



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 to increase security and simplify system management

A new generation of notebook and desktop PCs provides 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 is unresponsive, software agents are disabled, a desktop PC's power is off, or a notebook's management agents have been disabled. Desktop PCs also include support for virtual appliances that allows IT managers to isolate and protect critical security and management applications in a tamper-resistant environment. In addition, the new generation of notebook and desktop systems delivers significantly improved performance for compute-intensive tasks – all in a power-efficient package that is Microsoft Windows Vista* ready.



Table of Contents

| | |
|---|-----------|
| Executive Summary | 3 |
| Intel® Centrino® Pro and Intel® vPro™ processor technology | 4 |
| Today's IT challenges | 4 |
| Improve security and simplify remote management..... | 4 |
| <i>Sidebar: Intel® Centrino® Pro and Intel® vPro™ processor technology.....</i> | <i>4</i> |
| Addressing both IT and user needs..... | 7 |
| Use an existing management console for both notebook and desktop PCs | 7 |
| Managing the wireless notebook | 8 |
| “Readily-available” tamper-resistant capabilities..... | 10 |
| Remote-communication channel runs outside the OS..... | 10 |
| <i>Sidebar: Wireless technologies</i> | <i>10</i> |
| Active states for the Intel® Management Engine..... | 12 |
| Robust security methodologies for tamper-resistant capabilities | 12 |
| Improved security for notebook and desktop PCs..... | 12 |
| New layers of defense | 12 |
| Automated, continual checking for agents | 13 |
| Push updates down the wire – regardless of PC power state..... | 13 |
| Filter threats and isolate PCs..... | 14 |
| Receive alerts even if a system is off the corporate network..... | 14 |
| Simpler remote management whether wired or wireless | 14 |
| Accurate, remote discovery and inventory for wired or wireless systems..... | 15 |
| Resolve more problems remotely..... | 15 |
| Common use cases..... | 17 |
| Support for hardware-assisted virtualization..... | 18 |
| Heavyweight vs. lightweight virtualization..... | 18 |
| What is a virtual appliance? | 18 |
| <i>Sidebar: Complementary types of outbreak containment.....</i> | <i>18</i> |
| Benefits of virtual appliances | 19 |
| Improved energy-efficient performance | 21 |
| Intel® Core™2 Duo processor | 21 |
| Cutting-edge transistor technologies..... | 21 |
| Optional Intel® Turbo Memory speeds up booting and application launching | 21 |
| Stable, standards-based, and ready for the future, with broad industry support | 21 |
| Built on standards..... | 21 |
| Ready for Windows Vista* and Office 2007*..... | 22 |
| Broad industry support..... | 22 |
| Stability and simplicity | 22 |
| Wired or Wireless: Proactive security and built-in manageability | 23 |

Executive Summary

Notebook PCs with Intel® Centrino® Pro processor technology and desktop PCs with Intel® vPro™ processor technology¹ deliver new, built-in security and remote management capabilities to meet critical business challenges. IT administrators can now more quickly identify and contain more security threats, take more accurate asset and hardware/software inventories remotely, resolve more software and OS problems faster and 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 secure and manage wireless notebooks across a variety of wireless networks – even if the OS is unresponsive or software agents are missing; and secure 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 virtualization² for mainstream business. IT technicians can now run critical security applications in a simplified, self-contained, 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 manageability and security 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

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.

Software-only management and security solutions for PCs have been unable to work around a fundamental limitation: they cannot secure or manage a PC that is powered off or whose operating system (OS) is unresponsive. 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 of technology. A critical capability that would help IT do more with the resources they have is the ability to remotely manage and effectively secure both notebook and desktop PCs regardless of wired or wireless state, power state, or the health of the OS.

Improve security and simplify remote management

Intel Centrino Pro and Intel vPro processor technology¹ are designed to address the top IT challenges in security and manageability. This new generation of notebook and desktop PCs delivers tamper-resistant security and management capabilities that are based in hardware, not software. The advantage of the hardware-based capabilities over traditional software-based solutions is in allowing remote access to PCs that have traditionally been unavailable to the management console.

