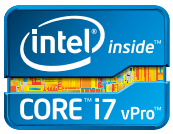
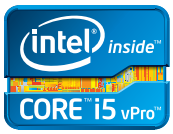
Crimeware Protection: 3rd Generation Intel® Core™ vPro™ Processors

White Paper

3rd Generation Intel® Core™ vPro™ Processor Family





Executive Summary

Today's sophisticated cyber-criminals are finding new ways to plant their crimeware into business clients. Their stealthy viruses and codes are digging in out of sight and out of reach of virus detection and the operating system (OS). The result is the most insidious and sophisticated malware that security experts have seen to date – and IT management must protect against.

3rd generation Intel® Core™ vPro™ processors address these new challenges with built-in security technologies[1] that work below and beyond the OS – in the hardware and firmware. These new technologies from Intel enable greater threat management, better detect and thwart identity theft, provide deeper and safer encryption, protect against data and device theft, and, in the event of a breach, help reduce the cost of remediation.

Built-in security technologies in 3rd generation Intel Core vPro processors deliver and protect business clients where current technologies cannot reach. This paper surveys these embedded technologies from Intel and how they can help IT's toughest security challenges.

Table of Contents

Managing the New Threats in IT

IT's Evolving Security Challenges

Unlike yesteryear's amateur virus-producing hackers, who created widespread threats, today's cyber-criminals instigate much more specific attacks. Their products are much more insidious, harder to detect, and more difficult to remediate, with specific targets and results in mind, such as corporate espionage, undermining operations, exposing secret data, hactivism, and more.

Criminals are using stealth techniques to deliver their crimeware, allowing it to find targets and dig in below the operating system (OS). The codes lie in wait out of sight and out of reach of the OS until the opportune time to attack, reproduce themselves in ways to make it harder to detect and remove them, steal identities, or more.

The malware pathology of Stuxnet and the toolkit provided by Zeus illustrate just how sophisticated these criminals are and how easy it is to create hidden, costly bugs. These are the types of new threats to IT security. And, according to security experts at McAfee, enterprises can expect these types of attacks to happen more often.[2]

The Complications of Evolving Business

Modern threats take advantage of every interaction your users have with your data, devices, and applications; evolving business operating models expand their opportunities.

New service deliveries, including virtual desktops and cloud-based services, add to the challenges of ensuring an infrastructure is protected against sophisticated threats. Each of the communications channels – web-based applications, identity and access to enterprise networks and confidential accounts, and e-mail – present vectors through which threats from data loss, identity theft, and invasion are possible.

Complicating security issues further is the expanding range of mobile devices that must be corralled within a secure perimeter. Besides the ubiquitous laptop, more mobile devices are mainstream, including smartphones and tablets, offering more vectors for crimeware to invade. IT has to protect them all. Not just from malware attacks, but also mitigating and remedying plain old "grab and run" theft.

Protective Strategies

Protecting against attacks requires a solid strategy across all fronts against which they might come. These include the following:

Threat Management – Not just identifying and stopping detectable insidious codes using virus detection and removal software, but protecting the vulnerabilities where they are finding entrances, especially below and beyond the operating systems.

Identity and Access – Ensuring users are who they say and not a malware imposter using a stolen identity.

Data Loss Prevention – Protecting against the damages from data and device theft and providing the highest level of encryption to prevent breaking through today's strong encryption methods.

Monitoring, Reporting, and Remediation – Preventing and mitigating threats through knowing and plugging vulnerabilities before the malware finds them, and reducing the costs and challenges of preventing and recovering from an attack.

Security Below and Beyond the OS

The reality of today's crimeware is that very smart software is able to find vulnerabilities and invade where it's hard for virus detection tools to reach and remove them. To outsmart these codes requires hardware-based solutions that complement – and even assist – sophisticated virus detection and security software that work below and beyond the OS, detecting and stopping threats as they try to take advantage of a vulnerability (Figure 1).

