White Paper

Intel® Centrino® Pro Processor Technology

Intel® vPro™ Processor Technology

Intel® Centrino® Pro and Intel® vPro™ Processor Technology

Remotely manage both wired and wireless PCs from the same IT console for increased security and simplified system management

A new generation of notebook and desktop PCs enables proactive security, enhanced maintenance, and improved remote management. Notebook PCs with Intel® Centrino® Pro processor technology and desktop PCs with Intel® vPro™ processor technology deliver down-the-wire security and manageability capabilities – even if hardware (such as a hard drive) has failed, the operating system (OS) is unresponsive, software agents are disabled, the desktop PC is powered off, or the notebook's management agents have been disabled. Desktop PCs also include support for virtual appliances that allow IT managers to isolate and protect critical security and management applications in a more secure, trusted environment. In addition, the new generation of notebook and desktop systems delivers significantly improved 64-bit performance for compute-intensive tasks – including fully integrated 64-bit graphics support – all in a power-efficient package that is Microsoft Windows Vista* ready.

Table of Contents

Executive Summary

Notebook PCs with Intel® Centrino® Pro processor technology and desktop PCs with Intel® vPro™ processor technology[1] deliver built-in security and remote management capabilities to meet critical business challenges. IT administrators can now quickly identify and contain more security threats, take more accurate asset and hardware/software inventories remotely, resolve more software and OS problems faster without leaving the service center, and accurately diagnose hardware problems down-the-wire.

The new security and management capabilities of these wired and wireless systems are based in hardware, not software. The advantage for IT is that the capabilities are available to authorized IT technicians down-the-wire, even for PCs that have traditionally been difficult to manage or unavailable to the IT management console. IT technicians can now protect and manage notebooks across wireless networks – even if the OS is unresponsive or software agents are missing; and protect and manage wired notebook and desktop PCs, even if power is off, hardware has failed, or the OS is unresponsive. The result is increased compliance, more accurate inventories, fewer service depot visits and deskside visits, and less interruption to business.

The new generation of Intel-based notebook and desktop PCs deliver significantly improved performance for compute-intensive applications and multitasking – all in a power-efficient package that is Microsoft Windows Vista* ready. Desktop PCs with Intel vPro processor technology also include additional, hardware-based capabilities that give IT administrators the option of a lighter-weight form of virtualization[2] for mainstream business. IT technicians can now run critical security applications in a simplified, self-contained, trusted, dedicated virtual partition – or "virtual appliance" – even while users are working on their own compute-intensive tasks in the user OS.

IT can now spend less time on routine tasks, and can focus resources where they are most needed for better security and manageability of both notebook and desktop PCs.

Intel® Centrino® Pro and Intel® vPro™ processor technology

A new generation of notebook and desktop PCs delivers down-the-wire proactive 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 operating system (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 wired or wireless state, or the state of the OS.

Challenge	Solution
Costly and time-consuming manual inventories	▪ Accurate, remote asset inventory, even if PC is powered off or management agents are missing
Undiscoverable assets	▪ 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
Spiraling and costly deskside visits	▪ Remote remediation, even if management agents are missing or the OS is unresponsive ▪ Remote problem resolution, even if OS is unresponsive or hardware (such as a hard drive) has failed
Systems unmanageable when powered down	▪ Access the PC even if PC power is off or the OS is unresponsive
Lack of configuration compliance	▪ Remote inventory and agent presence checking as a hardware-based, automated, policy-based service

Security and remote manageability on a chip

Notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology are designed to address the top IT challenges in security and manageability.[1] This new generation of notebook and desktop PCs delivers improved security and management capabilities that are based in hardware, not software.

The advantage of hardware-based capabilities over traditional software-based solutions is that they let authorized technicians remotely access PCs that have traditionally been unavailable to the management console. With Intel Centrino Pro and Intel vPro processor technology, technicians can manage the PC even if the OS is unresponsive, hardware (such as a hard drive) has failed, a desktop PC's power is off, or a notebook's management agents have been disabled.

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

PCs with Intel Centrino Pro and Intel vPro processor technology deliver:

- **Hardware-based security capabilities,** which help improve compliance down-the-wire, ensure that third-party security software is available when needed, remotely identify viruses, worms, and other threats faster, and stop those threats more effectively.
- **Remote problem-resolution capabilities,** which help you 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 capabilities,** which help eliminate manual inventories, improve compliance with government and industry regulations, and reduce management costs.
- **Remote configuration during deployment,** so that you have options to configure PCs remotely with various levels of automation in an enterprise environment.

Combined with third-party management applications, the new Intel® technologies allow IT administrators to eliminate a significant number of deskside visits, reduce overspending on existing resources, and minimize interruptions to business.

Common use cases to improve compliance, increase automation, and reduce service calls

Intel Centrino Pro and Intel vPro processor technology are designed to help IT administrators reach more PCs remotely, automate more tasks, perform more work from a remote, centralized location, and reduce user interruptions. Table 1 (on page 6) lists some of the new capabilities of Intel Centrino Pro and Intel vPro processor technology that help you achieve those objectives. Table 2 (on page 7) lists some common use cases for improved security and remote management, and the capabilities that enable them. The capabilities are available for wired, AC-powered PCs, and for wireless, awake notebooks within the corporate network, even if an OS is inoperable or hardware (such as a hard drive) has failed. Some capabilities, such as agent presence checking and access to hardware asset information, are also available for notebooks connected to the corporate network through 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 automate more diagnostics, repair, and remediation tasks, eliminate many site visits, improve service efficiencies, and free resources for other projects.

Intel® Centrino® Pro and Intel® vPro™ processor technology[1]

Notebook and desktop PCs based on these advanced technologies deliver validated, fully integrated systems that help IT organizations improve security and remote management for both wired and wireless systems, yet still give users excellent 64-bit performance for compute-intensive applications and multitasking – a unique combination of capabilities, only from Intel.

Intel® Centrino® Pro processor technology (2007)	Intel® vPro™ processor technology (2007)
Intel® Core™2 Duo processor T, L, and U 7000 sequence[3]	Intel® Core™2 Duo processor E6550, E6750, and E6850 and upcoming Intel® Core™2 Quad processors[3]
Mobile Intel® 965 Express Chipset with ICH8M-enhanced	Intel® Q35 Express Chipset with ICH9DO
Intel® Active Management Technology[1] (Intel® AMT), release 2.5 and 2.6	Intel® Active Management Technology[1] (Intel® AMT), release 3
Support for 802.11a/b/g wireless protocols, with available support for draft n	
Intel® Virtualization Technology[2] (Intel® VT)	Intel® Virtualization Technology (Intel® VT) including Intel® VT for Directed I/O
	Support for virtual "appliance" applications
	Intel® Trusted Execution Technology[4]
Support for Cisco Network Access Control* (Cisco NAC*)[5]	Support for Cisco NAC* v1.0
Support for 802.1x	Support for 802.1x
64-bit enabled[6]	64-bit enabled[6]
Execute Disable Bit[7]	Execute Disable Bit[7]
Intel® Stable Image Platform Program (Intel® SIPP)[8]	Intel® Stable Image Platform Program (Intel® SIPP)[8]
Windows Vista* ready	Windows Vista* ready
Integrated support for 64-bit graphics	Integrated support for 64-bit graphics
Windows Vista* BitLocker* ready	Windows Vista* BitLocker* ready

Table 1. Previous release vs. current release of Intel® Centrino® Pro and Intel® vPro™ processor technology[a]

Capability	Previous release of Intel® vPro™ processor technology	Current release of Intel® vPro™ processor technology[a] in 2007	Current release of Intel® Centrino® Pro processor technology[a]
Security Capability			
Remote power up[b]	Yes	Yes	Yes[b]
Remote power off/reset	Yes	Yes	Yes
Agent presence checking	Yes	Yes	Yes
System isolation and recovery	Yes	Yes	Yes
▪ Time-based filters	N/A	Yes	N/A
Support for Cisco NAC*	N/A	Yes	Yes[c]
Support for 802.1x	N/A	Yes	Yes
Access to critical information about security applications (such as .DAT file and version information)	Yes	Yes	Yes
Problem Resolution Capability			
Remote/redirected boot	Yes	Yes	Yes
Console redirection	Yes	Yes	Yes
Out-of-band alerting	Yes	Yes	Yes
Persistent event logs	Yes	Yes	Yes
Access to BIOS settings	Yes	Yes	Yes
Access to critical system information	Yes	Yes	Yes
Asset-management capability			
Persistent universal unique identifier (UUID)	Yes	Yes	Yes
Access to hardware asset information	Yes	Yes	Yes
Access to third-party data storage	Yes	Yes	Yes
Remote configuration options			
Light-touch remote configuration	Yes	Yes	Yes
Semi-automated remote configuration (USB key)	Yes	Yes	Yes
Fully automated remote configuration	N/A	Yes	Yes[d]

[a] Current release for Intel® vPro™ processor technology includes Intel® AMT release 3 and Intel® VT combined with Intel® VT for directed I/O and Intel® TXT. Current release for Intel® Centrino® Pro processor technology is Intel AMT release 2.5 or 2.6.
[b] Remote power-up is supported for AC-powered notebook and desktop PCs.
[c] Intel® AMT release 2.6 and higher.
[d] Fully automated remote configuration is available when the notebook is plugged into AC power. Requires Intel® AMT release 2.6 and higher.