Intel® Centrino® Pro and Intel® vPro™ processor technology¹

Notebook and desktop PCs based on these advanced processor 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 performance for compute-intensive applications and multitasking – a unique combination of capabilities, only from Intel.

| Intel® Centrino® Pro processor technology | Intel® vPro™ processor technology |
|--|---|
| Intel® Core™2 Duo processor T, L, and U 7000 ^A sequence | Intel® Core™2 Duo processor E6000 ^A sequence |
| Mobile Intel® 965 Express Chipset with ICH8M-enhanced | Intel® Q965 Express Chipset with ICH8DO |
| Intel® Active Management Technology ¹ (Intel® AMT) | Intel® Active Management Technology ¹ (Intel® AMT) |
| Intel® Virtualization Technology ² (Intel® VT) | Intel® Virtualization Technology ² (Intel® VT) |
| Support for 802.11a/b/g wireless protocols, with available support for draft n | Support for virtual "appliance" applications |
| 64-bit enabled ³ | 64-bit enabled ³ |
| Execute Disable Bit ⁴ | Execute Disable Bit ⁴ |
| Intel® Stable Image Platform Program (Intel® SIPP) | Intel® Stable Image Platform Program (Intel® SIPP) |
| Windows Vista* Ready | Windows Vista* Ready |
| Windows Vista* BitLocker* Ready | Windows Vista* BitLocker* Ready |

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

- **Hardware-based security capabilities**, to help improve compliance down-the-wire, ensure that third-party security software is available when needed, and remotely identify viruses, worms, and other threats faster and stop those threats more effectively.
- **Remote problem-resolution capabilities**, to help accurately diagnose hardware problems and troubleshoot and resolve more software and OS problems – including OS rebuilds – without leaving the service center.
- **Remote hardware and software inventory capabilities**, even if the OS is unresponsive or a system is powered off.
- **Remote asset inventory (discovery) capabilities**, to more accurately identify notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology on the network.

The new capabilities make it easier to automate more diagnostics, repair, and remediation tasks, further improving service efficiencies and freeing resources for other projects.

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.

Authorized technicians can use the new security and remote management capabilities of Intel Centrino Pro and Intel vPro processor technology for:

- **Wired systems.** Whenever a system – notebook or desktop – is plugged into a power source (AC power) and connected to the corporate network with an Ethernet cable, the security and management capabilities of Intel Centrino Pro and Intel vPro processor technology are fully enabled.

These notebook and desktop PCs can be managed similarly through the standard features of your third-party management software. Even when an AC-powered, wired notebook is asleep, virtually all management capabilities are available. The capabilities for AC-powered PCs are available to authorized technicians even when PC power is off, the OS is inoperative, hardware (such as a hard drive) has failed, or software agents are missing.

- **Wireless notebooks.** Notebooks can be remotely secured and managed within the corporate network, anytime they are in an active state (“awake”). This helps make sure that IT processes use battery power only when the system is powered up and awake. Capabilities for these systems are available even if the OS is unresponsive, software agents are compromised or missing, or hardware (such as a hard drive) has failed.⁴
- **Wireless notebooks outside the corporate network.** Some capabilities – such as agent presence checking, access to hardware/software asset information, and alerting – are available even if the wireless notebook is outside the corporate network and connected over a host OS-based virtual private network (VPN).

Figure 1, on the next page, shows the various states in which notebook and desktop PCs can be remotely managed using Intel Centrino Pro and Intel vPro processor technology. Refer to the discussion, *Managing the wireless notebook*, on page 8, for a list of capabilities available in wired and wireless states, active and sleep states, and various power states.

