Executive Summary

Today’s enterprises demand a lot from their business PCs. To maintain competitive productivity and agility requires instant access and response with a wide range of methods to communicate—securely. 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 4th generation Intel® Core™ vPro™ processors are built for the needs of business and engineered to help 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 4th 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.
Business Productivity, Security, and Manageability by Design

Staying competitive means staying productive and protecting identities and corporate data from threats. To help the enterprise keep its edge, business users need to stay innovative and productive, in the office and on the move. These professionals need secure communications, instant access to data, fast response from their PCs, and advanced technologies to remove any obstructions that slow them down. For companies to stay agile, IT must support a growing fleet of consumer devices and new computing and management models, such as desktop virtualization and big data, while able to protect identities and networks and troubleshoot from afar.

Business clients based on 4th generation Intel® Core™ vPro™ processors include Intel® vPro™ Technology. These PCs integrate new embedded technologies for business users and hardware-based features that strengthen security and help IT personnel be proactive, effective, efficient, and responsive. Since the technologies are in the hardware, they are out of view and beyond the reach of today’s PC threats and stealthy malware, which penetrate security perimeters through software and the operating system (OS). Table 1 lists the Intel® technologies integrated into 4th generation Intel Core vPro processor-based platforms.

These platform enhancements enable new levels of business user productivity and protect identities and enterprise data, while helping IT departments to remotely manage their fleet of business PCs; automate troubleshooting, repair, and maintenance tasks; and reduce deskside and on-site visits. Together, they help keep identities safe, protect company data, and enable IT departments to affect their bottom lines with lower total cost of ownership (TCO) and higher operational efficiency.
# Table 1. 4th Generation Intel® Core™ vPro™ Processor Family Embedded Technologies

<table>
<thead>
<tr>
<th>Benefit Category</th>
<th>Embedded Intel® Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Productivity</td>
<td>• Intel® Pro Wireless Display</td>
</tr>
<tr>
<td></td>
<td>• Intel® vPro™ Technology with Location-Based Services</td>
</tr>
<tr>
<td></td>
<td>• Intel® VMCS Shadowing&lt;sup&gt;1,2&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® Rapid Start Technology&lt;sup&gt;3&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® Smart Connect Technology&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Enable multiple, innovative form factors</td>
</tr>
<tr>
<td>Enterprise-Class, Hardware-Assisted Security</td>
<td>• Intel® Trusted Execution Technology&lt;sup&gt;5&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® Platform Protection Technology with Boot Guard&lt;sup&gt;6&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® OS Guard&lt;sup&gt;7&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® Virtualization Technology&lt;sup&gt;2&lt;/sup&gt; and McAfee Deep Defender&lt;sup&gt;*&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• McAfee DeepSAFE Technology&lt;sup&gt;*&lt;/sup&gt;</td>
</tr>
<tr>
<td>Identity &amp; Access Protection</td>
<td>• Intel® Identity Protection Technology&lt;sup&gt;8&lt;/sup&gt; with Public Key Infrastructure (PKI) or</td>
</tr>
<tr>
<td></td>
<td>One-Time-Password (OTP)</td>
</tr>
<tr>
<td></td>
<td>• Intel Identity Protection Technology with Protected Transaction Display&lt;sup&gt;9&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• No-Password VPN&lt;sup&gt;6&lt;/sup&gt;</td>
</tr>
<tr>
<td>Data &amp; Asset Protection</td>
<td>• Intel® Advanced Encryption Standard – New Instructions&lt;sup&gt;9&lt;/sup&gt;</td>
</tr>
<tr>
<td>Security Monitoring &amp; Remediation</td>
<td>• McAfee ePolicy Orchestrator*/Deep Command*/Risk Advisor&lt;sup&gt;*&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® Platform Protection Technology with BIOS Guard&lt;sup&gt;6&lt;/sup&gt;</td>
</tr>
<tr>
<td>Manageability &amp; Automation</td>
<td>• Intel® Professional Series SSDs</td>
</tr>
<tr>
<td></td>
<td>• Intel® Setup &amp; Configuration Software</td>
</tr>
<tr>
<td></td>
<td>• Enhanced KVM Remote Control&lt;sup&gt;11&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® vPro™ Powershell Module for Windows Powershell&lt;sup&gt;*&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• Intel® Active Management Technology&lt;sup&gt;12&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

## Business Productivity

To keep ahead of the competition, enterprises need to enable professionals to stay productive and focused, and to help eliminate the tasks that deter them from their creativity and innovation. Several Intel® technologies built into Intel vPro Technology-based business clients help achieve these goals.

### Make Meetings More Productive

Mundane business meeting interruptions, such as passing the cable to a conference room projector to the next presenter, can break the flow of creative thinking and slow the speed of innovative change. The more time spent being productive in a meeting, sharing ideas and data, understanding new opportunities, and making better decisions, can help drive success.