Table 2. Built-in capabilities deliver new level of service

Capability	What it does	Common uses
Security Capability		
Remote power up/down/reset[a]	Securely and remotely power up, power down, or power cycle a PC.	▪ Power up PCs off-hours for updates and patches, even for PCs that don't have agents installed ▪ Mass shut-down during malicious attacks
Agent presence checking	Third-party applications check in with hardware-based timers at IT-defined intervals. A "miss" triggers an event and can send rapid alert to IT console to indicate potential problem.	▪ Rapid, 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 OS and applications load and after they close down.	▪ Monitor inbound / outbound network traffic for threats ▪ Identify suspicious packet headers (PCs with Intel® Centrino® Pro processor technology) ▪ Identify suspicious packet behavior, including fast-moving and slow-moving worms (PCs with Intel® vPro™ processor technology) ▪ Port-isolate or quarantine PCs even if agent or OS is disabled
Support for Cisco NAC*	Lets the network verify a PC's security "posture" – even before the OS loads – before allowing the PC access to the network.	▪ Enable remote, out-of-band management of the PC while still maintaining full network security in a Cisco NAC environment
Support for 802.1x	Lets the network authenticate a PC before allowing the PC access to the network.	▪ Enable remote, out-of-band management of the PC while still maintaining full network security
Access to critical system information[b]	Lets you access critical system information (such as software version information, .DAT file information, and machine IDs) anytime.	▪ Verify a PC's posture ▪ Identify PCs that need to be updated or patched, even for PCs that do not have an agent installed
Problem Resolution Capability		
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.	▪ Remote boot PC to clean state ▪ Remote boot PC to remediation server ▪ Remote watch as BIOS, OS, and drivers load to identify problems with boot process ▪ Remote provision PC before agents are installed ▪ Remote rebuild or migrate OS ▪ Remote BIOS updates
Console redirection	Secure console redirection to remotely control a PC without user participation.	▪ Troubleshoot PC without user participation ▪ Remote 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.	▪ Alert on event, such as falling out of compliance (in combination with agent presence checking) ▪ Alert on thresholds, before component fails
Persistent event logs[b]	Event log stored in persistent, dedicated memory (not on the hard drive), available anytime.	▪ 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.	▪ Correct BIOS settings accidentally changed by user ▪ Change settings to solve application conflicts ▪ Change PC's primary boot device to meet user needs
Access to critical system information[b]	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.	▪ Identify "missing" (failed) hardware components
Asset-management capability		
Persistent universal unique identifier (UUID)[b]	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.	▪ Accurately discover and identify PCs on network ▪ Identify unauthorized devices on the network
Access to hardware asset information[b]	Access hardware asset information (such as manufacturer and model number) anytime.	▪ Accurate remote hardware-asset inventory ▪ End-of-lease planning ▪ FRU inventory management ▪ Identify upgrade opportunities
Access to third-party data storage[c]	Store and access critical software asset information (such as version information) in dedicated, persistent memory.	▪ Remote software-asset inventory[c] ▪ Software license planning

[a] Remote power-up is not available over wireless networks.
[b] 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.
[c] 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.

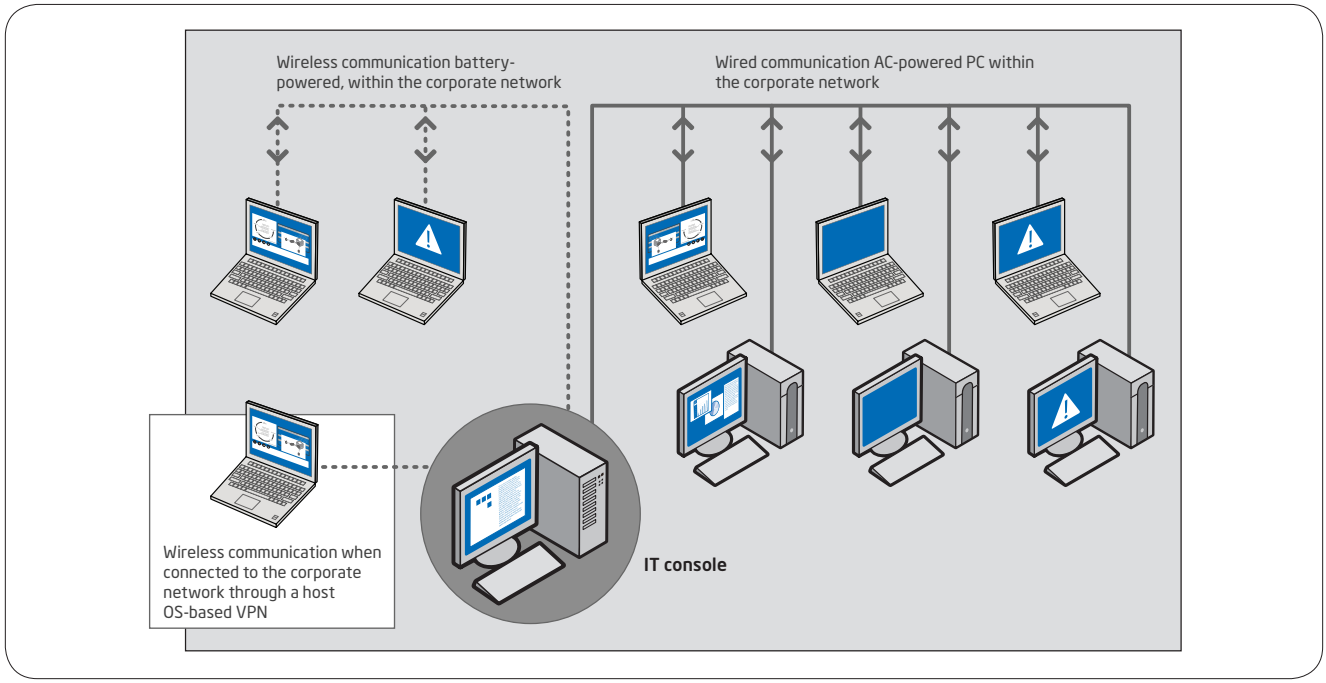

Figure 1. Capabilities are available for both wired and wireless PCs. Hardware-based communication and capabilities are available for desktop PCs and wired notebooks on AC power within the corporate network even if the PC is powered off or its OS is inoperable. The capabilities are also available for wireless notebooks on battery power inside the corporate network when the notebook is awake, even if its OS is inoperable. Agent presence checking and hardware-asset tracking is available even when a notebook is awake, working properly, and connected to the corporate network through a host OS-based VPN.

Wired and wireless PCs

Managing notebook and desktop PCs requires that technicians be aware of the state of the system. For example, before servicing a PC, a technician should know whether the system is AC-powered or battery-powered, on or off, awake or asleep. Being able to identify and change – if appropriate – the state of the PC allows the technician to identify when it is most advantageous to service a notebook or power up a desktop to perform work off-hours, when it won't interrupt the user.

Figure 1 shows the various states in which notebook and desktop PCs can be remotely managed using Intel Centrino Pro and Intel vPro processor technology.[9] 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.

Use an existing management console for both notebook and desktop PCs

The management capabilities built into Intel Centrino Pro and Intel vPro processor 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 remote configuration, but 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 Centrino Pro and Intel vPro processor technology. These vendors support both previous and current versions of Intel Centrino Pro and Intel vPro processor technology. IT administrators who have already deployed PCs with Intel Centrino Pro and Intel vPro processor technology do not have to change their management console to use PCs with the current version of Intel Centrino Pro and Intel vPro processor 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

One of the challenges IT technicians face today is managing notebooks without using up battery life which the user might need at that moment for work. Intel Centrino Pro processor technology is designed to help conserve energy and enable extended battery life for users by providing remote capabilities depending on the state of the system. States include AC-powered or battery-powered, on or off, awake versus asleep. This helps ensure that IT tasks are performed at the most advantageous times for the mobile user.

