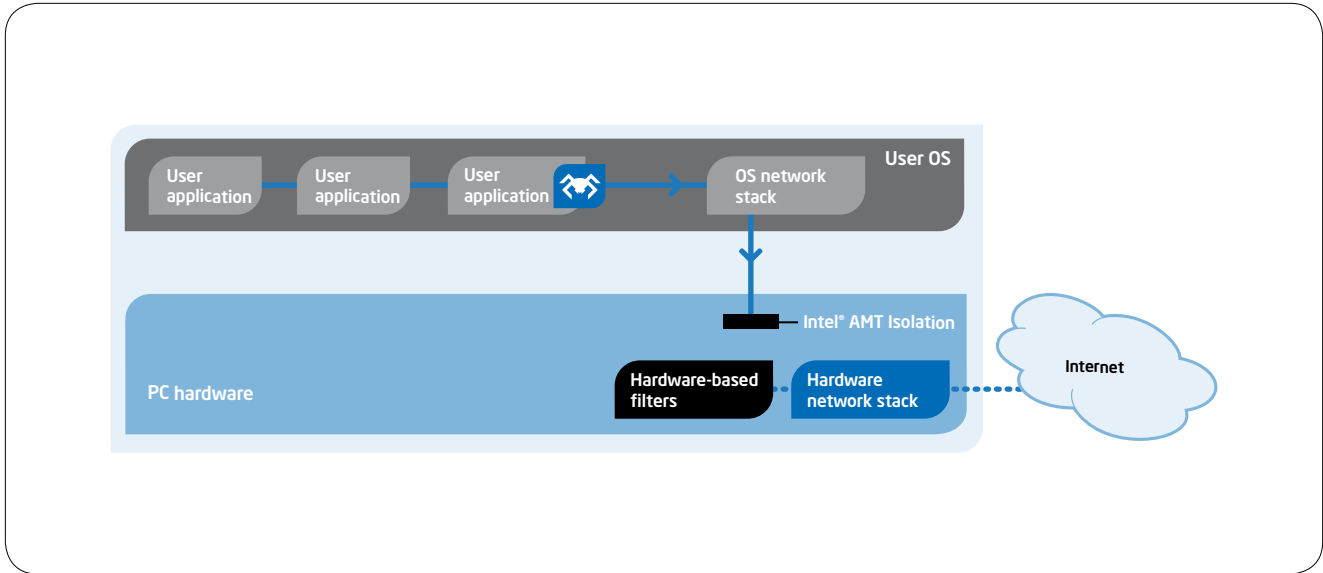


Figure 5. System defense filters inspect network traffic for desktop PCs. A PC with Intel® vPro™ technology can port-isolate itself or cut off its own network data path to quarantine itself when suspicious behavior is recognized – even if its OS is not available – to help prevent threats from spreading to the network.

Receive alerts even if a system is off the corporate network

Notebook and desktop PCs with Intel vPro technology have policy-based alerting built into the system. IT administrators can define the types of alerts they want to receive. Although all alerts are logged in the persistent event log, IT administrators can receive only the alerts they want. Less critical alerts do not add substantially to network traffic.

Since alerting uses the “readily-available” communication channel, IT administrators can receive critical notifications from PCs within the corporate network out-of-band and virtually anytime, even if the OS is inoperable, hardware has failed, PC power is off, or management agents are missing. IT can even receive notifications from a notebook (awake and OS operable) that is connected to the corporate network through a host OS-based VPN or when connected via wired LAN on an open network outside the corporate firewall.

IT administrators can now be notified rapidly and automatically when a system falls out of compliance, hardware is about to fail, or applications hang – sometimes even before users know they have a problem. With out-of-band alerting, IT administrators can shift more work from a costly reactive stance to more cost-effective, proactive service.

Substantially improve efficiencies for remote maintenance and management

Intel vPro technology provides many innovative hardware-based capabilities to significantly improve maintenance and management tasks, such as discovery, inventory, daily maintenance, updates, and problem resolution. These capabilities are available to authorized technicians virtually anytime.

Studies show that the new capabilities can help IT organizations reduce the number of desktside visits or service depot calls traditionally required to inventory, upgrade, repair, rebuild, or reimage PCs by up to 56%.¹⁹

With better remote tools, IT administrators can also automate more of these tasks. And, with greater visibility and access to the PC’s state, more work can be performed off-hours or when it is otherwise convenient to users.

Resolve more problems remotely

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

Table 7. Intel® vPro™ technology reduces deskside visits¹⁹

Issue	Estimated improvement with Intel® vPro™ technology ¹⁹
Hardware problems for notebook and desktop PCs	Reduce service depot and deskside visits by up to 56%
Software problems for notebook and desktop PCS	Reduce service depot and deskside visits by up to 58%

Positive ROI of 294% realized over 3 years²⁹

EDS is a leading global technology services company with 130,000 employees. The company delivers IT and business outsourcing services to clients in a variety of industries, such as manufacturing, health care, communications, government, and consumer retail.

Recently, EDS conducted an ROI analysis of Intel vPro technology at an EDS-managed call center located in Canada that supports three major clients across financial services, retail, and government. Results of the analysis showed substantial benefits:

- **Estimated positive ROI of 294% over 3 years** with a break-even at two years, when deploying PCs with Intel vPro technology.
- **Estimated savings of nearly \$320,000 in 3 years** through reduced deskside visits and improved productivity of existing desktop support staff.
- **Productivity benefit equivalent to \$440,000 across 3 years** since call-center employees can take more calls per agent each year, because Intel vPro technology enables off-hours patching.
- **Reduced power consumption by 25%** through the ability to remotely turn PCs on/off and remotely power them back up via Intel vPro technology to ready systems for the next work shift.

