3rd Generation Intel® Core™ vPro™ Processor Family Overview

Built for Business. Engineered for Security.

White Paper

3rd Generation Intel® Core™ vPro™ Processor Family

Executive Summary

Today's enterprises demand a lot from their business PCs. To maintain competitive productivity and agility requires instant access, anywhere responsiveness, and a wide range of methods to communicate. Yet companies are very aware of the growing, targeted attacks and persistent threats making their way around the globe and into a PC in their own back yards. Performance and protection are top-of-mind in enterprise IT departments. Business clients based on 3rd generation Intel® Core™ vPro™ processors are built for the needs of business and engineered to protect their data with new levels of performance and unprecedented embedded security technologies combined into a single high-performance, secure business tool. A host of silicon-based technologies within the 3rd generation Intel Core vPro processor family make this possible. This paper surveys those technologies and the benefits they bring to today's demanding, agile enterprises.

3rd Generation Intel® Core™ vPro™ Processor Family

Speed and Security by Design

Business is borderless, mobility is mandatory, and multimedia is mainstream. Business productivity and agility today demands instant access, anywhere responsiveness, and a wide range of methods to communicate. While IT must support these work modes with high-performance PCs, security is top-of-mind for fixed and mobile business clients, and remote and automated manageability is a requirement to help control costs.

Business clients based on 3rd generation Intel® Core™ vPro™ processors include Intel® vPro™ Technology.[1] These PCs integrate hardware-based, built-in features IT personnel need to be proactive, effective, efficient, and responsive. Since the technology is embedded in the hardware, it is out of view and beyond the reach of stealthy malware, and able to deliver unprecedented PC security, secure out-of-band (OOB) communications, and remote manageability. These features help IT departments protect their fleet of business PCs; automate troubleshooting, repair, and maintenance tasks; and reduce deskside and onsite visits. Together, they help IT departments impact their bottom line with lower total cost of ownership (TCO) for business clients and higher operational efficiency.

Unprecedented Security

Embedded security technologies[2] in the 3rd generation Intel Core vPro processor family enable a level of protection not seen in business PCs until now. Operating below the OS, installed agents and applications, these technologies provide a deeper level of threat management; identity and access authentication; data protection; and monitoring, remediation, and reporting to keep the business and data protected. Built-in functionality even allows the business client to monitor and protect itself. Table 1 highlights 3rd generation Intel Core vPro processor family security features.

Table 1. 3rd Generation Intel® Core™ vPro™ Processor Family Security Features

User/IT Requirement	Solution	Intel® Technology
Threat Management Reduce/eliminate ability for invading agents to dig in below the OS.	▪ Prevent sophisticated attacks by virus and malware using rootkits and other stealth techniques. Protect virtual realms, such as data center-hosted desktop virtualization and virtualized environments on business clients, from penetrating rootkits and malware.	▪ Intel® OS Guard[3] ▪ Intel® Trusted Execution Technology[4] ▪ Intel® Virtualization Technology[5]
Identity and Access Protect OTP tokens and PKI certificates. Help ensure only real and authorized users can access authentication credentials.	▪ Secure tokens and certificates in silicon, below the OS, while providing easy maintenance and mitigation. ▪ Protect user input from key loggers and screen scrapers prior to releasing authentication credential.	▪ Intel® Identity Protection Technology[6] with Public Key Infrastructure (PKI) or One-Time-Password (OTP) ▪ Intel Identity Protection Technology with Protected Transaction Display
Data Protection Enable ubiquitous encryption, safer key and encryption foundations, and protect PCs from theft and non-compliance.	▪ Enable fast encryption/decryption without a performance penalty. ▪ Deploy encryption everywhere for safe data. ▪ Generate true random number seeds out of sight and touch of malware. ▪ Protect data on lost or stolen laptops. ▪ Disable lost and stolen laptops automatically.	▪ Intel® Advanced Encryption Standard – New Instructions[7] ▪ Intel® Secure Key[8] ▪ Intel® Anti-Theft Technology[9]
Monitoring, Remediation, and Reporting Enable secure, remote access to clients for quick diagnoses, repair, and token/certificate repair/revocation/re-provisioning.	▪ Enable remote access and troubleshooting/repair for PCs, regardless of power or OS state. ▪ Automatically isolate infected PCs from the network. ▪ Remotely reactivate recovered PCs.	▪ Intel® Active Management Technology[10] ▪ Hardware-based KVM Remote Control[11] ▪ Secure, out-of-band communications