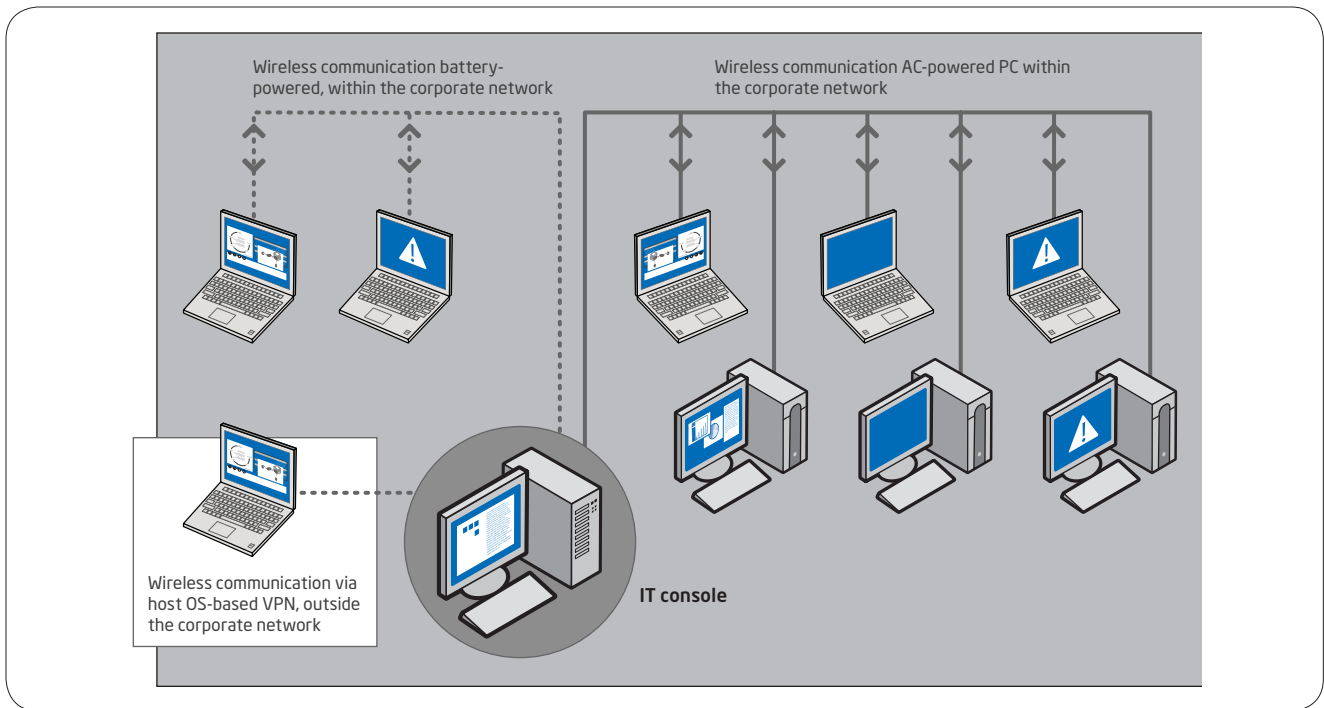


Figure 1. Capabilities are available for both wired and wireless PCs. Hardware-based communication and capabilities are available for desktop PCs and wired-notebooks on AC power within the corporate network even if the PC is powered off or its OS is inoperable. The capabilities are also available for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

Built-in capabilities 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. Some of the security and manageability capabilities that help deliver these benefits include:

- **Remote power-up**, so IT technicians can more securely power up, power down, power cycle, or reset PCs from the management console. This allows technicians to reach more PCs remotely anytime, especially for critical tasks, such as security updates and patching.
- **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.

- **Console redirection**, through serial-over-LAN (SOL), so IT technicians can guide the system through a troubleshooting session without user intervention, and without leaving the management console. 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.
- **Automated, continual 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.
- **System isolation and recovery**, which uses hardware- and software-based filters to check inbound and outbound network traffic for known threats. This capability also provides circuitry that allows IT to define the rules that set rate-limits, trigger port-isolation, or fully isolate a PC (except for the remediation port) by disconnecting its 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.