Tables 3 and 4 show how the capabilities are enabled for wired and wireless notebooks and desktop PCs in various states, both inside and outside the corporate network.

More secure, 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 Centrino Pro and Intel vPro processor technology deliver 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 Centrino Pro and Intel vPro processor technology, as well as your stored information are well protected.

Table 3. Wired capability matrix for notebooks and desktop PCs

Use Cases	Usages	Wired: Ethernet-wired capabilities for notebooks with Intel® Centrino® Pro processor technology or desktop PCs with Intel® vPro™ processor technology within the corporate network:					
		Plugged into AC power source – notebook or desktop			Battery power – notebook		
		Awake/ operable	Awake/ inoperable	Asleep[a]	Awake/ operable	Awake/ inoperable	Asleep[a]
Agent presence checking and alerting	Ensure critical applications are running	Yes	Yes	NA	Yes	Yes	NA
System isolation and recovery	Automated or manual policy-based protection against virus outbreaks	Yes	Yes	NA	Yes	Yes	
Remote power up/power cycle	IT resets PC to clean state (or powers up PC for servicing)	Yes	Yes	Yes	Yes	Yes	
Remote diagnosis and repair	IT diagnoses remotely via out-of-band event log, remote/redirected boot, and console redirection	Yes	Yes	Yes	Yes	Yes	
Remote hardware and/or software asset tracking	Take a hardware and software inventory regardless of OS or power state	Yes	Yes	Yes	Yes	Yes	
Encrypted, remote software update	Third-party application discovers/updates antivirus engines and signatures	Yes	Yes	Yes	Yes	Yes	

[a] For remote management of notebook PCs, asleep refers to the S3 (hibernate) and S4 (suspend) sleep states.

Remote-communication channel runs outside the OS

The communication channel used by Intel Centrino Pro and Intel vPro processor 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 securely virtually anytime.

Because the channel is independent of the state of the OS, authorized IT technicians can communicate with an AC-powered PC anytime. Even if hardware (such as a hard drive) has failed, the OS is unresponsive, the PC is powered off, or its management agents are missing,[1] the communication channel is still available.

As long as the system is connected to the network and 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. The communication channel is even available for wireless or wired notebooks connected to the corporate network over a host OS-based VPN when notebooks are awake and working properly.

Further, because PCs with Intel Centrino Pro and Intel vPro processor technology support 802.1x and Cisco NAC, authorized technicians can now have out-of-band communication and management capabilities even in an environment with full Cisco NAC network security.

Table 4. Wireless capability matrix for notebooks with Intel® Centrino® Pro processor technology[a]

		Wireless[a]: Capabilities for wireless notebooks with Intel® Centrino® Pro processor technology within the corporate network					
		Plugged into AC power source – notebook			Battery power – notebook		
Use Cases	**Usages**	Awake/ operable	Awake/ inoperable	Asleep[b]	Awake/ operable	Awake/ inoperable	Asleep[b]
Agent presence checking and alerting	Ensure critical applications are running	Yes[c] Also supported in presence of host OS-based VPN	Yes	NA	Yes[c] Also supported in presence of host OS-based VPN	Yes	NA
System isolation and recovery	Automated or manual policy-based protection against virus outbreaks	Yes	Yes		Yes	Yes	
Remote power up/power cycle	IT resets PC to clean state	Yes	Yes		Yes	Yes	
Remote diagnosis and repair	IT diagnoses remotely via out-of-band event log, remote/redirected boot, and console redirection	Yes	Yes		Yes	Yes	
Remote hardware and/or software asset tracking	Take a hardware and software inventory regardless of OS or power state	Yes[c] Also supported in presence of host OS-based VPN	Yes		Yes[c] Also supported in presence of host OS-based VPN	Yes	
Encrypted, remote software update	Third-party application discovers/updates antivirus engines and signatures	Yes	Yes		Yes	Yes	

[a] Wireless access to the powerful capabilities of Intel Centrino Pro processor technology requires WPA, WPA2/802.11i security.
[b] For remote management of notebook PCs, "asleep" refers to the S3 (hibernate) and S4 (suspend) sleep states.
[c] This capability is available even for wireless notebooks in an awake and operable state which are connected to the corporate network through a host OS-based VPN.

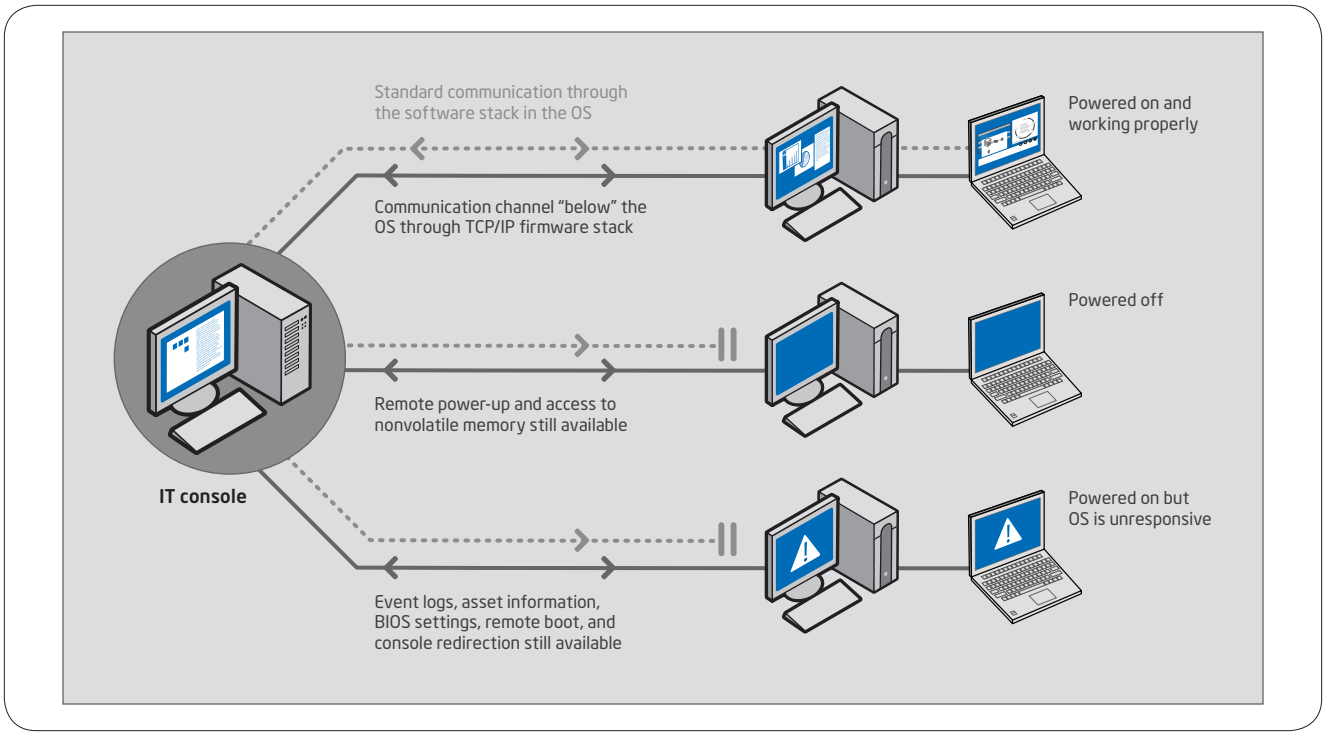

Figure 2. Remote communication with wired systems. All applicable capabilities are available for notebooks with Intel® Centrino® Pro processor technology and desktop PCs with Intel® vPro™ processor technology that are plugged into AC power and connected to the corporate network via an Ethernet cable.