Enhanced Manageability

Using a management console, IT personnel can access built-in manageability functions outside the PC's operating system (OS). Thus, the features are always available, allowing IT to update, troubleshoot, monitor, and secure a business PC, regardless of its power, OS, or hard drive states.

With PCs based on 3rd generation Intel Core vPro processors, IT can connect to management functions over the corporate wired or wireless network, and, in most cases, even if the PC is connected outside the firewall through an open wireless network. These business clients can self-initiate communication with the console for management and maintenance purposes, when a threat is detected, or under other conditions specified by IT management. Table 2 highlights 3rd generation Intel Core vPro processor family manageability features.

Widely Supported

PCs based on 3rd generation Intel Core vPro processors take advantage of the processor, chipset, and networking silicon features, along with protected flash memory. When combined with existing independent software vendor (ISV) consoles, these business clients can deliver a comprehensive, responsive, tamper-resistant solution for security and manageability. Leading management software companies such as HP, LANDesk, Microsoft, and Symantec have optimized their software for 3rd generation Intel Core vPro processor features.

Proven and Trusted ROI

In IT departments, automation and remote access to business clients can have a tremendous impact on IT efficiency and the bottom line. With better remote troubleshooting and problem resolution—through secure console redirection and KVM Remote Control—IT can reduce user downtime, help improve user productivity, keep deskside visits to a minimum, and help businesses significantly reduce TCO. For example:

- For desktop PCs, reduce the need for software-related deskside visits by up to 56%.[13]
- For laptops, improve ability to inventory previously undetected software by up to 47%, and reduce laptop asset inventory failures by up to 62%.[13]
- Run business applications up to 60% faster, experience up to 2x faster multitasking, and see visible performance gains of up to 4x faster encryption/decryption of sensitive data.[14]
- Reduce energy costs and speed up patch saturation by 56%.[13]

Unmanaged PCs waste energy. Simply by remotely powering down the system during off-hours, some companies have recouped their investment in a PC in as little as nine months.[15] Implementing other cost- and time-saving features can result in further savings.

Table 2. 3rd Generation Intel® Core™ vPro™ Processor Family Manageability Features

Manageability Requirement	Benefit/Functionality
Console redirection/ KVM Remote Control[11,a,b]	**Reduces onsite/deskside visits, improves user productivity.** Enables remote assistance, troubleshooting, and repair with access to the client PC as if the technician was in front of it. IT can see and control the PC through all states – power up/down, BIOS, normal operation – regardless of PC power state, OS state, or hard drive availability. IT can redirect bootup to other client device, local IT storage, or network.
Remote power control[a,b]	**Reduces onsite/deskside visits. Reduces power costs.** IT can remotely power PC up or down to troubleshoot, update/upgrade, or for power savings during off hours.
Remote software updates[a,b]	**Reduces onsite/deskside visits and helps maintain health, performance, and reliability of PC.** Remotely update/upgrade OS, agents, and software. Can be done during off-hours to maintain worker productivity. Automatically update and push patches, etc.
Client-initiated wake-up and call-in[a,b]	**Automatically maintains PC health without deskside/onsite visits.** Client-initiates scheduled wake-up (time set by IT). A third-party agent on the PC can then call into a server to initiate updates, maintenance, and other off-hours tasks.[12]
Agent presence checking and alerting[a,b,c]	**Automatically maintains PC health and compliance.** Periodic check-in by client-side agent ensures critical applications are running, and IT is quickly notified when they miss a check-in.[c]
Network traffic monitoring[a,b]	**Maintains PC health and reliability.** Programmable filters monitor network traffic headers and rates for suspicious content.
System isolation and recovery[a,b]	**Protects against virus proliferation across the network.** A detected threat initiates shutdown of the local network connection; management (OOB) connection remains accessible.
Remote diagnosis and repair[a,b]	**Reduces deskside/onsite visits. Lowers TCO.** Diagnose and repair problems remotely via an out-of-band event log, remote/redirected boot, console redirection, KVM Remote Control, and preboot access to BIOS settings.
Remote hardware and/or software asset tracking[a,b,c]	**Maintains PC compliance and health.** Take a hardware or software inventory regardless of OS state or PC power state[c] Asset data is stored in PC's non-volatile memory where IT can access it any time.