Business Clients with Built-in Security

Business clients based on 3rd generation Intel Core vPro processors integrate built-in security technologies in the processor silicon, the platform hardware, and the firmware – below the operating system. Intel® technologies work along the fronts of threat management, identity and access, data loss prevention, and monitoring, reporting, and remediation. Intel technologies and built-in tools detect software-based threats, bypass and prevent identity theft before it happens, strengthen strong encryption, and thwart the costs of physical theft – even helping recover lost laptops.

With these technologies, business clients help IT management prevent the attacks from today's sophisticated, stealthy crimeware, while reducing the costs of prevention and remediation.

How is this possible? What are the Intel technologies that help IT ward off today's sophisticated threats?

Figure 1. Intel® Security Pillars: Holistic approach to protecting your enterprise.

Threat Management

The Root-kit of All Evil and Other Malware

Today's sophisticated criminals use root-kits, knowledge of zero-day vulnerabilities, and injection of viruses into application memory to hide their malicious code out of sight and reach of anti-virus software. Undetected, it can be executed by the OS, embedded in a virtual environment, or unknowingly called during normal application processes.

Intel® threat management technologies guard against such attacks, with the following capabilities embedded in the silicon:

- Protection against malware using escalation of privilege attacks.
- Providing a secure root of trust for virtual environments.
- Monitoring memory against malware invasions.
- Device isolation for protection against direct memory access (DMA) attacks.

Protection Below the OS

Intel® Execute Disable Bit, implemented many Intel® processor generations ago, has helped protect thousands of business clients from buffer overflow attacks, by preventing malicious code executions from data memory. However, threats are inserting themselves in application memory space and executing under a privilege level assumed for the application.

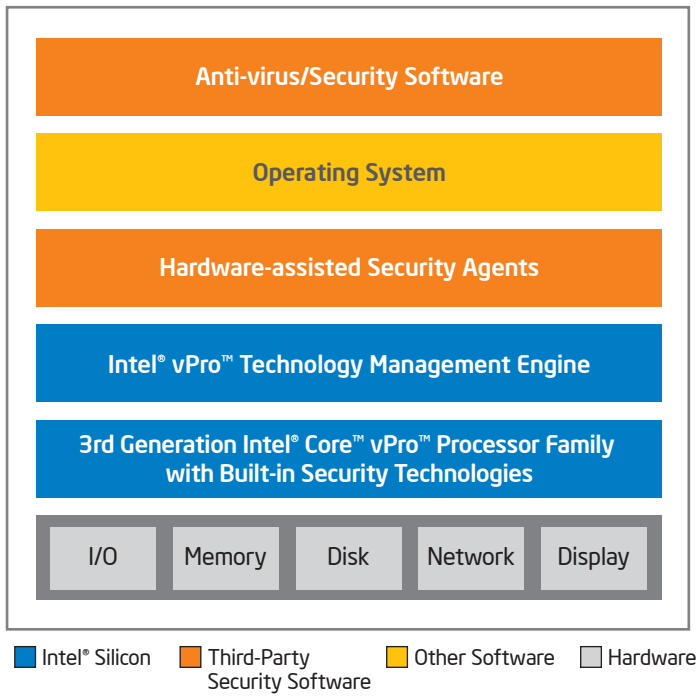


Figure 2. Intel built-in, hardware-level security.

Intel® OS Guard,[3] the next generation of Intel Execute Disable Bit, protects against such escalation of privilege attacks, by preventing malicious code from executing out of application memory space, in addition to data memory. This protection below the OS guards against more sophisticated viruses and the damage they can do.

Protecting Virtual Realms

New service delivery models, such as cloud-based computing and virtual desktops, introduce new challenges for IT personnel. Undetected code that manages to inject itself into a virtual machine (VM) as it is launched, compromises an entire environment for the users attaching to it, whether it is a single-use virtual desktop or an entire service. Intel® embedded security technologies, including new applications for Intel® Virtualization Technology[4] (Intel® VT), help protect physical and virtual environments, both at the service delivery level and for single virtualized clients.