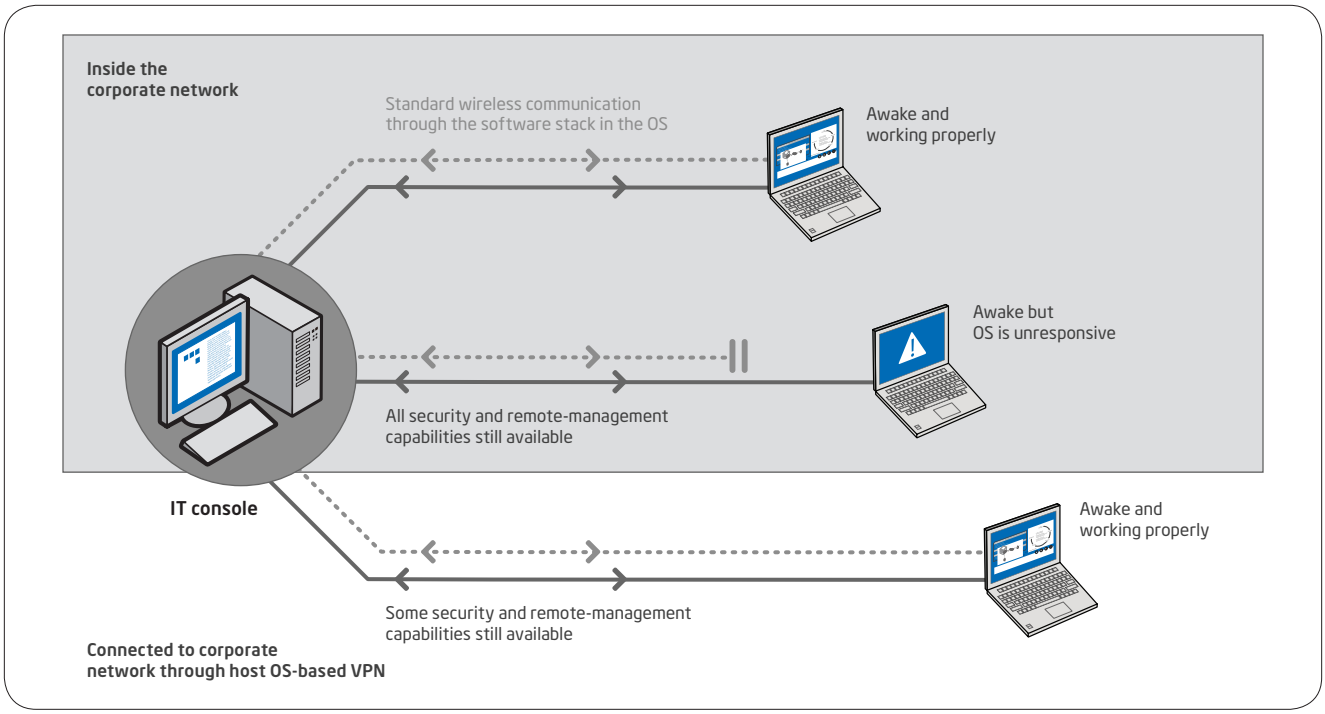

Figure 3. Remote communication with wireless systems. Technicians have some remote service capabilities for wireless notebooks with Intel® Centrino® Pro processor technology both inside the corporate network, and when connected to the corporate network through a host OS-based VPN.

Robust security methodologies

The hardware-based communication and manageability capabilities are secured through a variety of robust schemes.[10] 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

Even when the PC is off, its software agents have been disabled, or its OS is unresponsive, the security measures built into these notebook and desktop PCs help ensure the confidentiality and authentication of the communication channel and hardware-based capabilities, and the security of stored information.

Protecting your business is crucial – it's time for PC defense in depth

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 or secure systems that are powered off or whose OS is unavailable. The solution? Intel's proven hardware-assisted security, which enables proactive protection that helps guard your business from data loss and interruptions. These capabilities let you:

- Eliminate virtually all deskside visits traditionally required to update or patch PCs.[11]
- Remotely power on desktop 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.

Wireless technologies

Notebooks with Intel® Centrino® Pro processor technology support many wireless technologies, such as Wireless LAN, including:

- 802.11a/b/g protocols for more secure, flexible wireless connectivity.[12]
- 802.11n, the new draft standard expected to deliver up to 5x improvement in data throughput on a wireless n network.[13]
- Current Cisco*-compatible extensions and features for improved network performance and Voice over WLAN, by optimal access-point selection technology.

802.11n – delivering performance gains of up to 5x. Notebooks with Intel Centrino Pro processor technology and optional Intel® Next-Gen Wireless-N[14] on a new wireless 802.11n network 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.[13] It offers faster and broader wireless coverage, and helps reduce dead spots and dropped connections to improve productivity with fewer wireless interruptions.

Intel is committed to the adoption of the 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 Centrino Pro processor 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.

New layers of defense

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

- **Programmable filtering of network traffic and isolation,** which lets IT managers use third-party software to define the policies that will trigger isolation of a PC. PCs with Intel Centrino Pro processor technology use programmable, hardware-based filters to check inbound and outbound network traffic packet headers for

threats. PCs with Intel vPro processor 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. When a threat or suspicious behavior is discovered, isolation circuitry can set rate-limits for network traffic, isolate the PC by specific port(s), or fully isolate a PC (the remediation port remains open). 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.

- **Remote visibility of software agents** through agent-presence checking via hardware-based timers, so third-party applications and management software can check in with the system at IT-defined intervals. IT administrators no longer need to wait for multiple serial polls to verify that an agent has been disabled or removed. And, since software checks in with the hardware, your network isn't flooded with healthy "heartbeat" signals. This capability is available even on notebooks connected to the corporate network through a host OS-based VPN.
- **Dedicated memory** to better protect critical system information from viruses, worms, and other threats.
- **Out-of-band management even with 802.1x and Cisco NAC,** so the network can authenticate a PC before the OS and applications load, and before the PC is allowed to access the network. This capability allows the 802.1x or Cisco posture profile to be stored in hardware (in protected, persistent memory), and presented to the network even if the OS is absent. This capability allows IT administrators to use out-of-band management while maintaining full network security, including detailed, out-of-band compliance checks. (Notebooks require Intel AMT release 2.6.)
- **Optional hardware-based "virtual appliance"** for desktop PCs with Intel vPro processor technology. Virtual appliances are based on third-party software and provide vital security or management services to a user OS. (See the virtual-appliance discussion on page 19 in the virtualization section.)
- **Intel® Trusted Execution Technology (Intel® TXT)** for desktop PCs with Intel vPro processor technology. This capability helps build and maintain a chain of trust from hardware to the virtual machine monitor (VMM) to protect information in virtualized environments from software-based attacks. (See the virtualization section on page 21.)

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.

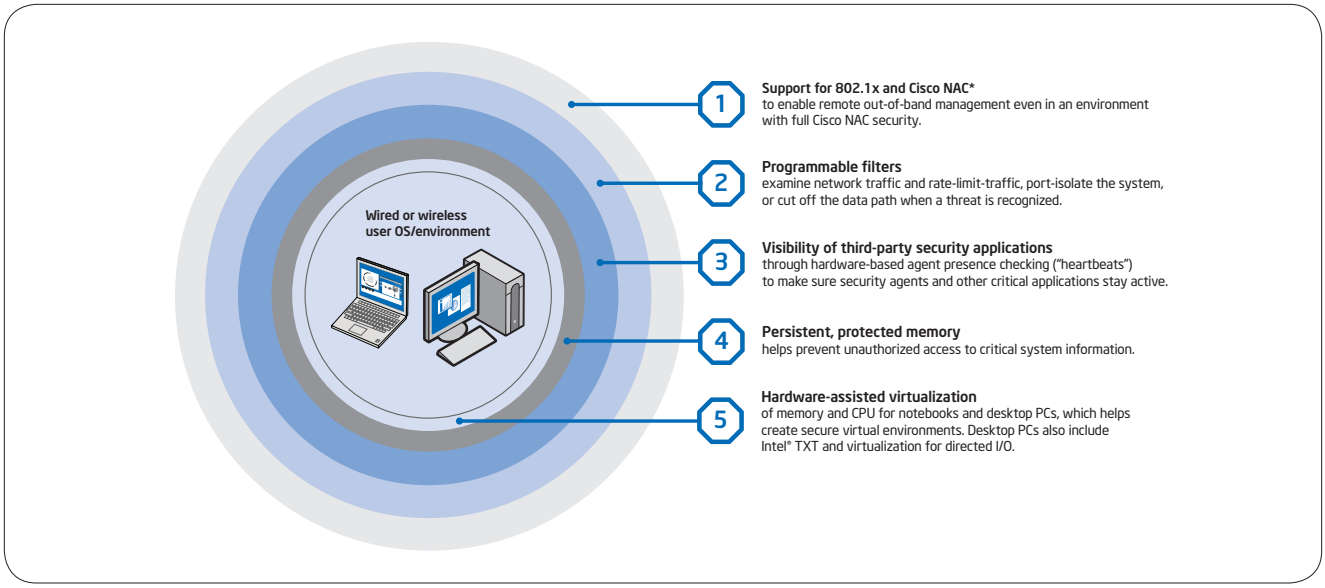

Figure 4. New layers of defense. Hardware-based security capabilities offer new layers of defense to fortify the PC against many critical threats.