[a] IT must activate Intel® vPro™ technology in order to take advantage of these intelligent security and remote manageability technologies. For more information about activating Intel vPro technology, which includes Intel® AMT visit www.intel.com/content/www/us/en/remote-support/implementation-of-intel-vpro-technology.html.

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

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

Unprecedented Protection from Embedded Security

Today's threats attempt to take advantage of every interaction users have with company data and systems. As a result, companies are facing more targeted attacks that do more damage than yesterday's viruses. And cyber-criminals are engaging stealth techniques to make it harder to detect, prevent, and remove threats.

Business PCs based on 3rd generation Intel Core vPro processors offer unprecedented security with embedded security technologies enabled in silicon, rather than software. These built-in, hardware-based technologies enable greater threat management, tighter identity and access protection, better data security, and remote and automated monitoring, remediation, and reporting of events.

Hardware-based Threat Management, Identity and Access

Embedded, hardware-based security technologies in 3rd generation Intel Core vPro processors work below the OS, agents, and application software to prevent threats from attacking and digging in. Plus, they help protect data and machines. Tokens and PKI certificates are protected in silicon, providing the benefit of hardware-based security with the ease of management and fast mitigation response of software-based solutions.

Embedded security technologies in business clients based on 3rd generation Intel Core vPro processors that help manage threats and protect against identify theft and unwanted access include the following:

- **Intel® Identity Protection Technology[6] with OTP or PKI –** Protects One-Time-Password (OTP) tokens and PKI certificates using hardware-assistance, out of sight and reach of malware and the OS – the security of hardware with the convenience and response of software.
- **Intel® Identity Protection Technology[6] with Protected Transaction Display –** Hardware-based authentication proves user presence with secure input.
- **Intel® OS Guard[3] –** Helps keep malware from rooting below the OS.
- **Intel® Trusted Execution Technology[4] –** Verifies a known safe environment for a virtual machine being launched.
- **Intel® Virtualization Technology[5] –** Enhances and secures certain tasks in virtualized environments that further protect the PC.
- **Intel® Anti-Theft Technology[9] –** Protects laptops on the go.

Protecting Data and PCs – Wherever They Are

Hardware-based embedded security technologies in business clients built on 3rd generation Intel Core vPro processors help keep data out of reach of cyber-criminals and protect PCs on the go.

Intel® Advanced Encryption Standard – New Instructions

Encrypted data is protected data. But, traditionally, real-time encryption came at a high performance cost and productivity tax for the user. With Intel® Advanced Encryption Standard – New Instructions[7] built into the processor, encryption and decryption runs up to 4X faster.[14] This performance boost eliminates the performance penalty and enables ubiquitous encryption across business clients based on 3rd generation Intel Core vPro processors.

Intel® Secure Key

When random numbers are needed for encryption, the results are safer with high-quality random numbers generated out of sight and out of reach of malware. Intel® Secure Key[2,8] generates random numbers in discrete silicon using true random number instructions. During generation, nothing is exposed, keeping the process out of reach of any agent that might affect number-generation instructions in software.