Intel® Trusted Execution Technology[5] (Intel® TXT) establishes a hardware-based root of trust for VMs being launched on a host. Intel TXT measures a known-good hosting environment and stores its conditions and states as a trusted baseline. Whenever the host system boots, Intel TXT validates the behaviors of key components against the known-good measurements, and will boot VMs only if the environment is trusted. Once launched, Intel TXT isolates assigned memory partitions from other software in the system, keeping out potential attacks from the host or other VM environments. When an application or the VM shuts down, Intel TXT closes software without exposing its data to other applications or environments by wiping the memory space clean. Since Intel TXT is based on hardware-enabled technology, it protects virtual and physical environments from malware and rootkits attempting to corrupt the client software.

Intel Virtualization Technology has been a trusted resource for several generations of Intel processors, enhancing virtual environment robustness and performance. Intel VT also provides specific security protection from two aspects of Intel VT: Intel VT-x and Intel VT-d.

- **Intel VT-x** isolates each VM execution environment and monitors memory, so malware existing in or attempting to invade one VM environment cannot affect another VM on the same host.
- **Intel VT-d** isolates virtual devices, their memory spaces, and virtual addresses. Attacks using DMA accesses are thwarted, because the threat does not have direct access to the device's memory.

Identity and Access

Who's Whom?

Enterprises have seen a growing number of targeted attacks through identity breaches. To mitigate these, they use secure credentials requiring authentication to access them. Software-only credentials are stored in view of the OS and applications, where they are vulnerable to theft and corruption by sophisticated, stealthy crimeware. Many organizations have deployed hardware tokens, smartcards, or USB keys to reduce this risk. But provisioning, management and support of these solutions can be costly.

Intel® Identity Protection Technology[6] (Intel® IPT) is a suite of products offering built-in hardware-level security to protect against identity theft, without the need for discreet tokens or smartcards. Intel Identity Protection technology offers the security of discreet tokens with the ease of maintenance and fast response capabilities to security breaches provided by software-based solutions.

Intel® Identity Protection Technology

Security experts agree – single-factor authentication, such as a fixed password, is not enough. Many enterprises have chosen to protect access points, such as VPN logins and web portals, or secure e-mail and document encryption, with strong, two-factor authentication. The two most common forms are one-time-password (OTP) tokens and public key infrastructure (PKI) certificates, often deployed on discreet tokens or smartcards, respectively.

This hardware-based identity protection helps significantly reduce or eliminate fraud and limits access to protected networks and accounts to only valid users. However, enterprise experiences and recent events have highlighted the challenges with these[7]:

- Lost or forgotten credentials overburden help desk departments.
- Tokens, smartcards, and additional management software can be costly.
- Recent breaches on token stores have highlighted the cost of replacing physical tokens and the lost productivity while users wait for replacement tokens. And, while smartcards are not as difficult to replace, they are still vulnerable to attacks.

To reduce costs associated with hardware security maintenance, some solutions store tokens and PKI certificates on the PC. They can be easily revoked and re-provisioned when needed. However, software-based solutions are typically stored in view of the OS and applications, where they face increased risks from targeted attacks.

Hardware-based Security with Software-based Convenience

Intel IPT stores OTP tokens and PKI certificates in the silicon, out of view and access of the OS and applications. Yet Intel IPT still enables easy revocation, re-provisioning, and management. The issues with lost hardware devices are eliminated. Keys are released only when appropriate authentication is provided, such as a password or PIN.

Intel IPT combines the security of hardware-based solutions with the flexibility and cost savings of software by providing the following capabilities:

- Protects PKI certificates or OTP credentials in silicon out of reach of malware, below the software and operating system.
- Prevents access to keys without proper authentication only an actual user could enter.
- Hides the user's data entry from the OS and applications, such as key loggers and screen scrapers.