- **“Readily-available” alerting**, so the PC can send alerts and simple network management protocol (SNMP) traps to the management console anytime, based on IT policies. This gives technicians greater visibility of software inventory changes, OS lock-ups, boot problems, hardware failures, fan speeds, temperatures, case intrusions, and other critical events as they occur.
- **Persistent event logs**, so IT technicians can access the list of events that occurred before a hardware or software problem became apparent, including events that occurred before the notebook or desktop PC connected to the network.
- **Persistent universal unique identifier (UUID)**, stored in persistent, nonvolatile memory. This identifier persists even if a hardware or software configuration has changed, the system has been reimaged, or the OS has been updated. IT technicians can now accurately identify virtually all notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology on the network.
- **Access to preboot BIOS settings**, for verifying configuration information and changing settings as needed to help resolve problems.
- **Access to hardware asset information**, stored in persistent, nonvolatile memory. This information is automatically updated each time the system goes through power-on self-test (POST).
- **Access to third-party data storage**, a persistent, nonvolatile memory space where third-party vendors can store software version information, .DAT file information, machine IDs, pointers to database information, or other data. IT technicians can upload the information in this protected memory space to help with problem resolution, software-asset inventories, application or OS migrations, and so on.
- **Multithreaded performance with Intel® Core™2 Duo processor.** The new notebook and desktop PCs are powered by the state-of-the-art Intel® Core™2 Duo processor. These PCs deliver increased multitasking and multithreading for significantly improved performance over previous-generation notebook and desktop PCs. IT technicians can now run virus scans, e-mail synchronization, back-ups, and other tasks 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 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 and great battery life for users.
- **Ready for Microsoft Windows Vista*:** Notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology are ready for the new Windows Vista OS and three-dimensional Windows Vista Aero* interface. The new PCs include built-in graphics to support the highest levels of the Windows Vista Aero experience, include support for 64-bit applications, and deliver the performance required for the intensive, multithreaded OS.

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.

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 use the same management console and communication mechanisms as other PCs.

Leading management software companies such as Altiris, HP, LANDesk, and Microsoft have already optimized their software to take advantage of the advanced capabilities of Intel Centrino Pro and Intel vPro processor technology. Ask your management-console vendor about support for the new hardware-based security and remote-management capabilities of Intel Centrino Pro and Intel vPro processor technology.

IT administrators now have more control where they need it: at the remote IT console for both wired and wireless systems. 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.

Addressing both IT and user needs

IT organizations typically serve two masters: IT itself, with its requirements for security, maintenance, management, and migration; and users, with their requirements for performance. Notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology deliver:

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 extend battery life for users

by providing remote capabilities depending on the state of the system: 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 1 and 2 show how the capabilities are enabled for wired and wireless notebooks in various states, both inside and outside the corporate network.

Table 1. Capability matrix for wired Intel® Centrino® Pro processor technology based-notebooks and Intel® vPro processor technology-based desktop PCs

| Use Cases | Usages | Ethernet-wired capabilities for Intel® Centrino® Pro processor technology-based notebook or Intel® vPro™ processor technology-based desktop PC, within the corporate network | | | | | |
|--|---|--|------------------|--------|--------------------------|------------------|--------|
| | | Plugged into AC power source - notebook or desktop | | | Battery power - notebook | | |
| | | Awake/operable | Awake/inoperable | Asleep | Awake/operable | Awake/inoperable | Asleep |
| Agent presence checking and alerting | Ensure critical applications are running | Yes | Yes | NA | Yes | Yes | NA |
| System isolation and recovery | Virus outbreak protection | 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, out-of-band via event log stored in nonvolatile memory and SOL / IDE-R | 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 | |

Table 2. Capability matrix for wireless Intel® Centrino® Pro processor technology-based notebooks^a

| Use Cases | Usages | Wireless ^a capabilities for Intel® Centrino® Pro processor technology-based notebooks within the corporate network | | | | | |
|--|---|---|------------------|--------|---|------------------|--------|
| | | Plugged into AC power source - notebook | | | Battery power - notebook | | |
| | | Awake/operable | Awake/inoperable | Asleep | Awake/operable | Awake/inoperable | Asleep |
| Agent presence checking and alerting | Ensure critical applications are running | Yes ^b Also supported in presence of host OS-based VPN | Yes | NA | Yes ^b Also supported in presence of host OS-based VPN | Yes | NA |
| System isolation and recovery | Virus outbreak protection | 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, out-of-band via event log stored in nonvolatile memory and SOL/IDE-R | Yes | Yes | | Yes | Yes | |
| Remote hardware and/or software asset tracking | Take a hardware and software inventory regardless of OS or power state | Yes ^b Also supported in presence of host OS-based VPN | Yes | | Yes ^b 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 | |

^aWireless access to the powerful capabilities of Intel® Centrino® Pro processor technology requires WPA, WPA2/802.11i security.