Intel® Anti-Theft Technology

When a PC goes missing, the impact can be severe. Intel® Anti-Theft Technology[2,9] (Intel® AT) in every business laptop significantly mitigates the impact. Intel AT automatically and tightly secures the PC under detection of a threat, locking the hard drive(s) and embedded security key(s), which makes the unit useless. Even if the hard drive is removed, the data is inaccessible. On a 3G network, Intel AT can even send a GPS beacon or relay a MAC address to a server, identifying its own location. If the device is recovered, IT personnel can remotely reactivate the unit.

Monitoring, Remediation, and Reporting

For rapid response to detected threats, PCs based on 3rd generation Intel Core vPro processors enable automatic monitoring, automatic and manual remote remediation, and reporting. IT can take advantage of this built-in functionality to rapidly address a threat remotely.

Automatic network monitoring and threat detection

IT managers can program defense filters that monitor inbound and outbound network traffic to guard against viruses and malicious attacks. A detected threat can automatically notify a management server and securely disconnect the PC from the network, while allowing the remediation channel to remain open, so IT can access the PC and repair it.

Continual, autonomous agent checks

Instead of a management console polling PCs for security agents, which can create unwanted network traffic, laptop and desktop PCs with 3rd generation Intel Core vPro processors can be configured to periodically run their own security agent check autonomously. Successful checks are stored in the event log. With the PC itself running its own internal polls, it automatically helps safeguard against certain types of malware and malicious attacks, while not burdening the network with unwanted traffic.

If an agent doesn't check in before its expected check-in time, the PC assumes the agent has been removed, tampered with, or disabled. The unit then immediately logs the alert in nonvolatile memory. If specified by IT policy, the client contacts the management console and sends the alert across the network to a management server.

Receive alerts even if a system is off the corporate network

Policy-based monitoring and alerting is built into PCs with 3rd generation Intel Core vPro processors. All alerts are logged in the persistent, protected event log. IT administrators can define the types of alerts they want to receive, preventing non-critical alerts from adding to network traffic. The event log with all alerts remains available and remotely accessible over the network.

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

Savings from Automation and Remote Manageability

According to industry studies, deskside and service-center calls make up only a small percent of PC problems in a typical business, but they take up the majority of the budget. PCs with 3rd generation Intel Core vPro processors make it easier to reduce maintenance costs by eliminating many deskside and onsite visits, automating maintenance tasks, and ensuring conformance to policies. Built-in management capabilities include:

- Remote configuration, diagnosis, isolation, and repair of PCs, even if systems are unresponsive.
- Automated client wake-up and update of software and agents, even after normal business hours and when the PC is turned off.
- Automated inventory of hardware and software.
- Automated upgrade of applications or OS to Windows 7.*

In addition to positive impacts on IT efficiencies and TCO, PCs stay healthier and businesses can minimize user downtime, while improving productivity.

Greater Automation for Software and PC Compliance

Many leading third-party software vendors offer management consoles that automate functions within PCs based on 3rd generation Intel Core vPro processors. 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, or schedule it for update at a more appropriate time, such as off-hours. After the update, the management application can then remotely return the system to its previous power state. Without the direct intervention of IT, the PC remains healthy and compliant with corporate policies.

Direct Access with Intel® vPro™ Powershell Module

In addition to management consoles, IT technicians can create scripts and automation that might not be available in their management console. Using Windows Powershell* and the Intel® vPro™ Powershell Module, IT personnel can directly access management features to create unique functionality they require.

Resolve More Problems Remotely

3rd generation Intel Core vPro processors can help IT managers reduce deskside visits by up to 56%[13] through features such as:

- **Remote/redirected boot –** Remotely boot a PC to a clean state, or redirect the boot device to a clean image on local storage, on a CD at the help desk, or to an image on another remote drive.
- **Serial-Over-LAN (SOL) console redirection –** Control the keyboard outside of the OS to perform tasks, such as editing BIOS settings from the service center—without user participation.
- **KVM Remote Control –** Take control of the PC as if sitting in front of it to remotely resolve the most complex software failures.