Protection for User Input

As seen in some recent attacks, authentication passwords and PINs can be captured by a key logger to access sensitive data. Intel IPT with Protected Transaction Display helps eliminate identity theft through key logging and screen scraping by capturing and displaying user input out of sight of the OS and device drivers. Key logger and frame buffer reader codes are blinded to the user's activity.

Easily Deploy Intel IPT with OTP

Many enterprises have chosen one of the popular authentication providers to implement their OTP solutions. Intel IPT with OTP is supported by many of these leading vendors. Using Intel IPT with OTP requires only minimal changes to current implementations, while providing hardware-based security with software-based convenience. As enterprises migrate their fleet of business clients to PCs based on 3rd generation Intel Core vPro processors, they can use the same authentication provider to provision hardware-based OTP credentials to these machines and phase out their physical tokens.

Quickly Migrate to Intel IPT with PKI

For enterprises that implement PKI certificate-based solutions, Intel IPT with PKI simplifies certificate management while providing hardware-based security. Intel IPT with PKI is compatible with Symantec Managed PKI Solution.* It needs only minimal changes to an enterprise's current implementation. As companies replace their PCs with 3rd generation Intel Core vPro processors-based clients, they can provision hardware-based PKI certificates to these machines using the same authentication provider and phase out physical smartcards.

Data Loss Prevention

How Safe is Safe?

Business data resides in many forms and places today, and often travels outside the corporate physical boundaries: contact lists and communications on smart phones, marketing and business plans on laptops, intellectual property and designs on servers, etc. And it is accessed locally and remotely from a variety of devices through secured tunnels on public networks and over private networks. Protecting the devices as they travel and the data throughout transit and storage from threats is no small IT challenge.

Intel embedded security technologies address data loss prevention – both the data and the devices on which the data might reside with the following capabilities:

- Accelerated encryption/decryption technology.
- Secure, high-performance, pure random number generation technology for seeding the encryption algorithms.
- Physical device security technology.

Enabling Ubiquitous Encryption

Encrypted data is the safest data. Without solid encryption, thieves can easily access an enterprise's single-most important asset – its collective knowledge. Encryption allows an organization to secure its confidential information using complete disk or selective file/folder encryption. Traditionally, however, on-the-fly encryption and decryption would tax the client's performance, impacting employee productivity. Thus, enterprises have been reluctant to deploy encryption company-wide.

Algorithms of the Advanced Encryption Standard are widely used in encryption/decryption processes in operating systems and security software. Intel® Advanced Encryption Standard – New Instructions[8] (Intel® AES-NI) includes seven new processor instructions that accelerate encryption and decryption up to four times faster in applications optimized for Intel AES-NI, such as McAfee Endpoint Encryption.* When an optimized encryption product is employed, users avoid a "productivity/performance tax" with Intel AES-NI, enabling enterprises to employ ubiquitous encryption throughout the enterprise across business clients based on 3rd generation Intel Core vPro processors.

Now, it's possible to simultaneously make data safer, while keeping employees productive.

True Random Numbers

Secure, protected encryption starts with a random number seed, typically provided by a pseudo-random number generator within the client. Higher quality numbers are less predictable and provide better security. And the more protected the number is during generation, the safer is the encryption. Numbers stored in memory during generation are eventually at risk by sophisticated malware.

Intel® Secure Key[9] provides a clean source of random numbers through generation in hardware, out of sight of malware. The autonomous, self-contained digital random number generator resides on the processor package, making it chipset-independent.

Intel Secure Key is:

- Standards-compliant (NIST SP 800-90) and NIST FIPS 140-2 Level 2 certified.
- Easily accessible to all applications and at any privilege level using a new processor instruction.
- A closed system – the state of the system is never seen, never placed in memory, and never "stored anywhere."

Any software application can benefit from Intel Secure Key, including the following:

- Security ISVs that issue certificates
- Secure web browsers with SSL security links
- Data encryption providers
- Operating systems

Intel Secure Key deepens encryption protection without a performance tax.