The ROI analysis shows how Intel vPro technology can significantly help enterprise save time and money, realize ROI on their technology investment in a short period of time, and at the same time, extend their remote management capabilities.

Intel vPro technology delivers powerful tools that let IT technicians more accurately diagnose hardware and software problems from the service center, update BIOS settings, and resolve software problems – down the wire and without user participation. The results are substantially fewer deskside visits (see Table 7), faster mean time to repair, less user downtime, and improved technician efficiencies.

Problem-resolution capabilities in Intel vPro technology include:

- **Remote/redirected boot**, through integrated drive electronics redirect (IDE-R), a more powerful and secure capability than wake-on-LAN (WOL). 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 and video console 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.
- **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.
- **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 notebooks – even outside the corporate firewall.⁵

IT technicians can now remotely:

- Access asset information anytime, to identify “missing” or failed hardware components, and verify software version information.
- Update BIOS settings, identify BIOS versions, or push a new BIOS version to the PC to resolve a particular problem.
- Guide a PC through a troubleshooting session – without requiring user participation.
- Watch as BIOS, drivers, and the OS attempt to load, to identify problems with the boot process.
- 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.

Save on power bills with better power management

IT technicians can now schedule PCs to be powered down overnight, and use Intel® vPro™ technology to securely and remotely power up the PC from the service center to perform work off-hours or simply ready the PC for the next work shift.

Power savings: Siemens study

Siemens conducted a study of power savings using desktop PCs with Intel vPro technology. In the study, PCs were scheduled to be powered down for 8 hours per night. The study showed that, using Intel vPro technology for an IT infrastructure of 5000 desktop PCs, Siemens could:

- Save 1.28 KWh per PC per day.²⁰
- Save \$52.80 per PC per year.²⁰

“This one feature alone saves the company \$264,000 yearly [and] pays for the cost of adding Intel vPro processor technology.”²⁰

– Siemens IT Solutions and Services newsletter, 2007

- Push new copies of missing or corrupted files, such as .DLL files, to restore an OS.
- Rebuild the OS or fully reimage the hard drive remotely.
- Perform OS migrations and application upgrades.
- Power-manage PCs more effectively to lower power consumption and reduce energy costs.

If a system becomes inoperable (see Figure 6 on the next page), a technician can now use secure remote/redirected boot or a secure PXE boot (within a Cisco SDN, and 802.1x networks or a Microsoft NAP network for notebooks). This allows the technician 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 notebook or desktop 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 desk-side visit.

Many technology evaluations and case studies have already shown that the new capabilities can help substantially reduce IT service costs for problem resolution (refer to the Intel Web site for case studies in various industries²¹). For example, Intel training facilities, which include many sites across several continents, investigated the new technology and determined that remote software installs could reduce technician time by 65-75%.²²

Accurate, remote discovery and inventory for wired or wireless systems

One of the primary challenges in managing PCs is acquiring information that is typically lost or unavailable when a system is powered down, reconfigured, rebuilt, or inoperative.

On average, up to 20% of a business's PCs are not in compliance at any given time.¹⁹ Adding to this problem is the difficulty in getting accurate software inventories. For example, software inventories for notebooks are often up to 11% inaccurate.²³

And, inaccuracies caused by underreporting 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.

The latest notebook and desktop PCs with Intel vPro technology give authorized technicians access to critical system information virtually anytime. This information is stored in protected, persistent memory (memory not on the hard drive) to improve discovery and inventory tasks. System information includes:

- **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.

IT technicians can now:

- 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.