With these tools, IT technicians can now:

- **View asset information anytime,** to identify "missing" or failed hardware components, and verify software version information.
- **Guide a PC through a troubleshooting session** without requiring user participation—even for complex issues such as BIOS issues, blue-screens, freezes, patch failures, and other "edge" software issues.
- **Reboot a system to a clean state,** or redirect the PC's boot device to a diagnostics or remediation server (or other device).
- **Watch as BIOS, drivers, and the OS attempt to load,** to identify problems with the boot process.
- **Update BIOS settings, identify BIOS versions, or push a new BIOS** version to the PC to resolve a particular problem.

- **Upload the persistent event log** to identify the sequence of events (such as temperature spikes or an unauthorized software download) that occurred before the system failed.
- **Restore an OS** by pushing new copies of missing or corrupted files, such as .DLL files.
- **Rebuild the OS** or fully reimage the hard drive remotely.
- **Perform OS migrations and application upgrades,** and troubleshoot upgrade problems remotely.
- **Power-manage PCs more effectively** to lower power consumption and reduce energy costs.
- **Schedule a local wake from a full power down,** to prepare systems for incoming workers.

KVM Remote Control

In spite of improved management tools, almost 20% of problem tickets still require that users help resolve the problem.[16] Even with built-in remote management capabilities, the complexity of these "corner case" or "edge" failures have traditionally meant that a technician must still make a deskside visit or ask users to help resolve the problem. Studies show that hardware-based KVM Remote Control can reduce problem resolution time by 20% for complex software issues[16] by allowing a technician to "get behind the user's keyboard" without leaving the help desk.

Unlike software-based remote desktop, hardware-based KVM Remote Control allows the technician to see and control the PC through all states. This helps technicians resolve software failures for both wired and wireless PCs, even for PCs outside the corporate firewall.

KVM Remote Control in PCs based on 3rd generation Intel Core vPro processors is now available in 27 languages and supports up to three monitors (up to 1920 x 1200 with 16-bit color) in portrait and landscape modes.

Remotely access critical system information

Business PCs with 3rd generation Intel Core vPro processors store preboot BIOS configuration data, hardware and software inventory data, alerts, and other critical system information in nonvolatile memory. This data is available out-of-band – even outside the corporate firewall. IT can remotely access system information that can help with troubleshooting, diagnostics, and repair, even if the OS is not available, the hard drive has failed, or the PC is powered off.

Secure Communications – Inside and Outside the Corporate Network

Software-only management applications installed at the same level as the OS leave their management agents vulnerable to attack. In addition, communicating unencrypted over the in-band network leaves the management transactions open and unsecure. Clients with 3rd generation Intel Core vPro processors use out-of-band (OOB) communication, as well as robust security technologies, designed into the hardware – beyond view and out of reach of the OS and other software – to protect and secure management activities.

The OOB channel uses a special TCP/IP stack embedded in the firmware instead of the OS network stack. The channel secures critical system communication (such as alerting) and operations (e.g., agent presence checking, remote booting, and console redirection), regardless of OS, applications, or hard drive state. Because management is hardware-based, IT can continue to communicate with the business client to troubleshoot, repair, and reboot the PC when there is a problem. Technicians can even remotely take inventory of the PC by reading the PC's protected memory space – even if the management agent is missing.

Outside the corporate firewall, PCs based on 3rd generation Intel Core vPro processors can initiate communications with a remote management console through a secured tunnel. This allows IT technicians to manage and maintain PCs in satellite offices and in locations that don't have an onsite proxy server or management appliance, such as at a small business client's remote location. An onsite visit is eliminated, making IT more efficient and lowering TCO.