Support for 802.1x and Cisco NAC

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 NAC. With Intel Centrino Pro and Intel vPro processor technology, network security credentials can be embedded in the hardware. This includes an Intel® Active Management Technology[1] (Intel® AMT) posture plug-in, which collects security posture information (such as firmware configuration and security parameters), and the Intel AMT Trust Agent. These capabilities allow a PC to be admitted to an 802.1x /Cisco NAC network for management or security purposes even if their OS is absent. 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.

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, notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor 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, saving valuable network bandwidth, yet still offering rapid notification of problems. More importantly for notebooks, agent presence checking is enabled for wireless notebooks that are operating outside, not just inside the corporate network. 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 desktop 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 Centrino Pro and Intel vPro processor technology help reduce security risks by allowing authorized technicians to remotely power up PCs. This will help IT organizations substantially speed up critical updates and patches. Technicians can now:

- **Remotely power up** AC-powered, wired 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.

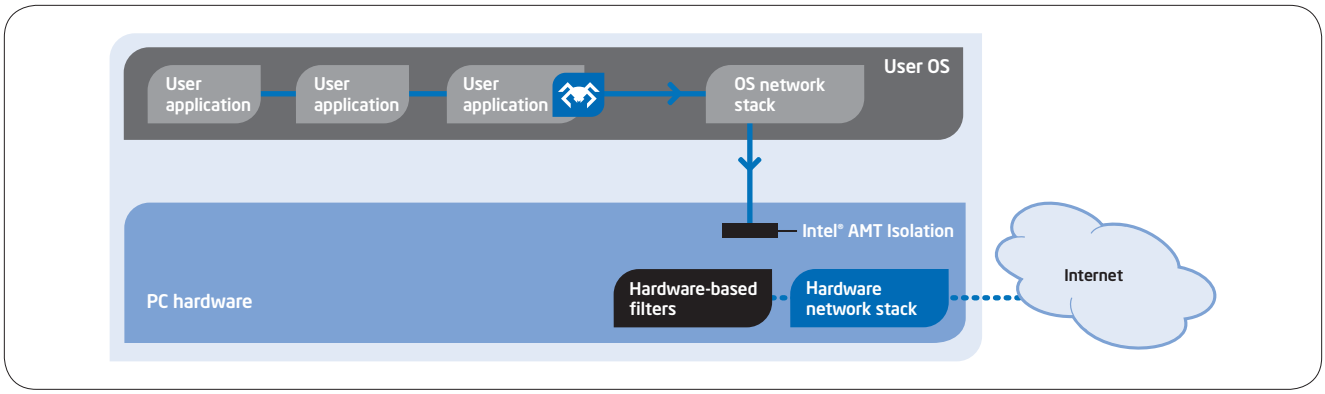

Figure 5. Time-based filters inspect network traffic for desktop PCs. A PC with Intel® vPro™ processor technology can port-isolate itself or cut off its own network data path to quarantine itself when suspicious behavior is recognized – even if its OS is not available – to help prevent threats from spreading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

Filter threats and isolate PCs automatically based on IT policy

PCs with Intel Centrino Pro and Intel vPro processor technology include programmable hardware-based filters for examining network traffic. Notebooks include filters for examining network packet headers for known threats. Desktop PCs include time-based filters that use heuristics to identify potential threats (see Figure 5), including both slow-moving worms and fast-moving worms.

Both notebooks and desktop PCs include isolation circuitry designed into the PC's hardware. When a threat is identified, a policy and hardware-based "switch" can:

- **Isolate the system by port** to halt a suspicious type of traffic.
- **Disconnect the network data path at the OS** (or set a rate limit) to contain threats more quickly.
- **Rate-limit network traffic** to give a technician more time to investigate a threat.

Receive alerts even if a system is off the corporate network

Notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor 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, a desktop PC is powered down, or a wireless notebook is missing its management agents. IT can even receive notifications from a notebook (awake and operable) that is connected to the corporate network through a host OS-based VPN.

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.

Time is money: Save both with simpler remote management whether wired or wireless

Intel Centrino Pro and Intel vPro processor technology provide many innovative hardware-based capabilities to improve discovery and inventory tasks. The key for IT organizations is that the new capabilities are available to authorized technicians anytime: even if the OS is unresponsive, hardware (such as a hard drive) has failed, a hard drive has been reimaged, the OS has been rebuilt, a hardware or software configuration has changed, management agents are missing, or an AC-powered system is off.

Studies show that the new capabilities can help IT organizations reduce the number of deskside visits or service depot calls traditionally required to inventory, upgrade, repair, rebuild, or reimage PCs by up to 80% to 90%.[15] 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, deskside and service-center calls make up only 20% of PC problems in a typical business, but they take up 80% of the budget.[16] In fact, the cost of a deskside visit is seven times the cost of a remote problem resolution. According to an Intel study of 44,000 trouble tickets, approximately 40% or more of the cost of deskside and service center calls could have been eliminated if IT had had better remote capabilities for problem resolution.[16]

Intel Centrino Pro and Intel vPro processor technology deliver many new tools to improve the accuracy of remote hardware diagnostics and substantially reduce the deskside visits or service-depot calls required for OS/software problem resolution:

Problem resolution capabilities in Intel Centrino Pro and Intel vPro processor technology include:

- **Remote/redirected boot,** through integrated drive electronics redirect (IDE-R), a more powerful and secure capability than wake-on-LAN (WOL) and preexecution environment (PXE). 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 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 notebook 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.

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.
- **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.

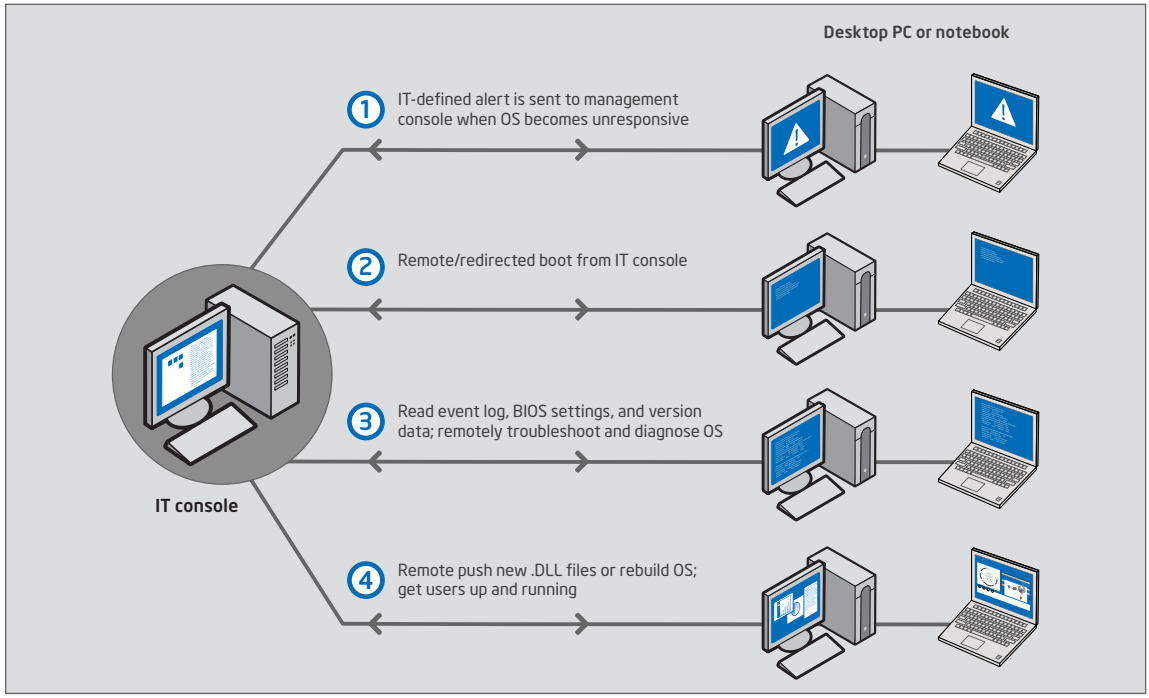

Figure 6. Remote problem resolution for an inoperable OS. New capabilities allow a technician to access, diagnose, and remotely repair or rebuild an OS that has become inoperable, for wired, AC-powered PCs and for awake, wireless systems within the corporate network.