^bThis capability is available even for wireless notebooks in an awake and operable state which are operating outside the corporate network.

“Readily-available” tamper-resistant capabilities

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 rely on two keys: “readily-available” remote communication with the PC, and robust security technologies. The security methodologies and technologies help make sure both the capabilities and the communication channel are well-secured and resistant to tampering by users, hackers, viruses, worms, and other security threats.

Remote-communication channel runs outside the OS

The communication channel used by Intel Centrino Pro and Intel vPro processor technology runs outside the OS (refer to Figures 2 and 3 on the next page). The 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, it allows authorized IT administrators to 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 missing¹, the communication channel is still available to technicians. 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 channel is available anytime the system is awake and connected to the corporate network via an Ethernet cable. The communication channel is even available for wireless notebooks connected over a host OS-based VPN outside the corporate network when notebooks are awake and working properly.

Wireless technologies

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

- 802.11a/b/g protocols for secure, flexible wireless connectivity.⁵
- 802.11n, the new draft standard expected to deliver up to 5x improvement in data throughput.⁶
- 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 Intel® Next-Gen Wireless-N⁷ 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.⁶ 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.

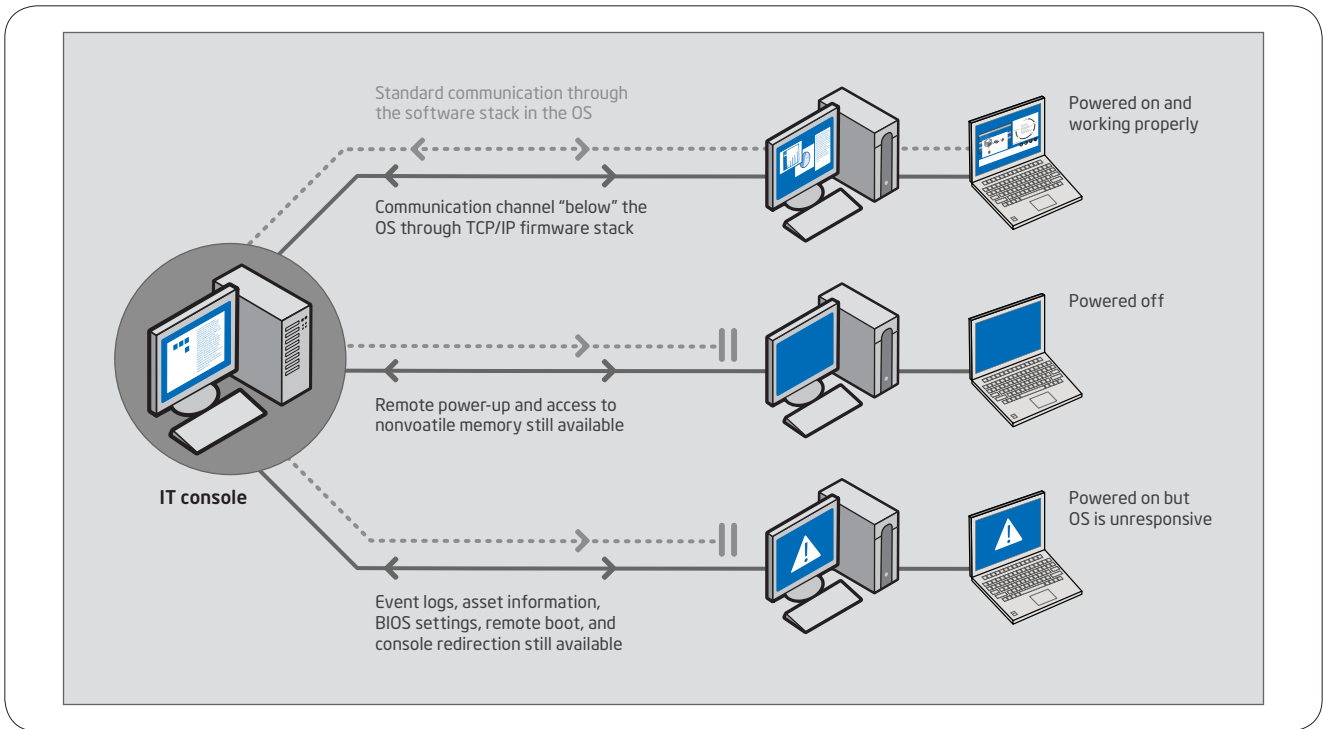


Figure 2. Remote communication with wired systems. All applicable capabilities are available for notebooks with Intel® Centrino® Pro processor technology and desktop PCs with Intel® vPro™ processor technology that are plugged into AC power and connected to the corporate network via an Ethernet cable.