With client-initiated, secure connectivity, IT can:

- **Schedule regular times when the client contacts the console,** allowing IT to securely update and service PCs – even during off-hours.
- **Schedule the remote PC to automatically wake itself up** and run scheduled checks, inventories, etc., and then connect to the console for additional tasks or updates.
- **Configure a keyboard hotkey on the client,** so a user can quickly connect the PC to the IT console for help or system servicing, giving the user peace of mind and making it easy for IT to support remote personnel without a phone call.

Out-of-Band Management with 802 .1x, Cisco SDN,* and Microsoft NAP*

PCs based on 3rd generation Intel Core vPro processors support full network security using 802.1x, Cisco SDN,* or Microsoft NAP.* This capability also provides IT administrators with OOB access for maintenance, security, management, or PXE purposes, while still maintaining full network security, including detailed, out-of-band compliance checks.

Maintaining Compliance

The asset management capabilities and asset information stored in nonvolatile memory help reduce time-consuming manual inventories, which can save significant costs in labor. In addition, unused software licenses can be appropriately reallocated to other resources, while hardware assets can be better utilized and warranties better managed. Businesses can be more confident that their audits are in compliance with government regulations.

Keeping Workers Productive

Today's work modes, with greater use of multimedia and video conferencing, wider use of data encryption, emerging desktop-based virtual environments, and demanding applications put a significant burden on a business PC's processor. 3rd generation Intel Core vPro processors with built-in visuals and a host of other Intel® technologies keep workers productive and responsive.

Some of the performance and efficiency features of 3rd generation Intel Core i5 vPro processors include:

- Encryption/decryption up to 4x faster[14] with Intel AES-NI.
- Adaptable performance through new Intel Turbo Boost Technology 2.0, which can accelerate the processor speed when higher performance is needed.[14]
- Up to 2x faster multitasking[14] with Intel® Hyper-Threading Technology.
- Up to 60% faster on business productivity applications.[14]

Adaptive Performance with Intel® Turbo Boost Technology 2.0

Intel Turbo Boost Technology 2.0[17] manages power and thermal headroom to optimize performance. It intelligently allocates extra processing power to demanding applications. Intel Turbo Boost Technology 2.0 compares the workload to the processor specification levels, and it automatically adjusts processor cores to run faster than the base operating frequency when it's safe to do so.

Smart Multitasking with Intel® Hyper-Threading Technology

With Intel® Hyper-Threading Technology,[18] 3rd generation Intel Core vPro processors have access to extra resources to run more tasks – up to four threads with two cores and up to eight threads with four cores. For the user, this means higher productivity with seamless switching between different applications.

Stunning Visual Performance with Built-in Visuals

3rd generation Intel Core vPro processors include built-in visuals,[19] which are hardware-based technologies that improve multi-media processing, 3D imagery, and media conversion – all capabilities needed in business PCs today to support collaboration and digital content creation and consumption. These built-in visuals accelerate many media processing tasks without requiring a dedicated graphics card, as well as the cost burden and power requirements associated with additional discrete hardware.

Simplify and Speed Up Activation

The embedded technologies in business clients using 3rd generation Intel Core vPro processors deliver a system-wide solution that extends across the entire IT infrastructure to enable security, manageability, and power savings. Configuration and deployment of the solution is beyond the scope of this paper. You can find more information about configuration on the Intel Web site at www.intel.com/go/scs.

Once the PCs are deployed, activating any management and security services not already running can be done in minutes. Intel® Setup and Configuration Software 8.0 allows IT personnel to quickly configure the services, so the business and user gets the full benefits of embedded security, remote management, and performance immediately with their third-party solution. For more information on implementing management and security services, see the Intel Web site at www.intel.com/go/vpro.

The Ultimate in Visibly Smart Performance for Business

The 3rd generation Intel Core vPro processor family delivers top-of-the-line benefits in embedded security, automated and remote management, and cost effectiveness. This processor family delivers unprecedented security, "always available" access to the PC both inside and outside the corporate firewall, improved remote manageability, and remote control to resolve even the most complex issues without leaving the help desk.