Intel® Pro Wireless Display lets colleagues share screens without crossing wires. Intel Pro Wireless Display uses protected wireless, private networks to simplify secure connectivity with conference room projectors and wireless displays, enabling enhanced group collaboration and visualization. Collaboration, sharing, and creativity can keep progressing instead of stalling. While, secure, restricted, and private connectivity protects sensitive ideas and programs from leaks or unwanted sharing.

Additional features help improve collaboration, allow IT to manage network bandwidth, restrict connectivity to the wireless display, and remotely manage the network, plus provide customization and notifications useful during meetings.
Locate Assets Quickly
Time spent looking for a printer, lost notebook, or meeting room adds up to hours of lost business productivity and potential opportunities. Intel® vPro™ Technology with Location-Based Services in business clients enable users and IT to quickly locate a missing device within the campus, find an unused meeting room for some immediate, secure collaboration, or send jobs to the nearest printer for fast retrieval.

Enhance Virtual Environment Experiences
As virtualization continues to evolve with more environments running together, new implementations, such as virtual machine control structure (VMCS) shadowing and nested virtualization help improve this vital technology. But, it becomes even more critical to ensure separation of these environments and that user experiences are not impacted by multiple VMMs running on the same system.

Silicon-based Intel® Virtual Machine Control Structure (Intel® VMCS) Shadowing helps deliver a more secure experience when multiple computing environments are simultaneously run together. Intel VMCS Shadowing provides advanced security and compute model flexibility, by enabling greater control and separation of operating environment partitions, such as IT-managed and user-owned areas.

Get Back to Work Quickly
Waiting for a business PC to get ready for work wastes valuable time. Intel® Rapid Start Technology gets users back to work quickly, while saving power, by allowing the device to go deep asleep but resume instantly. Ultrabook™ device users will be able to work longer on battery, while other PCs, like All-in-Ones (AIOs), will help cut power usage across the enterprise.

Make Smarter Decisions Faster
Instant access to important information can help decision makers arrive at smarter resolutions more quickly. Intel® Smart Connect Technology keeps network- and Internet-sourced information accessible and up to date on the PC while busy professionals are on the move, so their data is ready when they are.

Gain Productivity from More Devices
4th generation Intel Core vPro processors support more business platforms and innovative form factors, including all-in-one PCs (AOIs), Ultrabook devices, notebooks, desktops, ultra-small platforms, and enterprise-class tablets, enabling a wide range of business clients that help keep users productive wherever they go. As enterprises continue to embrace consumerization and IT departments manage a wider variety of devices, Intel® technologies help companies stay agile and competitive without sacrificing critical IT policies.

Embedded, Hardware-Assisted 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 attacks are using stealth techniques to make it harder to detect, prevent, and remove threats.

Business PCs based on 4th generation Intel Core vPro processors offer unprecedented security with embedded technologies enabled in silicon, rather than software. These built-in, hardware-based technologies, operating below the OS, installed agents, and applications, allow greater threat mitigation, tighter identity and access protection, better data security, and effective security monitoring and remediation. Built-in functionality even allows the business client to monitor and protect itself.

Threat Mitigation
Embedded, hardware-assisted security technologies help mitigate threats from today’s sophisticated attacks on business PCs.

Keep Virtual Environments Secure
Intel® Virtualization Technology goes beyond enhancing virtual environments. This embedded technology provides the foundation for protection of virtual machines using Intel® Trusted Execution Technology (Intel® TXT) and McAfee DeepSAFE Technology.

• Intel TXT protects virtual machines against stealthy malware attacks by verifying a known safe environment for the VM as it launches.

• Intel Virtualization Technology and McAfee DeepSAFE Technology enhance and secure certain tasks in virtualized environments that further protect the PC.
Boot Securely on Windows 8*
With the launch of Windows 8*, new security features in the OS help protect the platform and users. Intel® Platform Protection Technology with Boot Guard® supports Windows 8 secure boot and helps protect against boot block level malware execution by saving critical platform characteristics outside the OS in hardware, which later provide a known good baseline for Windows bootup and attestation.

Prevent Privilege Escalation Attacks
Some sophisticated malware has been known to take advantage of OS conditions that allow code to escalate execution in restricted system areas, below the OS and security agents. Intel® OS Guard® keeps malware from rooting below the OS by helping ensure against escalation of privilege attacks.

Enable Protection Beyond the OS
Malware often uses rootkits and other devices to thwart system-level antimalware software and security agents. These threats then propagate their code or attack specific areas by remaining hidden below the OS. McAfee DeepSAFE Technology co-developed with Intel detects, blocks, and remediates advanced, hidden attacks from bootup through user operation.

Identity and Access Protection
Intel security technology hardware helps keep identities and sensitive data safe.