If a system becomes inoperable (see Figure 6), a technician can now use secure remote/redirected boot to change the system's boot device to a CD or to an image located on a remote network drive – without leaving the service center. The technician can then use secure console redirection to remotely guide the 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 deskside 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 industries[17]). For example, Intel training facilities, which include many sites across several continents, investigated the new technology and determined that it could reduce on-site visits for software problem resolution and hardware diagnostics by as much as 75% or more, and speed up IT response time by 80%.[15]

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, U.S. businesses can't find or inventory up to 20% or more of their assets at any given time, and the percentage of "missing" assets for overseas businesses is even higher.[16] Even with excellent asset-location applications and processes, IT organizations still can't find 5% of their assets.[16] In terms of asset maintenance and licensing services alone, today's businesses overspend on average by a factor of 2.[16] 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.

Intel Centrino Pro and Intel vPro processor technology give authorized technicians access to critical system information in protected, persistent memory (memory not on the hard drive) to improve discovery and inventory tasks. This information includes the:

- **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.

IT technicians can now:

- **Write asset and other information** (or pointers to asset information) into protected memory.
- **Poll both wired and wireless systems** for hardware and software asset information stored in protected memory.
- **Identify noncompliant PCs** even if management agents have been disabled.
- **Power up wired, AC-powered 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 wireless PC** the next time it is awake, 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.

Two virtualization models

There are two primary models for virtualization, each suited to particular tasks and innovation opportunities. Both are enabled by the hardware-based Intel® Virtualization Technology[2] (Intel® VT) in notebook and desktop PCs.

General-purpose virtualization

In general-purpose virtualization, the user has access to multiple fully functional OS environments running in separate virtual machines. For example, the PC could have Microsoft Windows XP* and Linux* running side-by-side. General-purpose virtualization usually requires that you install a VMM software package from a vendor like VMware, Microsoft, or Parallels, then build OS and applications images on top of the VMM software.

General-purpose virtualization has been widely 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. Lately, this model has also been used by companies to aid in Microsoft Windows Vista migration, by keeping unportable legacy applications running in an earlier OS, while moving the rest of their applications over to Windows Vista. Other companies are using application isolation to maintain the security and privacy of highly sensitive data.

Intel VT is enabled today in general-purpose VMM packages from vendors such as VMware, Microsoft, and Parallels.

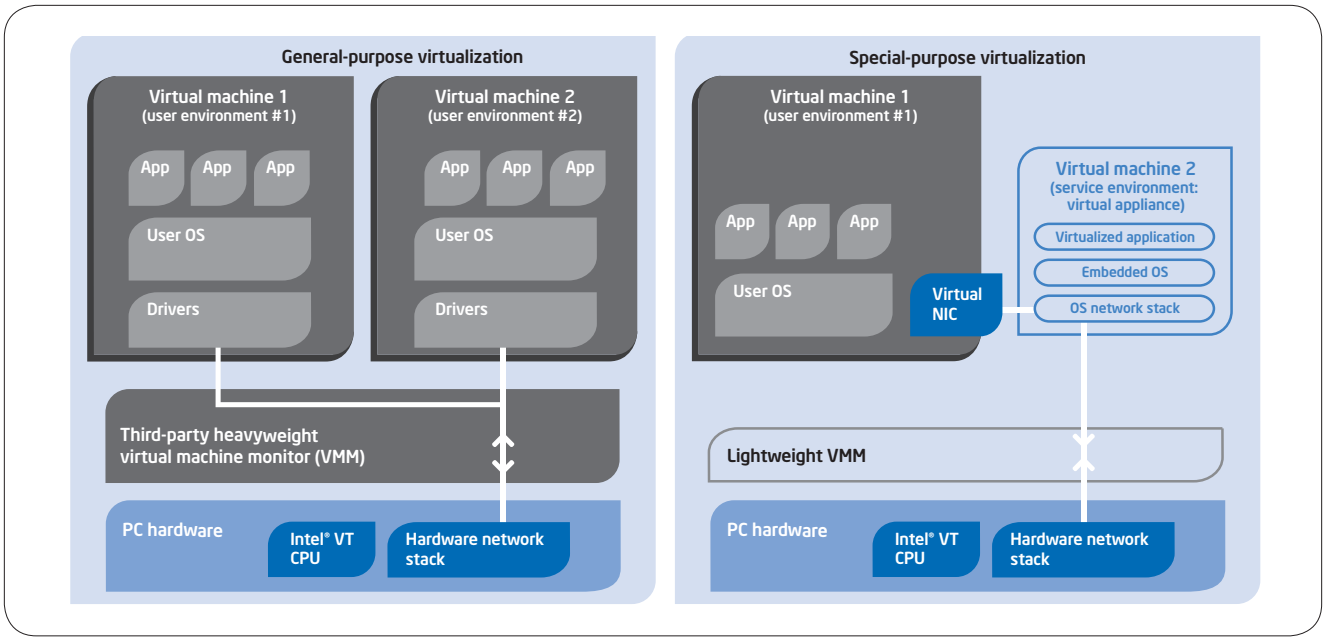

Figure 7. General-purpose virtualization vs. special-purpose virtualization. On desktop PCs with Intel® vPro™ processor technology, virtualization can also be accomplished through the use of a special-purpose virtual appliance designed for a specific function.

Special-purpose virtual appliance

The second model is called the virtual appliance model. Here, the PC has one fully featured OS that supports all user applications. The PC also has a second, special-purpose OS (virtual machine) that provides vital security or management services to the user OS (see Figure 7).

What a virtual appliance does. The "service" virtual machine contains a compact application designed for a specific purpose, such as intrusion prevention, software policy compliance monitoring, and virus outbreak containment. Because of its relatively simple architecture and special-purpose, a service virtual machine is called a "virtual appliance." The virtual appliance is isolated from the user OS, and is nearly invisible to the user.

What a virtual appliance includes. A virtual appliance is a single software package that includes the application code, an embedded OS, all required drivers, and a lightweight VMM. Virtual appliances are managed centrally by IT and generally don't allow or require user interaction. Also, the lightweight VMM is designed to divert network traffic through the appliance, but there is usually no need to virtualize all other platform functions, such as graphics or hard-drive functions.

Benefits of a virtual appliance. There are several benefits to using a virtual appliance:

- **Self-contained environment** offers tremendous control over the scope, functions and interactions of the appliance.
- **The appliance is more resistant to user tampering or software attack** since it resides in a separate virtual machine, out of view of the users and not visible to application software running in the user OS.
- **The relatively compact size** of the appliance provides a smaller attack surface that must be defended, as compared to defending security software in a fully featured user OS (see Figure 8 on the next page).