Many case studies have shown how PCs with 3rd generation Intel Core vPro processors can help substantially reduce IT service costs for problem resolution and software updates (refer to the Intel Web site, www.intel.com/references/ecm/index.htm, for case studies in various industries).

The 3rd generation Intel Core vPro processor family – with unprecedented embedded security, powerful remote management, and visibly smart performance – is the ideal foundation for business clients that meet the demands of an agile business. Find out more about business clients with 3rd generation Intel Core vPro processors online at www.intel.com/go/vpro.

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

[2] No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Core™ processors and may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details.

[3] No system can provide absolute security. Requires an Intel® OS Guard enabled system with a 3rd gen Intel® Core™ vPro™ processor and an enabled operating system. Consult your system manufacturer for more information.

[4] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, see http://www.intel.com/technology/security.

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

[6] No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd or 3rd gen Intel® Core™ processor, enabled chipset, firmware, and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://ipt.intel.com.

[7] Intel® Advanced Encryption Standard – New Instructions (AES-NI) requires a computer system with an AES-NI-enabled processors, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® Core™ processors. For availability, consult your system manufacturer. For more information, visit http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni

[8] No system can provide absolute security. Requires an Intel® Secure Key enabled PC with a 3rd gen Intel® Core™ vPro™ processor and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.

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

[10] Security features enabled by Intel® Active Management Technology (AMT) require an enabled chipset, network hardware and software and a corporate network connection.   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. Setup requires configuration and may require scripting with the management console or further integration into existing security frameworks, and modifications or implementation of new business processes. For more information, visit http://www.intel.com/technology/manage/iamt.

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

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

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

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

Mobile - Comparing pre-production Intel® Core™ i5-2410M Processor (2C4T, 2.3GHz, 3MB cache), Intel Emerald Lake CRB, 4GB (2x2GB) PC3-10700 (DDR3-1333)-CL9, Hitachi* Travelstar 320GB hard-disk drive, Intel® HD Graphics 3000, Driver: 2185 (BIOS:v.34, Intel v.9.2.0.1009) , Microsoft* Windows* 7 Ultimate 64-bit RTM Intel® Core™2 Duo Processor T7250 (2M Cache, 2.00 GHz, 800 MHz FSB), Intel Silver Cascade Fab2 CRB, Micron* 4 GB (2x2GB) PC3-8500F (DDR3-1066)-400, Hitachi* 320GB hard-disk drive, Mobile Intel 4 Series Express Chipset Family w/ 8.15.10.2182 (BIOS: American Megatrends AMVACRB1.86C.0104.B00.0907270557, 9.1.2.1008).

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

Business productivity claims based on SYSmark* 2007, which is the latest version of the mainstream office productivity and Internet content creation benchmark tool used to characterize the performance of the business client. SYS-mark 2007 preview features user-driven workloads and usage models developed by application experts. Multitasking claims based on PCMark Vantage, a hardware performance benchmark for PCs running Windows 7 or Windows Vista, includes a collection of various single and multi-threaded CPU, Graphics, and HDD test sets with a focus on Windows* application tests. Security workload consists of Si Software Sandra* 2010 -AES256 CPU Cryptographic subtest measures CPU performance while executing AES (Advanced Encryption Standard) encryption and decryption algorithm. For more information go to http://www.intel.com/performance.

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

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

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

[17] Requires a system with Intel® Turbo Boost Technology capability. Intel Turbo Boost Technology 2.0 is the next generation of Turbo Boost Technology and is only available on 3rd generation Intel® Core™ processors. Consult your PC manufacturer. Performance varies depending on hardware, software and system configuration. For more information, visit http://www.intel.com/technology/turboboost.

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

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

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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

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

Printed in USA 0412/SL/OCG/XX/PDF ♻ Please Recycle 324823-002US