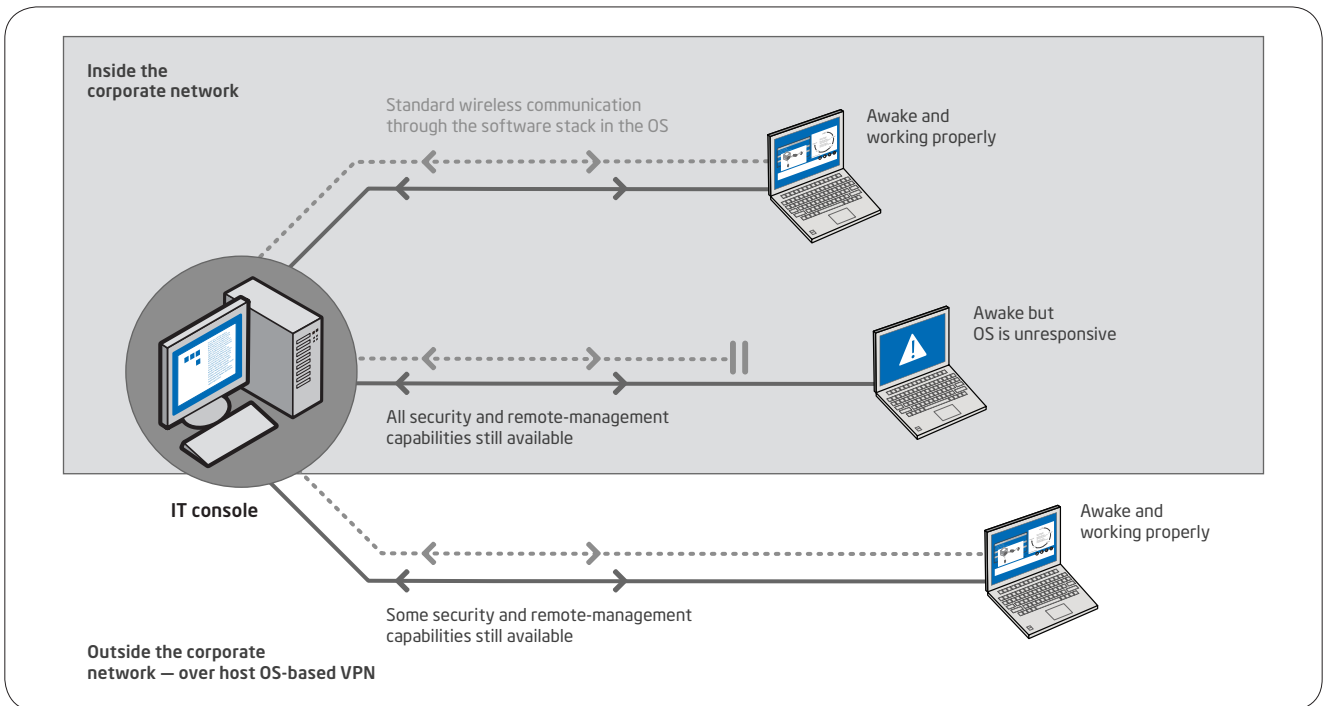


Figure 3. Remote communication with wireless systems. Technicians have some remote service capabilities for wireless Intel® Centrino® Pro processor technology-based notebooks both inside and outside the corporate network.

Active states for the Intel® Management Engine

The security and management capabilities of Intel Centrino Pro and Intel vPro processor technology are embedded in the system's hardware and firmware as part of the Intel® Management Engine.