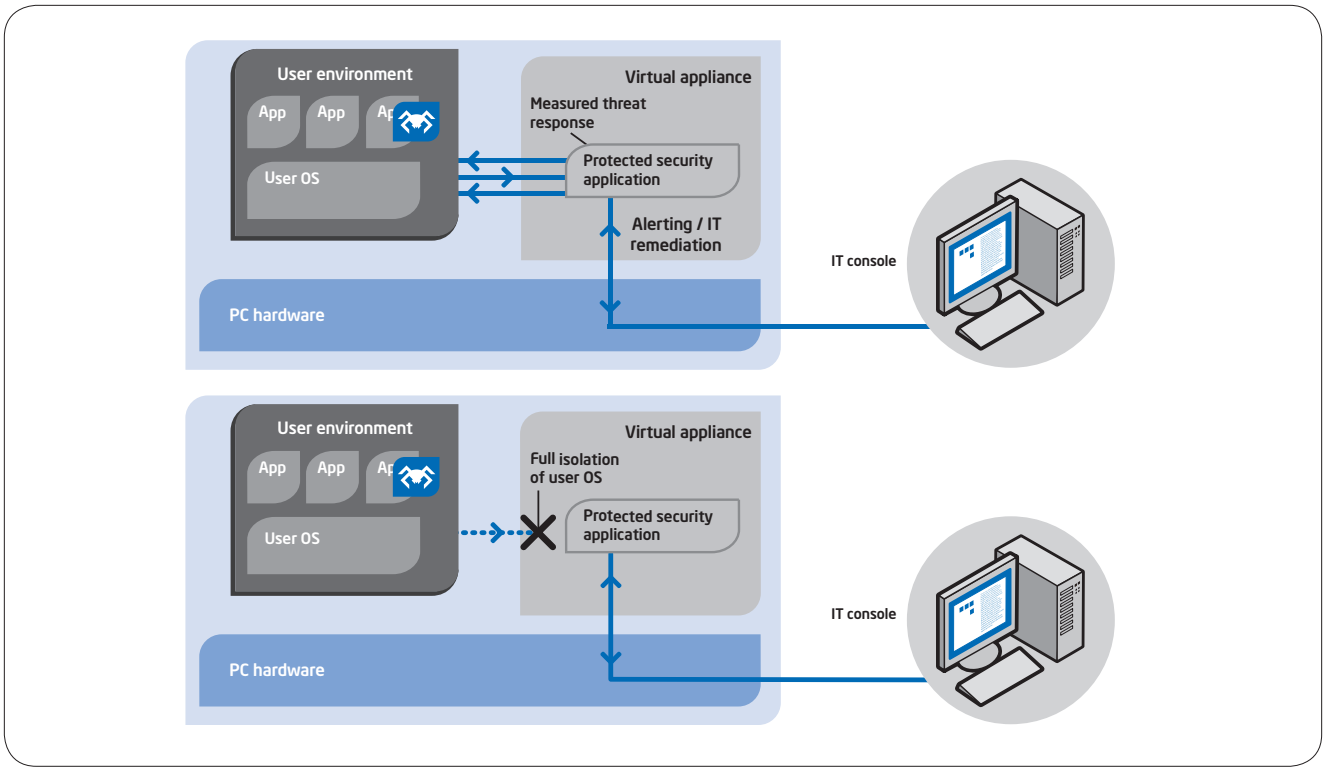

Figure 8. A virtual appliance can offer sophisticated capabilities. Fully integrated application code offers IT a rich set of capabilities for management and security of the user OS. For example, a security appliance can offer IT many remediation paths, from a measured response to full isolation of the user OS.

Virtual appliance: Turnkey solution. Virtual appliances based on Intel VT give IT administrators a turnkey solution that can be installed and managed like any other self-contained application. Unlike general-purpose virtualization, in special-purpose virtualization, there is no need for IT administrators to build the OS and application stacks in a virtual appliance. The service OS and application stacks are part of a single install from the third-party vendor. For desktop PCs with Intel vPro processor technology, Intel VT is enabled today on virtual appliances from leading providers, such as Lenovo and Symantec.

Compatible with other technologies. Standard memory, storage, and graphics cards work with virtual-appliance technology.[2] Desktop PCs with Intel vPro processor 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 Intel security and management technologies, such as Intel AMT.

Intel processor technologies improve virtualization

Today, virtualization can be achieved entirely with software – but this approach has several limitations. There are two areas in particular where improvement is needed: first, reducing overhead of virtualization, and second, improving isolation of each virtual machine from the other virtual machines on the system and from an attack on the VMM. In PCs with Intel Centrino Pro or Intel vPro processor technology, hardware enhancements both simplify and reduce the overhead of virtualization, and help make virtualization more secure and efficient.

Reducing complexity and overhead

Much of the overhead in software-based virtualization comes from managing the functions required to keep the software stack working properly for a full user OS environment.

- **Without virtualization: OS runs at Ring 0.** In a PC that is not virtualized, the OS runs 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. In software virtualization, the VMM must work hard to manage all the hardware calls, traps, driver translations, and other functions that keep the software stack working properly.
- **Hardware-enhanced Intel VT: New Ring below Ring 0.** The OS, drivers, and applications run at their normal privilege levels. The VMM now runs at "Ring -1." This significantly reduces VMM overhead and complexity.

With Intel Centrino Pro and Intel vPro processor 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 Centrino Pro and Intel vPro processor technology) support isolated memory spaces for each virtual machine. In these virtual machines, data in reserved memory spaces is isolated and protected from software running in the processor that is supporting other virtual machines. This feature provides a significant new level of hardware enforcement for the VMM's memory manager.

Improved isolation and security: Virtualization for Directed I/O

With the current release of Intel vPro processor technology (2007), Intel adds new isolation and protection mechanisms through Intel VT for Directed I/O. This feature prevents unauthorized direct memory accesses (DMAs) from the hardware from reading or writing information to other virtual machines that do not have access permission.

The combination of processor virtualization in Intel VT and Intel VT for Directed I/O protects each virtual machine from any application, OS, driver or hardware DMA that it did not request. The result is significantly improved isolation of the virtual appliance and better security for critical processes and sensitive data.

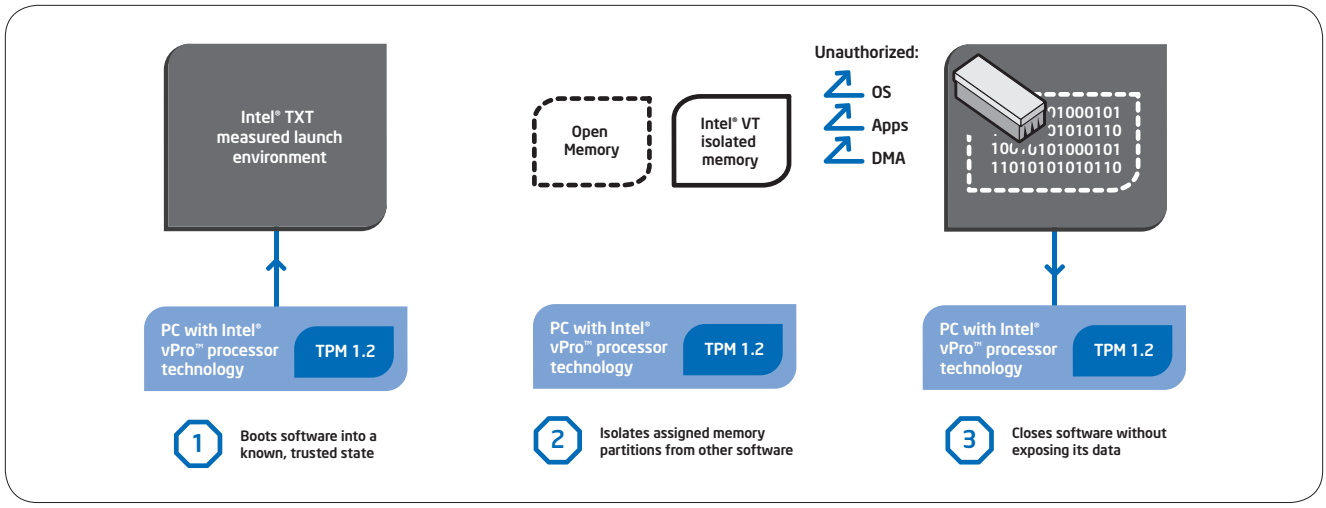

Figure 9. Intel® Trusted Execution Technology (Intel® TXT) verifies launch environment and establishes the chain of trust. Virtual machine data stored in memory is erased by the VMM during orderly shutdowns, and erased by Intel® TXT in the event of a disorderly shutdown or system crash. This significantly reduces the likelihood of confidential data being exposed.

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)[4]

Intel TXT (see Figure 9) is designed to address the important security issue of protecting and establishing trust in the VMM using a hardware-rooted process that builds 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 now available in desktop PCs with the current release of Intel vPro processor technology (2007).

Building the chain of trust

The root of trust for a trusted software stack is the Intel® Core™2 Duo processor E6x50, Intel® Q35 Express chipset,[18] 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 virtual appliance, 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 TPM.
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.

Table 6. Virtualization software support

Advanced technology	Offers	Intel® Centrino® Pro processor technology (2007)	Intel® vPro™ processor technology (2007)	Expected in Intel® Centrino® Pro processor technology[a] (2008)
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
Virtual appliance ready	Supports special-purpose virtual machines (appli-ances)	No	Yes	Yes

[a] Features in future platforms are for planning purposes only and are subject to change.

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.

Roadmap for virtualization technology

Table 6 briefly lists the virtualization technologies available in notebooks with Intel Centrino Pro processor technology (2007) and desktop PCs with Intel vPro processor technology (2007).