Keep Identities Safe
Today’s sophisticated identity threats attack software-based identity protection, such as passwords, certificate keys, and software tokens, through the OS. Intel® Identity Protection Technology® (Intel® IPT) uses hardware-assistance that is out of sight and reach of malware and the OS to help secure critical data and operations, such as key generation and user data entry, while supporting familiar applications, like VPN clients. Intel IPT offers the security of hardware with the convenience and response of software. Several Intel IPT implementations support different types of secure uses:

- Intel IPT with One Time Password (Intel IPT with OTP) enables hardware-protected secure one-time password tokens.
- Intel IPT with Protected Transaction Display (Intel IPT with PTD) uses hardware-based authentication to protect against screen scrapers and key loggers, and it improves security by verifying user presence with secure input.

- Intel IPT with Public Key Infrastructure support (Intel IPT with PKI) relies on hardware-assistance to create and process private keys, plus it encrypts certificate data with a Platform Binding Key, which binds the certificate to the platform.

Intel IPT helps protect user identities, keep logins safe, and ensure against automated entries by robots and other non-human agents.

Simplify No-Compromise, Secure Access to Enterprise Data
Intel IPT with PKI can eliminate the need for dedicated VPN client passwords, keeping end-users productive and reducing Help Desk password resets requests, while providing enterprise-class security. No-Password VPN® is an effective and secure use case for two-factor authentication based on a login password to the device and PKI certificates authenticated with Intel IPT with PKI. No-Password VPN simplifies the user experience, while maintaining strong two-factor authentication for corporate networks.

Data Protection
The objective of enterprise security is to protect sensitive data wherever it resides, whether in transit or at rest. Intel embedded technologies deliver solid data protection without slowing user productivity.

Enable Encryption Everywhere
Data is better protected when it is encrypted. But, traditionally, real-time encryption came at a high performance cost and productivity tax for the user. With Intel® Advanced Encryption Standard – New Instructions® built into the processor, encryption and decryption runs very fast, eliminating the performance penalty to users and enabling ubiquitous encryption across business clients based on 4th generation Intel Core vPro processors.

Encrypt with Confidence
When random numbers are needed for encryption, the results can be safer with high-quality random numbers generated out of sight and out of reach of malware. Intel® Secure Key® generates random numbers in discrete silicon using true random number instructions. During generation, nothing is exposed, keeping the process out of reach of any malware that might affect number-generation instructions.
Security Monitoring and Remediation
For fast response to detected threats, business clients based on 4th generation Intel Core vPro processors enable automatic monitoring and remediation using McAfee enterprise security applications. IT can take advantage of built-in capabilities and McAfee software to rapidly detect and address a threat remotely.

- 4th generation Intel Core vPro processor-based platforms combined with McAfee ePolicy Orchestrator*, McAfee Deep Command*, and McAfee Risk Advisor* enable IT to reduce the cost of operations and allow comprehensive management of enterprise networks and endpoint security.
- Intel® Platform Protection Technology with BIOS Guard protects business clients against BIOS corruption from sophisticated malware by preventing changes without proper signing and authorization.

Manageability and Automation
With PCs based on 4th generation Intel Core vPro processors, IT can connect to management functions outside the PC’s OS over the corporate wired or wireless network, and, in most cases, even if the PC is outside the firewall or turned off.112 These business clients can even self-initiate communication with the IT console for management and maintenance purposes, when a threat is detected, or under other conditions specified by IT management. Thus, manageability features are always available, allowing IT to work fast and efficiently. Built-in automation and management capabilities include:

- Remote configuration, maintenance, and recovery of Intel® Professional Series SSDs.
- Fast, remote setup and configuration of new business clients with Intel® Setup and Configuration Software (Intel® SCS).
- Keyboard, video, and mouse (KVM) control of remote PCs with Enhanced KVM Remote Control.
- Custom automation scripting support with Intel® vPro™ Powershell Module for Microsoft Windows Powershell*.
- Remote diagnosis, isolation of problems, and repair using Intel® Active Management Technology (Intel® AMT).

With these capabilities, in addition to positive impacts on IT efficiencies and TCO, PCs stay healthier and businesses can minimize user downtime, while improving both employee and IT productivity.

SSD Storage Performance and Manageability
Besides being incredibly fast and reliable enterprise-class storage devices, Intel Professional Series SSDs provide full-time disk encryption, so data is always protected at rest. IT can easily configure new drives remotely with Intel Setup and Configuration Software, and personnel can unlock them using Intel® Remote Encryption Management to access important drive data through Intel vPro Technology built into the platform. Users get enhanced productivity from SSD performance, enterprises benefit from fully encrypted data, and IT remains efficient managing the devices from afar.