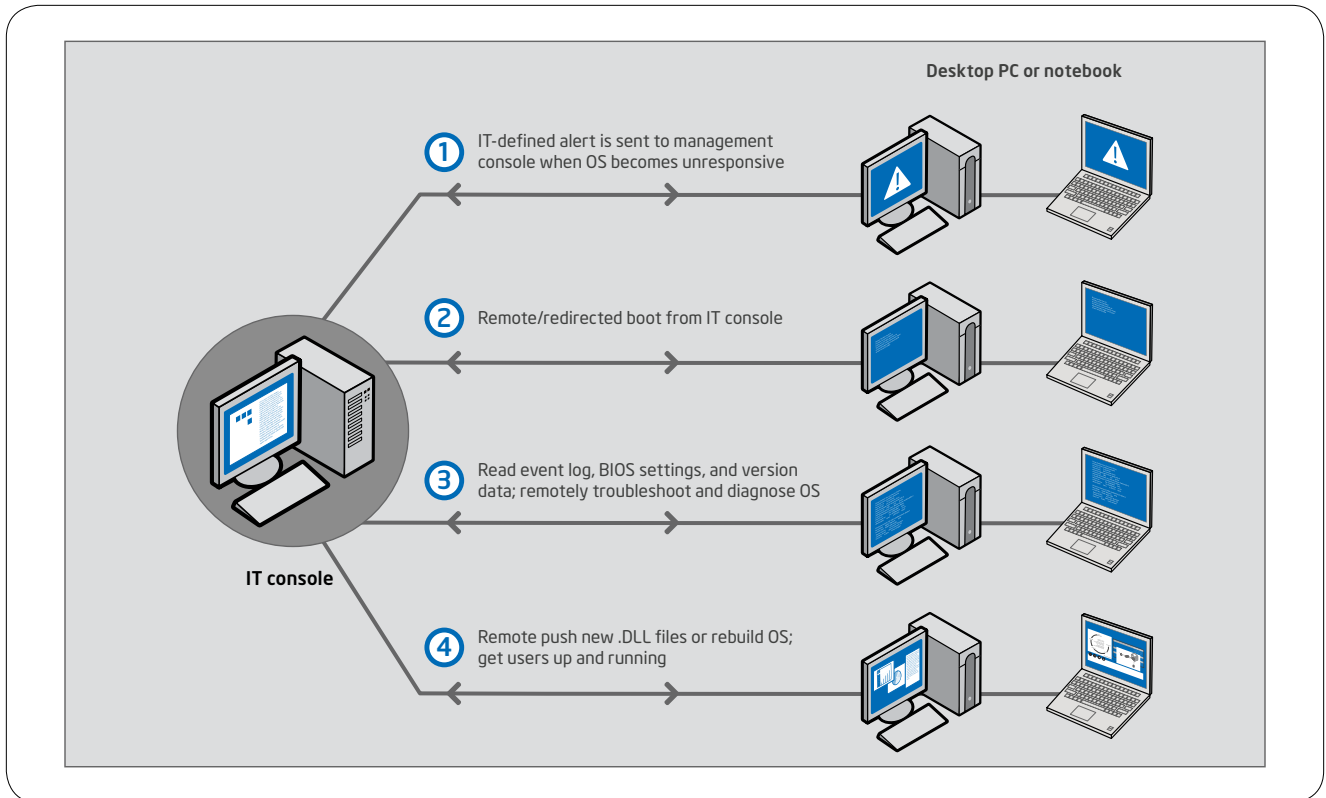


Figure 6. Remote problem resolution for an inoperable OS. New capabilities allow a technician to remotely access, diagnose, and repair or rebuild an OS that has become inoperable.

- Identify noncompliant PCs even if management agents have been disabled.
- Power up notebook and desktop PCs that are off to perform inventory tasks, push replacement management agents to the system, and remotely power the PC back to the state in which the user left it.
- Push replacement agents to a wired or wireless PC, to bring it back into compliance before further network access is allowed – even if management agents are missing.

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

Put a new tool in your security toolbox: hardware-assisted virtualization

Virtualization is an exciting tool that is being more broadly considered for deployment on business PCs. In virtualized systems, multiple OSs – with their associated applications – can run simultaneously inside “virtual machines.” Each virtual machine is a separate environment. Inside each environment, software can run in isolation from the other virtual machines on the system.

Isolation of each environment is achieved by introducing a layer of software below the OSs. This software layer is called a Virtual Machine Monitor (VMM). The VMM abstracts each virtual machine away from the physical hardware, manages memory partitions for the virtual machine, and intermediates calls for shared hardware resources, like graphics, hard drives, and networking.

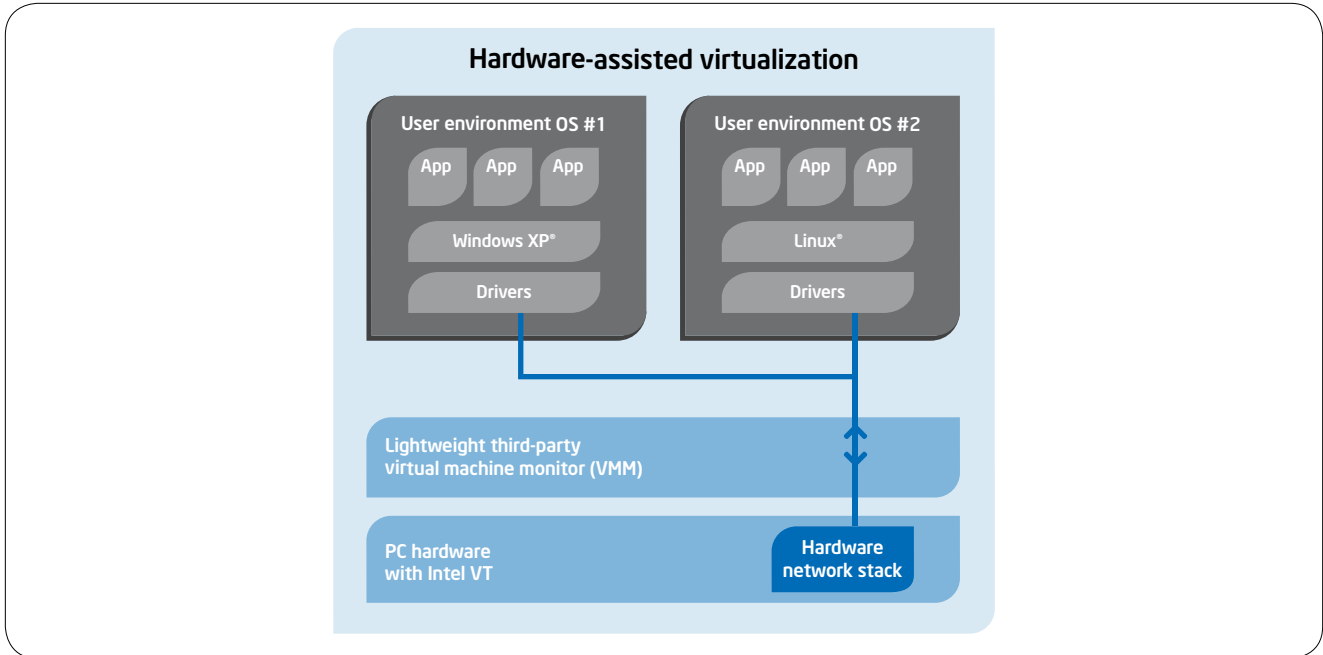


Figure 7. Hardware-assisted virtualization. Virtualization is supported on both notebook and desktop PCs.