Lost, but Not Forgotten

Data on laptops is often some of the most critical and most difficult to protect, even with the toughest mobile usage IT policies. Criminals involved in industrial espionage and trade secret theft understand the vulnerability mobile devices present.

Every day, hundreds of laptops go missing from airports around the world – many with highly sensitive data on them. Intel® Anti-Theft Technology[10] (Intel® AT), embedded in 3rd generation Intel Core vPro processors, self-protects the data and laptop on which it resides if it goes missing. It can even enable the missing client to report its own location. And, Intel AT enables IT to remotely restore a laptop when the system is found and returned.

With Intel AT enabled on a business client, IT security management can define a threat to the device. A threat can be an incorrect login identity entered by a thief, a "fake" login identity entered by a user under duress, or prevention of the device connecting to a corporate network to periodically "check in." The threat triggers the IT management system to send a "poison pill" to it, locking it down.

With Intel AT, locking down the system includes the following, making the device and data useless:

- Essentially scrambles any security keys embedded in the device so they cannot be used in identity theft; however, the keys can be restored by IT.
- Prevents disk drive access and data decryption, even if it is installed into another device, preventing access to the data on it.
- Disables access to any platform functions once powered on, even if a new drive is installed in the client.
- If the device includes 3G network connectivity, it can send its own GPS location to the IT department.

If the system is eventually recovered, it can be restored to working condition – even remotely by IT – simply by the user contacting the IT staff and providing appropriate authentication. Technicians can restore the identity keys and unlock the system, placing it back in service in minutes rather than hours or days.

Intel hardware-based, built-in security technologies protect data and laptops on the go.

Monitoring, Reporting, and Remediation with Intel® vPro™ Technology

Detecting a threat, notifying the IT management system of it, and restoring data and user productivity can be a time-consuming and costly process. The longer the time passed, the greater the potential cost of the threat.

Intel embedded security technologies and Intel® Active Management[11] Technology (Intel® AMT) help maximize IT's awareness, control, and response, while minimizing the costs of remediation and management. These technologies are part of business clients based on the 3rd generation Intel Core vPro processor family, enabling the following capabilities:

- On laptops, automated threat detection and lockdown – sometimes even before the user realizes it – threat reporting, and remote remediation when the device is recovered.
- Remote inventorying of hardware and software to ensure all security software and databases are up-to-date.
- Automated downloads to the client and updates of critical software, even during off-hours, whether or not the system is powered on.[12]
- Automated detection of critical, running security agents and notification when discovered missing or not active.
- Automatic network traffic filtering and disconnection in response to a threat.
- Remote access to business clients, with complete control over the system as if the technician was sitting in front of it.

Monitoring and Prevention

Every business client based on a 3rd generation Intel Core vPro processor maintains a high level of its situational awareness with constant health monitoring, hardware and software inventories, and appropriate responses to any detected irregularities.

Prevention is Better than Remediation

Detecting and *avoiding* potential risk is easier and less costly than remediating an *actual* one. That's why business clients with 3rd generation Intel Core vPro processors take periodic inventories of hardware and software, monitor their own health, and report irregularities.

These business clients keep records in non-volatile memory of all monitored activities and conditions, where IT personnel – or the automated console – can retrieve the information. Software inventories can be checked for currency and risk, and automatic updates scheduled accordingly – either immediately for high risk or during off-hours for lower risk applications. Known at-risk firmware can be remotely updated, and hardware can be flagged for upgrades or replacement as necessary. Prevention keeps costs down, and knowledge of every PC's assets empowers IT to make efficient, informed, and intelligent decisions about how to manage its fleet of business clients.

Constantly Vigilant – Automatic Monitoring and Reporting of Critical Agent Presence

Some IT central management systems poll remote clients over the network for the presence of running, critical security agents, like anti-virus and encryption software. Typically, the agents are present and active, meaning no threat is detected, but the request uses valuable network bandwidth for a positive report. And critical monitoring is interrupted if a network connection is unavailable, as with a laptop on the move.