When a PC (notebook or desktop) is AC-powered, the Intel Management Engine is on - even when the system is powered off. This allows technicians to securely access asset information, power up a PC to receive a security update, and perform other tasks off-hours or when it is most advantageous to users.

When notebooks are on battery power, the Intel Management Engine is active (and the security and management capabilities available) when the system is on and in the awake state. This helps preserve battery life when notebooks are asleep, hibernating, or powered off.

Robust security methodologies for tamper-resistant capabilities

The hardware-based communication and manageability capabilities are secured through a variety of robust schemes.⁸ 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.

Improved security for notebook and desktop PCs

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.

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 (refer to Figure 4 on the next page). There are now several distinct layers of protection for both notebook and desktop PCs, including filtering of network traffic, "heartbeat" presence checking of third-party agents, and other key capabilities:

- **Proactive filtering of threats and isolating PCs** through hardware/software filters.
- **Remote visibility of software agents** through agent-presence checking.
- **Nonvolatile memory** to better protect critical system information.
- **Optional hardware-based "virtual appliance"** for desktop PCs with Intel vPro processor technology. (Refer to the virtual-appliance section on page 18.)

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.

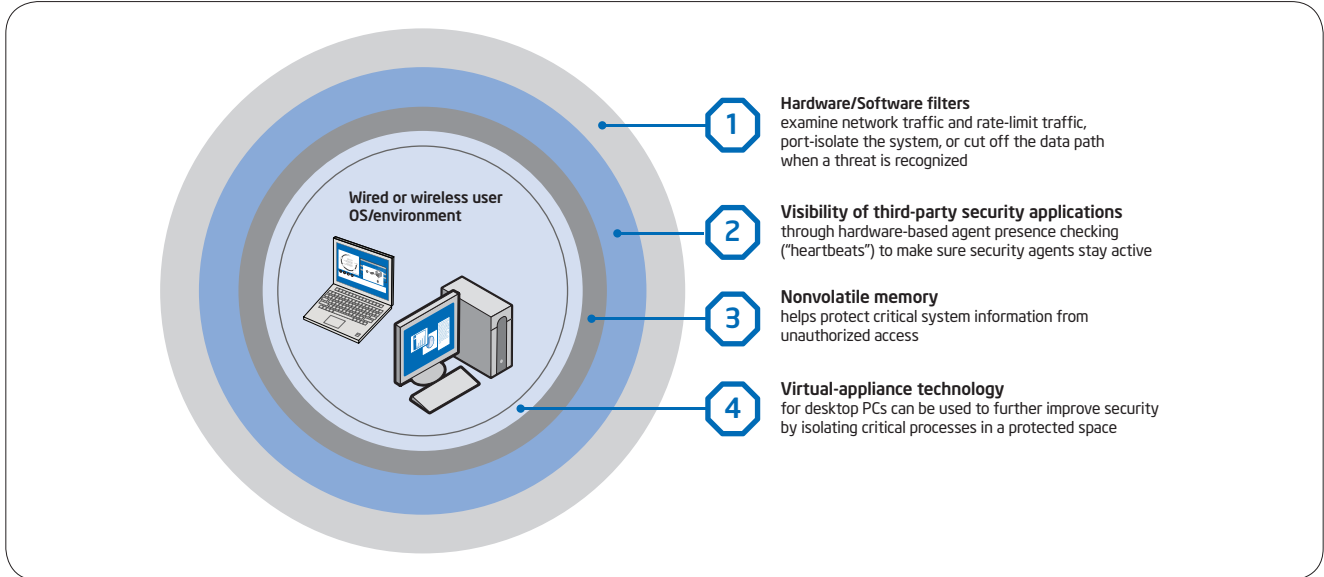


Figure 4. New layers of defense. Hardware-based security capabilities offer new layers of defense against many critical threats.

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. 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 (AC-powered and wired notebooks and desktop PCs). This will help IT organizations substantially speed up critical updates and patches. Technicians can now:

- 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.
- 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.

The new capabilities allow IT administrators to automate more security processes. In turn, this can help IT administrators establish a more secure, well-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 required for updates, critical patches, and remediation, and help reduce risks to the network as a whole.