Two virtualization models

There are two models for virtualization: traditional virtualization (multiple, fully functional OSs), and emerging uses.

Model 1: Traditional virtualization, with multiple, fully functional OSs

The traditional model of virtualization gives the user access to multiple fully functional OS environments running in separate virtual machines (see Figure 7). For example, the PC could have Microsoft Windows XP* and Linux* running side-by-side. This type of 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 Vista.

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.

Model 2: Emerging uses

The second type of virtualization enables new and emerging uses. Here, the PC has at least one fully featured OS and one or more additional OS environments that are self-contained. There are several ways to take advantage of a self-contained environment:

- **OS streaming.** Stream in applications or an OS from the network into the PC.
- **Application virtualization.** Run a specialized application more securely and in isolation.
- **Virtual "containers."** Create virtual containers to separate work environments – such as separating personal use applications from work use, confidential information from nonconfidential information, or a standard set of applications from applications that are streamed in from the network.

Virtualization improved by Intel® vPro™ technology

Today, virtualization can be achieved entirely with software – but this approach has traditionally had several challenges. There are two areas in particular where improvement is needed.

- First, overhead needs to be reduced so that VMMs can be smaller and the PC can deliver better performance.
- Second, each virtual machine needs to be better isolated from the other virtual machines on the system and from attacks on the VMM.

In PCs with Intel vPro technology, hardware enhancements both simplify and reduce the overhead of virtualization, making it easier for third-party vendors to build lightweight VMMs, and helping make virtualization more efficient and secure.

Reducing complexity and overhead

Much of the overhead in software-based virtualization comes from the fact that today's VMMs must manage all the functions required to keep the software stack working properly for each full user OS environment. Intel VT shifts some of that burden to hardware, so that software virtualization solutions can focus more on features and capabilities, and less on simply arbitrating calls to the PC's resources.

- **Without virtualization:** OS runs at Ring 0. In a PC that is not virtualized, the OS runs natively at Ring 0, the highest privilege level. Drivers and applications run at lower privilege levels, usually at Ring 2 or Ring 3.
- **Software-based virtualization:** VMM has exclusive use of Ring 0. The OS, drivers, and applications are deprivileged, since they are displaced from their natural level by the VMM. The VMM must work hard to manage all the hardware calls, traps, driver translations, and other functions that keep the software stack working properly. This adds overhead and can affect PC performance.
- **Hardware-assisted Intel VT:** New Ring below Ring 0. The OS, drivers, and applications run at their normal privilege levels. Hardware and firmware allow the VMM to run at a new privilege level (Ring -1). This significantly reduces VMM overhead and complexity and allows the virtualized OSs to run at near-native performance.

With Intel vPro technology, one of the major barriers to mainstream virtualization – excess overhead – is mitigated.

Existing security: Virtualization for memory and the CPU

Previous and current generations of Intel VT (found in Intel vPro technology) support isolated memory spaces for each virtual machine. In these virtual machines, data in reserved memory spaces is isolated and protected from memory access by other software running in the processor. This feature provides a significant level of hardware enforcement for the VMM's memory manager.

Improved isolation and security: Virtualization for Directed I/O

Intel VT for Directed I/O prevents unauthorized direct memory accesses (DMAs) from the hardware from reading or writing information to other virtual machines that do not have access permission.

Each virtual machine can now be protected – via the combination of Intel VT processor virtualization and Intel VT for Directed I/O – from any application, OS, driver or hardware DMA that it did not request. The result is significantly improved isolation of the virtual environment and better 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. Traditional antivirus or firewall applications run at the user OS level, and cannot access or scan the VMM running below the OS. This means that the VMM usually runs outside the protection of ordinary security software. Unfortunately, since the VMM controls access to the data in each virtual machine, it is a tempting target for malicious software. Such software, including spyware and viruses, could be extremely damaging and difficult to detect in the VMM from a software-only virtualized environment.

Intel® Trusted Execution Technology (Intel® TXT)²

Intel TXT (see Figure 8 on the next page) is designed to address the important security issue of protecting and establishing trust in the VMM 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. 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.

Intel TXT is available in the latest notebook and desktop PCs with Intel vPro technology.

Building the chain of trust

The root of trust for a trusted software stack is the Intel processor, Intel chipset, and industry-standard Trusted Platform Module version 1.2 (TPM). Intel TXT uses the trusted hardware components to build the chain of trust through four general steps:

1. During launch of the VMM, the Intel TXT authenticated code (AC) modules check for proper BIOS setup.
2. The AC modules authenticate themselves to the chipset, and provide trusted utilities to setup, check, and maintain the trusted execution environment.
3. Intel TXT checks the configuration of the trusted execution environment. Once the configuration is verified, Intel TXT measures the AC module in the TPM.