Business clients with Intel AMT contain self-polling agents embedded in the system; these agents monitor and record the presence of critical software. The results of all polls are stored on the system in non-volatile memory for remote access at any time by IT.

If the necessary software does not report correctly, Intel AMT can contact the management console to notify IT and respond according to IT policies. By self-monitoring instead of responding to network polls, the client is continuously protected, regardless of network access, and does not take up bandwidth when the system is operating normally. Automated monitoring without direct IT intervention results in better protection at lower cost.

Containing Contagions – Automatic Network Monitoring and Response

Business clients based on 3rd generation Intel Core vPro processors protect themselves against many types of intrusion vectors, including monitoring network traffic. This level of monitoring and protection is handled in the hardware, by the network adapter, not running software, which can be potentially corrupted.

IT can define network filters that trigger a security response to protect both the client and the corporate assets on the network. Network threat detection includes the following methods:

- **The type of traffic** coming through the network adapter to protect against threats embedded in data.
- **The rate of the activity** (in desktop clients) to protect against distributed denial of service (DDoS) attacks.

When the system detects a threat, it immediately responds by isolating itself from the network to prevent the spreading of a contagion, or further participating in a DDoS attack. Network disconnection is handled by the network adapter, not the operating system's network stack, to ensure the isolation is secured in hardware, beyond the reach of potentially invading stealthy crimeware.

The out-of-band remediation channel remains open for IT to remotely manage the system and restore it to service.

Staying Put – Minimizing Costs through Remote Remediation

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. When a visit is the result of an active threat, costs have already accumulated. Remote remediation minimizes the costs related to visits, and helps quickly return an employee back to productivity.

Intel AMT with KVM Remote Control[13] put IT personnel in the driver's seat – literally – with full remote control of a business client to enable the following capabilities:

- **Remote/redirected boot –** reboot to a clean state or redirect the boot device to a clean local or remote image, a diagnostics or remediation server, or other device.
- **Serial-Over-LAN (SOL) console redirection** to control the keyboard outside of the OS to perform tasks, such as editing BIOS settings from the service center—without user participation.
- **Access 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.
- **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** from non-volatile memory 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 or upgrade the OS** or fully reimage the hard drive remotely.

Hardware-based technologies help automate and simplify protection and remediation, thus reducing costs.

Conclusion

While today's cyber-criminals use new stealthy techniques for targeted attacks on companies and organizations, business clients based on 3rd generation Intel Core vPro processors help thwart these threats with built-in, hardware-based security technologies. These Intel technologies work below the OS and provide hardware assistance to advanced security agents beyond the OS.

- Intel OS Guard, Intel TXT, and Intel VT help IT manage threats by preventing malware from invading below the OS.
- Intel IPT with PKI, Intel IPT with OPT, and Intel IPT with Protected Transaction Display help prevent identity theft using hardware-based security with software-based convenience and remediation response.
- Intel AES-NI and Intel Secure Key enable safer, faster encryption.
- Intel AT protects laptops and their data on the go.
- Intel® vPro Technology[14] helps reduce the effort and cost of threat prevention and remediation.

All these built-in technologies, available only in systems based on 3rd generation Intel Core vPro processors, help keep companies and their data safer by protecting data and networks against today's advanced persistent threats and targeted attacks. For more information, see www.intel.com/vpro.

[1] 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.

[2] "2012 Threats Predictions" Report by McAfee Labs; http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf

[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] 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 configu¬rations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

[5] 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.

[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] "Chinese hackers target smart cards to grab US defense data;" by Techspot. http://www.techspot.com/news/47053-chinese-hackers-target-smart-cards-to-grab-us-defense-data.html

[8] 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

[9] 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.

[10] 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.

[11] 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.

[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] 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.

[14] 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/.

Printed in USA 0412/SL/OCG/XX/PDF Please Recycle 327161-001US