Simplify and Speed Up Activation
Once the PCs are deployed, activating any management and security services not already running can be done in minutes. The latest version of Intel Setup and Configuration Software allows IT personnel to quickly configure the services, so the business and user get full, immediate benefits of embedded security, remote management, and performance. You can find more information about configuration on the Intel web site at www.intel.com/go/scs.

The embedded technologies in business clients using 4th 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. For more information on implementing management and security services, see the Intel web site at www.intel.com/go/vpro.

Get Behind the Keyboard with Enhanced KVM Remote Control
In spite of improved management tools, some problem tickets still require that users help resolve the problem. 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 desk side visits or ask users to help resolve the problem. Hardware-based Enhanced KVM Remote Control can help reduce problem resolution time for complex software issues by allowing a technician to “get behind the user’s keyboard” without leaving the help desk.

Unlike software-based Windows remote desktop, hardware-based Enhanced 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.
Enhanced KVM Remote Control in PCs based on 4th generation Intel Core vPro processors is available in 27 languages and supports up to three monitors (up to 2560 x 1600 with 16-bit color) in portrait and landscape modes.

**Customize Automation**

Sometimes IT needs to customize automation beyond the standard functions of management consoles. Using Windows Powershell* and the Intel® vPro™ Powershell Module for Intel vPro Technology-based platforms, IT personnel can directly access management features to create unique functionality they require to be more efficient and effective.

**Resolve Problems Remotely**

Deskside and service-center calls can take up a large portion of an IT budget. Intel vPro Technology enables IT personnel to easily configure, diagnose, isolate, and repair PCs remotely, even if systems are unresponsive. Using Intel Active Management Technology features, such as remote/redirected boot, 4th generation Intel Core vPro processors can help IT managers reduce deskside visits and achieve the following:

- Get users back to work fast with remote configuration, diagnosis, isolation, and repair of PCs, even if systems are unresponsive and outside the corporate firewall.
- Reduce energy usage by automatically shutting down PCs during off-hours.
- Automatically power up PCs to get them ready for arriving workers.
- Easily re-direct, reboot, and re-image PCs from anywhere.
- Reduce costs by automatically inventorying hardware and software.
- Keep systems compliant by automatically waking up clients and updating software and agents, even after normal business hours and when the PC is turned off.
- Automatically upgrade applications or OS.

**Ready for Windows 8***

4th generation Intel Core vPro processors deliver performance to enable a powerful enterprise running on current and next-generation productivity platforms, including Office* 2010/2013, IE9*, and other Windows 8 applications. Now, companies can meet all their consumerization needs, from enterprise-class tablets to powerful laptops and desktops, with hardware-enhanced technologies all built on Windows 8 and 4th generation Intel Core vPro processors.

**The Ultimate in Enterprise Security and Productivity for Business**

The 4th generation Intel Core vPro processor family delivers top-of-the line benefits for business productivity, hardware-assisted security, and remote and automated manageability. This processor family enables unprecedented identity and data protection, “always available” access to the PC both inside and outside the corporate firewall, improved remote access, and remote control to resolve even the most complex issues without leaving the help desk. Many case studies have shown how PCs with 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 4th generation Intel Core vPro processor family is the ideal foundation for business clients that need to meet the demands of an agile business. Find out more about business clients with 4th generation Intel Core vPro processors online at www.intel.com/go/vpro.
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.

No system can provide absolute security. Requires an Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, and an Intel TXT-compliant measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.2. For more information, see http://www.intel.com/technology/security.

No no system can provide absolute security under all conditions. No system can provide absolute security under all conditions. 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.

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, and an Intel TXT-compliant measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.2. For more information, see http://www.intel.com/technology/security.

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

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.

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

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

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/manageramt.

Intel® Rapid Start Technology transitions a system that is in Sleep or Standby, an S3 power state that keeps memory and other components powered, to a hardware power state that does not do so, an S4 power state. Refer to manufacturer’s specifications for system specific information.

Trusted Execution Technology (Intel® TXT) requires the system to contain a TPM v1.2. For more information, see http://www.intel.com/technology/security.

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.

Rapid Start Technology requires a select Intel® processor, Intel® software and BIOS update, and Intel® Solid-State Drive (Intel® SSD). Depending on system configuration, your results may vary. Contact your system manufacturer for more information.

Requires a 3rd or 4th generation Intel® Core™ processor, Intel® software and OEM-enabled BIOS, Intel® Wireless adaptor, and Internet connectivity. Solid-state drive (SSD) or equivalent may be required. Depending on system configuration, your results may vary. Contact your system manufacturer for more information.

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, and an Intel TXT-compliant measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.2. For more information, see http://www.intel.com/technology/security.

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

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.

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

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

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/manageramt.

Intel® Rapid Start Technology transitions a system that is in Sleep or Standby, an S3 power state that keeps memory and other components powered, to a hardware power state that does not do so, an S4 power state. Refer to manufacturer’s specifications for system specific information.