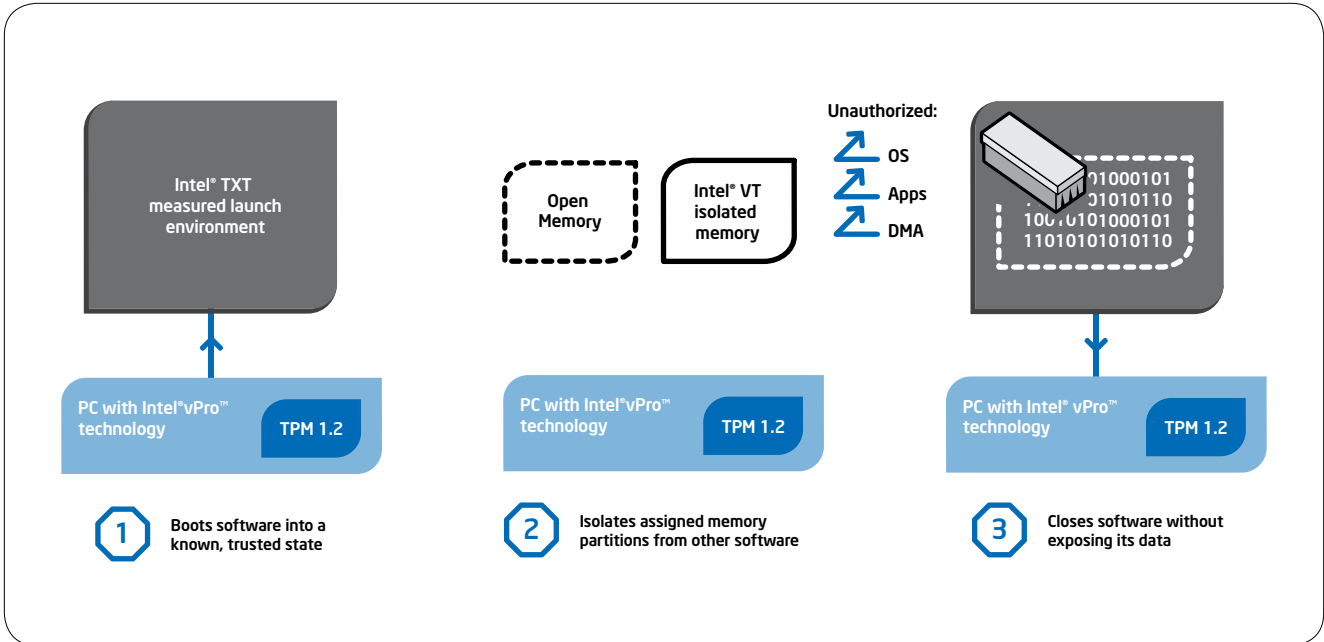


Figure 8. Intel® Trusted Execution Technology (Intel® TXT) verifies launch environment and establishes the root of trust. Intel TXT establishes a root of trust, which allows software to build a chain of trust and prove the integrity of the VMM before it launches. Also, with Intel TXT, virtual machine data stored in memory is erased by the VMM during orderly shutdowns, and erased by Intel TXT in the event of a disorderly shutdown or system crash. This significantly reduces the likelihood of confidential data being exposed.

4. Intel TXT then authenticates and verifies the measured launch environment (MLE) and the VMM, and launches the authenticated VMM.

The process allows the VMM to be verified earlier than with current software protection mechanisms (such as virus detection software). With a chain of trust from hardware to VMM to software, IT administrators can be more assured that critical applications and data in each virtual machine are well-protected.

Protection for secrets during application shutdown or power transition

Intel TXT offers another key capability: protection of secrets during power transitions. This capability helps protect security credentials for PCs during the traditionally vulnerable period when a virtual machine is shutting down. Intel TXT protects credentials for both orderly and disorderly shutdowns. (Disorderly shutdowns can be caused by many factors, including an application crash or a manual power-down.) The problem with previous virtualization models has been that, when a PC is improperly shut down, secrets such as passwords and keys typically remain in memory.

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® VT compatible with other technologies

Standard memory, storage, and graphics cards work with Intel VT.⁴ The latest notebook and desktop PCs with Intel vPro technology can also run most off-the-shelf OSs and applications without IT administrators having to perform special installation steps. The hardware-based virtualization technology is also designed to work with and complement other advanced security and management technologies from Intel, such as Intel AMT.

Roadmap for virtualization technology

Table 8 briefly lists the virtualization technologies available in notebook and desktop PCs with Intel vPro technology.

Intel VT is enabled in VMM packages from vendors such as VMware. Intel VT with Intel TXT is available from vendors such as Green Hills. Intel VT including Intel VT for Directed I/O are enabled in VMM packages from vendors such as VirtualLogix. Intel VT including Intel VT for Directed I/O and Intel TXT are enabled in VMM packages from vendors such as Parallels and enabled later in 2008 from vendors such as Red Hat.