Intel TXT and Intel VT for Directed I/O are expected to be enabled in software applications in late 2007, first in general-purpose VMM packages from vendors such as Parallels, then supported in virtual appliances in 2008.

Simplify and speed up remote configuration

Intel Centrino Pro and Intel vPro processor technology allow powerful out-of-band access and management of PCs. Because of this, 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. This can be done in several ways: light touch, partially automated, or fully automated process.

Three steps to deploy PCs

Deployment of PCs with Intel Centrino Pro or Intel vPro processor technology follows three general steps. Configuration is a self-initiated automated step that depends on security credentials being in place. You can use various levels of automation to create and establish security credentials to simplify deployment.

1. **Establish management console,** including the setup-and-configuration (SC) server.
2. **Create and establish security credentials manually or automatically:** Generate unique key pairs for each PC with Intel Centrino Pro or Intel vPro processor technology. Then enter the unique key pair on each PC: manually via BIOS, automatically via USB key, or as preestablished parameters via the OEM.
3. **Self-initiated, automated configuration:** Plug PC into power and the network to allow self-initiated, remote configuration.

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.

Various levels of automation

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 Centrino Pro and Intel vPro processor technology offer several options for using manual or automated processes to remotely establish security credential in order to automatically configure the PC:

- Fully automated remote configuration, via certificates
- Partially automated remote configuration, via preshared keys
- Light-touch configuration, via manually entered unique key pairs

Fully automated remote configuration

This process requires that your original equipment manufacturer (OEM) establish security credentials and set certain parameters in BIOS and the Intel Management Engine BIOS extension (MEBx). An AC-powered PC ready for fully automated remote configuration has these settings 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 in S0, or the Intel Management Engine must be shipped in the "enabled" state for all sleep states (S0-S5)
- The notebook or desktop PC must be AC-powered during the automated remote configuration process
- Security credentials (root certificates) are preloaded, and an Intel AMT SSL (secure sockets layer) certificate is established
- Network is configured for dynamic IP addressing (DHCP)

In fully automated remote configuration, 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 AC-powered notebook or desktop PC can initiate its configuration even before management agents are installed and set itself up for remote configuration in your environment based on the parameters specified by your setup-and-configuration server.

Partially automated configuration

This configuration option is for IT administrators who prefer to enter the security credentials for Intel AMT in-house, such as in an IT staging area (typically with an isolated, secure network). In partially automated configuration, the IT administrator enters credentials on each PC via a USB key. As soon as credentials are entered, the PC can be deployed to the user desk, and will initiate its own automated configuration.

Security credentials entered via USB key include:

- Administrator username and password
- Provisioning passphrase
- Provisioning ID

Light-touch configuration

This configuration option lets IT administrators enter security credentials (administrator password, provisioning passphrase, provisioning ID) manually through BIOS settings, a process typically used for the highest-security environments. As soon as security credentials are entered, the PC can be deployed to the user desk, and will initiate its own automated configuration.

With three methods for deployment, IT administrators can choose the level of security and automation appropriate for their 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 businesses can't afford to keep laying more power lines into their facilities just to provide users with the performance needed to get the job done.

Enter PCs with Intel Centrino Pro and Intel vPro processor technology. These notebook and desktop PCs deliver improved performance per watt, outstanding performance for multitasking, and support for future OSs.

Improved performance and efficiency

PCs with Intel Centrino Pro and Intel vPro processor technology deliver excellent performance per watt via:

- **64-bit Intel® Core™2 Duo processor for multithreaded performance.** This processor is optimized for improved multitasking and multithreading with compute-intensive applications, and it delivers 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 and great battery life.** Advanced architecture, package design techniques, power coordination, and thermal technologies let Intel CPUs 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. In desktop PCs, the result is excellent performance in quieter, smaller form factors. Notebooks with Intel Centrino Pro processor technology not only consume less power, but also include improved battery technologies, offering greater efficiency which enables great battery life for users.
- **Optional Intel® Turbo Memory for notebooks.** On notebooks with Intel Centrino Pro processor 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. For example, notebooks using Intel Turbo Memory typically launch applications up to 2x faster and boot up to 20% faster.[19]

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

Notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor 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 Centrino Pro and Intel vPro processor 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,[20] and other advanced features.[21]
- **Multithreaded CPU: Ready for Office 2007.*** The Intel® Core™2 Duo processor provides 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 Centrino Pro and Intel vPro processor 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 Centrino Pro and Intel vPro processor technology are:

- **Built on standards.** Intel Centrino Pro and Intel vPro processor technology are built on industry standards to give you many choices in selecting OEMs and software vendors. Some of the standards upon which Intel Centrino Pro and Intel vPro processor technology are built include ASF, XML, SOAP, TLS, HTTP authentication, and Kerberos. PCs with Intel vPro processor technology also support next-generation protocols such as DASH and WS-MAN.
- **Broad industry support.** Intel Centrino Pro and Intel vPro processor technology are supported by major software vendors in security software, management applications, and business software. PCs with these processor technologies are available from leading, worldwide desktop and notebook OEMs and are supported by major IT service providers and managed service providers.
- **Stable and simple.** PCs with Intel Centrino Pro and Intel vPro processor technology are available under the Intel® Stable Image Platform Program[8] (Intel® SIPP), so businesses can avoid unexpected changes that might force software image revisions or hardware requalifications. With Intel SIPP-compliant notebooks and desktops, IT can be more assured of having a stable platform that simplifies the deployment of new notebook and desktop PCs.

Wired or wireless: Security and manageability on a chip

Intel is uniquely positioned to provide critical business and IT capabilities on a notebook or desktop PC through extensive, breakthrough R&D, 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 manageability capabilities of notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology visit www.intel.com/go/businesspc.

[1] Intel® Centrino® Pro processor technology and Intel® vPro™ processor technology include powerful Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. With regards 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] Intel® Virtualization Technology (Intel® VT) 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.

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

[4] 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

[5] Support for Cisco NAC on notebook PCs with Intel® Centrino® Pro processor technology requires Intel® Active Management Technology (Intel® AMT) firmware version 2.6. Notebooks with Intel AMT release 2.5 cannot be upgraded to Intel AMT firmware release 2.6 in the 2007 mobile Intel® Stable Image Platform Program (SIPP) cycle due to Intel AMT and wireless LAN software driver change requirements.

[6] 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. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

[7] 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.

[8] Check with your PC vendor for availability of computer systems that meet Intel® Stable Image Platform Program (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® Centrino® Pro processor technology with Intel® Active Management Technology release 2.6 is not supported in the 2007 Intel Stable Image Platform Program.

[9] Wireless access to the powerful capabilities of Intel® Centrino® Pro processor technology requires WPA, WPA2/802.11i security.

[10] For detailed information about the security methodologies and technologies used to protect the capabilities of Intel® Centrino® Pro processor technology and Intel® vPro™ processor technology, refer to the Intel® Active Management Technology Deployment and Reference Guide, Intel, 2006, at www.intel.com/business/vpro.

[11] 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.

[12] 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 Intel Centrino processor technology systems. See http://www.intel.com/products/centrino/index.htm and http://www.intel.com/performance/mobile/benchmarks.htm for more information.

[13] 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.

[14] In order to experience the new benefits of wireless-n on notebooks with Intel® Centrino® Pro processor 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.

[15] Source: Various white papers, such as "Cutting-Edge Performance and Remote Manageability Reduce Training-Room Costs," published January 2007, Intel; "Reducing Manual Processes with Improved Remote Security, Inventory, and Problem Resolution," Intel, 2006; and other white papers available on the Intel Web site at www.intel.com/go/businesspc.

[16] Source: Intel white paper: "Reducing Costs with Intel® Active Management Technology," published August 2005. To download the white paper, visit www.intel.com/go/iamt.

[17] 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

[18] For Intel® AMT release 3, Intel® Trusted Execution Technology is supported by the Intel® Core™2 Duo processors E6550, E6750, and E6850.

[19] 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. Boot-time performance depends on BIOS and POST execution times as well as hard-drive performance. Power savings will depend upon the system power management settings as well as the specific hard drive used. See http://www.intel.com/performance/mobile/benchmarks.htm for more information.

[20] Any disk encryption technology may limit certain remote management capabilities. See your software vendor for information on interaction of disk encryption software and remote management.

[21] For information about system requirements for Windows Vista,* refer to http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/capable.mspx.

Printed in USA 0707/LKY/OCG/PP/5K Please Recycle 311710-004US