Filter threats and isolate PCs

Notebooks with Intel Centrino Pro processor technology and desktop PCs with Intel vPro processor technology include programmable hardware- or software-based filters that examine network traffic to help identify threats (refer to Figure 5). 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

The PC can now help protect itself and reduce the risk of threats spreading to the network.

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 designed into the system. IT administrators can now define the types of alerts they want to receive – so less critical alerts do not add substantially to network traffic (all alerts are logged in the persistent event log). Since alerting uses the “readily-available” communication channel, IT can receive critical notifications from PCs within the corporate network, 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 wireless notebook (awake and operable) that is outside the corporate network and connected via host OS-based VPN.

Simpler remote management whether wired or wireless

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

The new capabilities can help IT organizations reduce the number of deskside visits or service depot calls required to inventory, upgrade, repair, rebuild, or reimage PCs by up to 80% to 90%.⁹ 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.

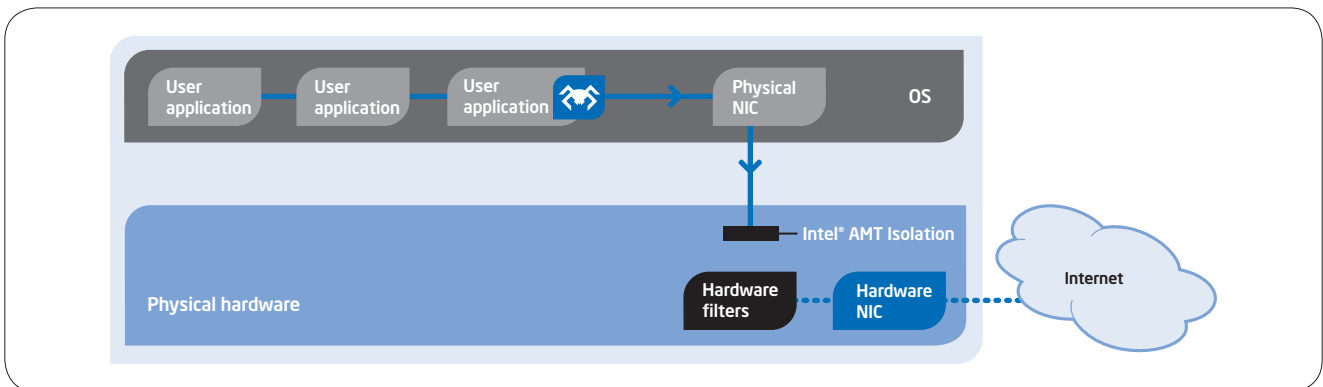


Figure 5. Filters inspect outbound network traffic. Using hardware or software filters, the PC can port-isolate itself or cut off its own network data path to quarantine itself when a threat is recognized – even if its OS is not available – to help prevent threats from spreading to the network.

⁴Intel 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.

[†]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.

¹Intel® Centrino® Pro processor technology and Intel® vPro™ processor technology include powerful Intel® Active Management Technology (Intel® AMT). Intel AMT requires the platform 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>.

²Intel® 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.

³64-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.

⁴Wireless access to the powerful capabilities of Intel® Centrino® Pro processor technology requires WPA, WPA2/802.11i security.

⁵Wireless connectivity and some features may require you to purchase additional software, services or external hardware. References to enhanced wireless performance as measured by Adjacent Channel Interference (ACI)*, 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> for more information.

⁶Up 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.

⁷In 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.

⁸For detailed information about the security methodologies and technologies used to secure 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.

⁹Source: 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/businesspp.

¹⁰Source: Intel white paper: "Reducing Costs with Intel® Active Management Technology," published August 2005. To download the white paper, visit www.intel.com/go/iamt.

¹¹Tests 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.

¹²For more information about system requirements for Windows Vista,* refer to <http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/capable.mspx>.

¹³Any disk encryption technology may limit certain remote management capabilities. See your software vendor for information on interaction of disk encryption software and remote management.

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

Copyright © 2007 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel. Leap ahead., Intel. Leap ahead. logo, Centrino, Intel vPro, Intel Core, and the Centrino logo are trademarks of Intel Corporation in the U.S. and other countries.

Printed in USA

0407/LKY/OCG/PP/SK

 Please Recycle

311710-003US