Table 8. Virtualization support in notebook and desktop PCs

Advanced technology	Offers	Intel® Centrino® with vPro™ technology	Intel® Centrino®2 with vPro™ technology	Intel® Core™2 processor with vPro™ technology
Intel® VT	Virtualization of processor and memory.	Yes	Yes	Yes
Intel® VT for Directed I/O	Virtualization of I/O hardware.	No	Yes	Yes
Intel® TXT	Trusted launch of the VMM and protection of secrets during proper or improper shutdown.	No	Yes	Yes

Simplify and speed up remote configuration

Intel vPro technology allows powerful out-of-band access and management of PCs. To maintain the proper level of security, it is important that IT administrators establish the initial security credentials for Intel AMT appropriately for their service environment before configuring the Intel AMT capabilities for remote management. The configuration process may be accomplished through use of keys or credentials to secure the communication channel between the management console and the client being configured.

Methods to deploy notebooks and desktop PCs with Intel® vPro™ technology

Deployment of PCs with Intel vPro technology follows these general steps. Configuration is a self-initiated automated step that depends on security credentials being in place. You can use various configuration processes to create and establish security credentials to simplify deployment.

1. Establish the management console, including the setup-and-configuration server (SCS).
- 2a. Using unique key pairs: Create and establish security credentials manually or automatically: Generate unique key pairs for each PC with Intel vPro technology. Next, enter the unique key pair on each PC in one of the following methods: manually via text entry into the Intel Management Engine BIOS extension (MEBx), automatically via USB key, or as preestablished unique key pairs loaded by your original equipment manufacturer (OEM).

After security credentials are established, as soon as you plug the PC into a power source and connect it to the network, the PC can continue its own self-initiated configuration as a remote, fully automated process.

- 2b. Using SSL certificates: Plug PC into power and the network to allow self-initiated, remote configuration using an SSL certificate on the setup-and-configuration server (SCS) and root certificates on the Intel vPro technology-based PCs.

Configuration process

In order to allow secure configuration over the production network, the communication for configuring Intel AMT must be encrypted. In order to make configuration easier for large deployments, Intel vPro technology offers several options for using manual or automated processes to remotely establish security credentials in order to automatically configure the PC.

Certificate-based remote configuration option

Certificate-based remote configuration is enabled in the new generation of notebook and desktop PCs with Intel vPro technology:

- When the wired or wireless notebook is on AC or battery power and awake
- When the desktop PC is on AC power and plugged into the Ethernet

The certificate-based Remote Configuration option requires that your original equipment manufacturer (OEM) establish security credentials (root certificates) and set certain parameters in BIOS and the Intel Management Engine BIOS extension (MEBx). A notebook or desktop PC ready for fully automated remote configuration has these example settings (not complete list) already in place:

- Intel AMT is shipped "enabled" with:
 - ZeroTouchSetupEnabled = TRUE
 - Manageability Mode = AMT
 - SOL Boot Capable and IDER Boot Capable set to TRUE
- The host (PC's OS) must be powered on and fully awake (S0 power state), or the Intel Management Engine must be shipped in the "enabled" state for all sleep states (S0-S5).

- Security credentials (root certificates) are preloaded (i.e., by your OEM), and an Intel AMT SSL (secure sockets layer) certificate is established.
- Network is configured for dynamic IP addressing (DHCP).

With certificate-based Remote Configuration, enterprise IT administrators can deploy the PC directly to the user desk, and the PC will initiate its own remote configuration as soon as it is plugged into AC power and connected to the Ethernet. As with other enterprise configurations, the wired notebook or desktop PC can initiate its configuration even before management agents are installed. The PC will then remotely configure itself in your environment based on the parameters specified by your setup-and-configuration server.

Key-based one-touch configuration option

Key-based Remote Configuration can be accomplished via USB key, preloaded unique key pairs by your OEM (optional), or manually entered via the Intel Management Engine BIOS extension (MEBx) setup screen.

In key-based Remote Configuration, the IT administrator enters credentials on each PC via a USB key or other mechanism. As soon as credentials are entered, the PC can be deployed to the user desk. Once plugged into AC power and connected to the Ethernet, the PC will initiate its own automated configuration.

Security credentials entered via USB key or other mechanism include:

- Administrator username and password
- Provisioning passphrase
- Provisioning ID

The unique key pairs can be entered by your OEM or manually by IT administrators. For those IT administrators who prefer to enter keys manually, the key-based Remote Configuration option lets IT administrators enter security credentials (administrator password, provisioning passphrase, provisioning ID) manually through the Intel Management Engine BIOS extension (MEBx) setup screen, a process typically used for the highest-security environments. As soon as security credentials are entered, the enterprise PC can be deployed to the user desk, plugged into AC power and connected to the Ethernet. The PC will then initiate its own automated configuration.

With these options for deployment, IT administrators can choose the level of security and automation appropriate for their network environments.

When your business needs to respond, your PCs will be responsive

IT organizations typically serve two masters: IT itself, with its requirements for security, maintenance, management, and upgrades/migration; and users, with their requirements for performance. Today, there is a third, growing business concern: power consumption, not just because of battery life for notebooks, but because energy costs are a significant operating expense and companies have an ever-increasing corporate focus on environmental responsibility.

Enter Intel Core 2 Duo processors – the powerhouse in all PCs with Intel vPro technology. These CPUs deliver improved performance per watt, outstanding performance for multitasking, and support for future OSs.

Best for business: Improved performance, energy efficiency and eco-smart computing

- **64-bit Intel Core 2 Duo processors deliver excellent performance per watt.** These processors are optimized for improved multi-tasking and multithreading with compute-intensive applications, and deliver significantly improved performance over previous-generation notebook and desktop PCs. IT technicians can now run critical IT tasks, such as virus scans and e-mail synchronization in the background without bogging down foreground user applications.
- **Energy efficiency, great battery life and eco-smart computing.** Advanced architecture, package design techniques, power coordination, and thermal technologies let Intel Core 2 Duo processors operate at very low voltages and use power more efficiently, so less unnecessary heat is generated and less cooling required for these high-performance systems designed to help meet Energy Star requirements. In desktop PCs, the result is excellent performance in quieter, smaller form factors. Notebooks with Intel vPro technology not only consume less power, but also include a power-optimized chipset, DDR3 memory, a new sleep state, and improved battery technologies to deliver great battery life for users. The latest PCs with Intel vPro technology are also designed using lead-free, halogen-free manufacturing processes.²⁴
- **Optional Intel® Turbo Memory for notebooks.** On notebooks with Intel vPro technology, Intel® Turbo Memory stores large amounts of information closer to your processor to help reduce boot time and enable faster application loading when running Microsoft Windows Vista.²⁵

IT administrators can now have the benefits of increased security and better remote management, while providing users with high-performance PCs that meet both wired and wireless needs.

Ready for the future

Notebook and desktop PCs with Intel vPro technology are stable, standardized platforms with broad industry support, ready for future operating systems and applications.

- **64-bit processor: Windows Vista ready.** PCs with Intel vPro technology handle today's OSs and are ready for Windows Vista, which has a heavily threaded architecture, updated Windows Display Driver Mode (WDDM), built-in security features like Windows Defender,* BitLocker drive encryption,²⁶ and other advanced features.²⁷
- **Multithreaded CPU: Ready for Office 2007.*** Intel Core 2 processors provide the performance needed for the next-generation of Microsoft Office,* including the performance for intense, always-on (by default) text-based search indexing, which is heavily multithreaded.
- **64-bit graphics support: No need for a discrete graphics card.** PCs with Intel vPro technology have built-in 64-bit graphics for an outstanding Windows Vista Aero* experience. There is no need for a discrete graphics card with these PCs.

Stable, standards-based, and with broad industry support

To help the industry get the most from its technology investments, PCs with Intel vPro technology are:

- **Built on standards.** Intel vPro technology is built on industry standards to give you many choices in selecting OEMs and software vendors. Some of the standards upon which Intel vPro technology is built include ASF, XML, SOAP, TLS, HTTP authentication, Kerberos, DASH,*²⁸ and WS-MAN.
- **Broadly supported by the industry.** Intel vPro technology is supported by major software vendors in security software, management applications, and business software. PCs with Intel vPro technology are available from leading, worldwide desktop and notebook OEMs and are supported by major IT service providers and managed service providers.
- **Stable and simple.** The latest PCs with Intel vPro technology are available under the Intel® Stable Image Platform Program¹³ (Intel® SIPP), so businesses can avoid unexpected changes that might force software image revisions or hardware requalifications. With Intel SIPP-compliant notebook and desktop PCs, IT can be more assured of having a stable platform that simplifies the deployment of new computing systems.

Wired or wireless: Security and manageability on the chip

Intel is uniquely positioned to provide critical business and IT capabilities on a notebook or desktop PC through extensive, break-through research and development, leading-edge manufacturing, and a unique ability to catalyze broad ISV support for creative solutions.

For IT organizations, the result is a professional-grade system designed from hardware to software with built-in capabilities that resolve the most critical challenges of business and IT – improved, proactive security and remote manageability – with energy-efficient performance. With Intel built in, IT organizations can address a wider range of enterprise needs and shift resources from managing and securing their notebook and desktop PCs, to accelerating business into the future.

To learn more about the built-in security and remote manageability capabilities of notebooks and desktop PCs with Intel vPro technology visit www.intel.com/vpro.

Blog with the pros who have deployed Intel vPro technology; visit www.intel.com/go/vproexpert.


- ¹ Intel® vPro™ technology includes powerful Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see <http://www.intel.com/technology/manage/iamt/>.
- ² 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>
- ³ The original equipment manufacturer (OEM) must provide TPM 1.2 functionality, and the PC must be provisioned with Windows Vista® Enterprise or Windows Vista® Ultimate Edition. TPM may not be available in all countries.
- ⁴ Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.
- ⁵ Based on measured Intel® Pentium® M 780 (2MB L2, 2.26GHz, 533FSB) and estimated Intel® Pentium M 770 (2MB L2, 2.13GHz, 533FSB) versus Pre-Production Mobile Intel Core™2 Duo Processor T8100 (3MB L2, 2.10GHz, 800MHz FSB) on Intel Matanzas Customer Reference Board board, Intel Chipset Software Installation File 8.2.0.012, 2x1GB Dual Channel Micron® PC2-5300 DDR2 800 5-5-5-15, Hitachi® 100GB TravelStar® Serial ATA 7200 RPM, Windows® Vista® Ultimate 32bit. Performance tests and ratings are measured using specific computer systems and / or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit <http://www.intel.com/performance/>
- ⁶ Systems using Client Initiated Remote Access (CIRA) require wired LAN connectivity and may not be available in public hot spots or "click to accept" locations. For more information on CIRA visit, www.intel.com/products/centrino2/vpro/index.htm.
- ⁷ Based on the theoretical maximum bandwidth enabled by 3x3 Draft-N implementations with 3 spatial streams. 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.
- ⁸ Package area plus z-height reduction.
- ⁹ Intel® processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number_for_details.
- ¹⁰ Support for Cisco SDN® on notebook PCs with Intel® Centrino® with vPro™ technology requires Intel® Active Management Technology (Intel® AMT) firmware version 2.6 or later. Notebooks with Intel AMT release 2.5, when upgraded to Intel AMT firmware release 2.6, are not compliant with the 2007 mobile Intel® Stable Image Platform Program (Intel® SIPP) cycle due to Intel AMT and wireless LAN software driver change requirements.
- ¹¹ 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel® 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.
- ¹² Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.
- ¹³ 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. Intel® Core™2 processor with vPro™ technology with Intel® Active Management Technology (Intel® AMT) release 3.2 is not supported in the 2007 Intel SIPP.
- ¹⁴ Wireless access to the powerful capabilities of Intel® vPro™ technology requires WPA, WPA2/802.11i security.
- ¹⁵ Source: "An Analysis of Early Testing of Intel® vPro™ Processor Technology in Large IT Departments," Charles LeGrand, Tech Par Group and Mark Salamasick, Center for Internal Auditing Excellence, University of Texas at Dallas; commissioned by Intel, April 2007.
- ¹⁶ Wireless connectivity and some features may require you to purchase additional software, services or external hardware. For references to enhanced wireless performance, refer to comparisons with previous-generation Intel® technology. Availability of public wireless LAN access points is limited, wireless functionality may vary by country and some hotspots may not support Linux®-based notebooks with Intel® Centrino® with vPro™ technology systems. See <http://www.intel.com/products/centrino/index.htm> and <http://www.intel.com/performance/mobile/benchmarks.htm> for more information.
- ¹⁷ Up to 2x greater range and up to 5x better performance with optional Intel® Next-Gen Wireless N technology enabled by 2x3 Draft N implementations with 2 spatial streams. Actual results may vary based on your specific hardware, connection rate, site conditions, and software configurations. See <http://www.intel.com/performance/mobile/index.htm> for more information. Also requires a Connect with Intel® Centrino® processor technology certified wireless n access point. Wireless n access points without the Connect with Intel® Centrino® processor technology identifier may require additional firmware for increased performance results. Check with your PC and access point manufacturer for details.
- ¹⁸ In order to experience the new benefits of wireless-n on notebooks with Intel® Centrino® with vPro™ technology, users must be connected to a wireless 802.11n network. Existing 802.11a, 802.11b and 802.11g networks/ access points will not provide the new benefits.
- ¹⁹ Results shown are from the 2007 EDS Case Studies with Intel® Centrino® Pro processor technology, 3rd party audit commissioned by Intel, of various enterprise IT environments and may not be representative of the results that can be expected for smaller businesses. The studies compare test environments of Intel® Centrino® Pro processor technology equipped PCs vs non- Intel® Centrino® Pro processor technology environments. Tested PCs were in multiple OS and power states to mirror a typical working environment. Actual results may vary. The study is available at www.intel.com/vpro and www.eds.com
- ²⁰ Source: Siemens IT Solutions and Services newsletter, 2007.
- ²¹ Visit the Intel® Web site for case studies and proofs-of-concept listed under Explore the Ecosystem at: <http://mysearch.intel.com/bizcontent/default.aspx?vs=&q=vpro&contentType=cs>.
- ²² Source: Managing Training Rooms with Intel® vPro™ Processor Technology, April 2007, Intel. The study is available at <http://www.intel.com/it/pdf/managing-training-rooms-with-intel-vpro-processor-technology.pdf>
- ²³ Results shown are from the 2007 Benefits of Intel® Centrino® Pro Processor Technology in the Enterprise, Wipro Technologies study commissioned by Intel. The study models projected ROI of deploying Intel® Centrino® Pro processor technology. Actual results may vary. The study is available at www.intel.com/vpro and www.wipro.com
- ²⁴ 45nm product is manufactured on a lead-free process. Lead-free per EU RoHS directive July, 2006 (2002/95/EC, Annex A). Some EU RoHS exemptions may apply to other components used in the product package. Residual amounts of halogens are below November 2007 proposed IPC/JEDEC J-STD-709 standards.
- ²⁵ Tests run on customer reference boards and preproduction latest generation Intel® Centrino® processor technology with optional Intel® Turbo Memory enabled against like systems without Intel® Turbo Memory. Results may vary based on hardware, software and overall system configuration. All tests and ratings reflect the approximate performance of Intel products as measured by those tests. All testing was done on Microsoft® Vista® Ultimate (build 6000). Application load and runtime acceleration depend on Vista's preference to pre-load those applications into the Microsoft® ReadyBoost® cache. See <http://www.intel.com/performance/mobile/benchmarks.htm> for more information.
- ²⁶ Any disk encryption technology may limit certain remote management capabilities. See disk software vendor for information on interaction of disk encryption software and remote management.
- ²⁷ For information about system requirements for Windows Vista®, refer to <http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/capable.aspx>.
- ²⁸ Intel® Core™2 processor with vPro™ technology (2007) DASH™ implementation is based on draft DASH 1.0 specifications.
- ²⁹ Source: EDS Intel vPro Call Center ROI Analysis, January 2008.

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

Copyright © 2008 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel. Leap ahead., Intel. Leap ahead. logo, Centrino, Intel Core, Core Inside, and Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

Printed in USA

0508/LKY/OCG/PP/5K

 Please Recycle

311710-006US

