Executive Summary

Business clients built on Intel® processors offer strengthened security with increased productivity for business users. The embedded security technologies in these processors work beyond the OS—in the hardware and firmware—to protect users and the enterprise from new stealthy attacks that are hard to detect with conventional software solutions. Working in the hardware and firmware, they enhance user productivity, 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.

These built-in security technologies help secure 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.
White Paper: Enterprise-Class Protection with Intel® Processors for Business Clients

Table of Contents

Executive Summary ...................................................... 1
Balancing Security, Productivity, and Manageability in the Enterprise .................. 3
Secure Business Productivity ........................................... 3
Enhance Virtual Environment Experiences ................................ 3
Get Back to Work Quickly ............................................ 3
Make Smarter Decisions Faster ........................................ 3
Gain Productivity from More Secure Devices .................................. 3
Embedded, Hardware-Assisted Security ........................................ 4
IT’s Evolving Security Challenges ....................................... 4
Protective Strategies – Security Below and Beyond the OS ......................... 4
Business Clients with Built-in Security ...................................... 4
Threat Mitigation .......................................................... 5
The Root-Kit of All Evil and Other Malware .................................... 5
Protecting Virtual Realms .................................................. 5
Booting Securely .................................................................. 5
Keeping Code in Its Place .................................................. 5
Enabling Protection Beyond the OS ......................................... 5
Identity and Access Protection ............................................. 6
Who’s Whom? ............................................................ 6
Intel® Identity Protection Technology ......................................... 6
Hardware-Based Security with Software-Based Convenience ....................... 6
Protection for User Input ................................................... 6
Easily Deploy Intel IPT with OTP .......................................... 6
Quickly Migrate to Intel IPT with PKI ....................................... 6
Data Protection ............................................................. 7
Lost, but Not Forgotten ..................................................... 7
Enabling Ubiquitous Encryption ............................................. 7
True Random Numbers ..................................................... 7
Security Monitoring and Remediation with Intel® vPro™ Technology .............. 8
System-Wide Monitoring ..................................................... 8
Monitoring and Prevention .................................................. 8
Manageability and Automation .............................................. 9
Simplify and Speed Up Activation .......................................... 9
Staying Put – Minimizing Costs through Enhanced Remote Control .............. 9
Conclusion ................................................................. 10
Balancing Security, Productivity, and Manageability in the Enterprise

Modern threats take advantage of every interaction your users have with your data, devices, and applications. New service deliveries, including virtual desktops and cloud-based services implemented to improve productivity, 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 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. IT has to protect and manage them all—protect not just from malware attacks, but also mitigate and remedy plain old “grab and run” theft.

To help IT accomplish their objectives, Intel® embedded technologies along with McAfee software and technologies work in the hardware and beyond the OS to help enable greater productivity, security, and manageability.

Secure Business Productivity

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 and security 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) Shadowing helps deliver a more responsive and secure experience on virtualized desktops. 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™ 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 secure yet 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 Secure Devices
4th generation Intel® Core™ vPro™ processors support more business platforms and innovative form factors, including all-in-one PCs (AIOs), Ultrabooks, 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

IT’s Evolving Security Challenges

Unlike yesteryear’s threats, today’s attacks bury themselves deeply in the system. These threats use stealth techniques, allowing them to dig in below the operating system (OS), making them harder to detect and more difficult to remediate.

The codes lie in wait, out of sight and out of reach of software agents and the OS, until the opportune time to attack and reproduce themselves in ways that make it harder to find. They often target specific activities, such as corporate espionage, undermining operations, exposing secret data, activism, financial theft, and more.

The malware pathology of Stuxnet and the toolkit provided by Zeus illustrate just how sophisticated these threats have become, 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.

Protective Strategies – Security Below and Beyond the OS

The reality of today’s threats 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).

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

- **Threat Mitigation** – 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 Protection** – Ensuring users are who they say and not a malware imposter using a stolen identity.
- **Data Protection** – Protecting against the damages from data and device theft and providing the highest level of encryption.
- **Monitoring 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.

**Business Clients with Built-In Security**

Business PCs based on Intel processors for business clients integrate built-in security technologies in the processor silicon, the platform hardware, and the firmware—below the operating system (Figure 2). Intel technologies, McAfee software*, and built-in tools help 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. Yet, while providing a high level of security, Intel technologies also keep from becoming complicated processes that hinder user productivity. They provide security with simplicity.

---

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

**Figure 2.** Intel built-in, hardware-level security.
Threat Mitigation

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 mitigation technologies guard against such attacks, with the following capabilities embedded in the silicon:

• Providing a secure root of trust for virtual environments.
• Enabling security from the start with Windows 8* secure boot support.
• Protection against malware that use escalation of privilege attacks.
• Working below the OS with technologies and strategies to help protect against malware invasions using McAfee DeepSAFE* Technology.

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® (Intel® VT), help protect physical and virtual environments, both at the service delivery level and for single virtualized clients.

Intel® Trusted Execution Technology® (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.

Booting Securely

Windows 8 adds a new level of protection from boot to OS initialization, and Intel processors for business clients support booting securely across a wide range of platforms with multiple technologies.

• Business clients based on 4th generation Intel® Core™ vPro processors implement a Trusted Platform Module* (TPM), which supports Windows 8 secure boot.
• Business clients based on Intel® Atom™ processors include Intel® Platform Trust Technology (Intel® PTT), which provides a firmware based trust technology for Windows 8 secure boot and always on, always connected (AOAC) services.
• Business clients based on 4th generation Intel® Core™ processors without UEFI can use Intel® Platform Protection Technology with Boot Guard*, a secure boot technology for below the OS protection.

Keeping Code in Its Place

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.

Intel® OS Guard*, 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.

Enabling Protection Beyond the OS

Malware often uses root-kits and other devices to thwart system-level protective 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 mitigates advanced, hidden attacks from bootup through user operation.
Identity and Access Protection

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 malware. 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® (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 past events have highlighted the challenges with these:

• 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 certificate keys 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 certificate keys 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

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 4th 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 4th 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 Protection

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 (Intel® AT), embedded in 4th 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 or to disable itself without a network connection.

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, including on self-encrypting disk drives, even if the drive is installed into another device.
- 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 wherever they are located.

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 (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 4th 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 with RdSeed 2.0 provides a very fast and 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 800-90B and 800-90C) 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.

**Security Monitoring 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 Technology® (Intel® AMT) can 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 4th 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.16
• 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.

**System-Wide Monitoring**

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.

**Monitoring and Prevention**

Every business client based on a 4th generation Intel Core vPro processor maintains a high level of its situational awareness with BIOS protection, constant health monitoring, hardware and software inventories, and appropriate responses to any detected irregularities.

**Protection for BIOS**

Very sophisticated threats are making their way around the globe and into the BIOS of PCs, corrupting the very core of the boot process. Intel® Platform Protection Technology with BIOS Guard® helps protect business clients against BIOS corruption from BIOS changes without proper signing and authorization.

**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 4th 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 antivirus 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 of 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 4th 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 malware.

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 Enhanced Remote Control

Deskside and service-center calls can take up the majority of IT’s 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 Enhanced KVM Remote Control 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.
• Choose your work style. KVM Remote Control supports up to three monitors at up to 2560x1600 resolution, and is available in 27 languages.

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

While today’s threats use new stealthy techniques for targeted attacks on companies and organizations, business platforms based on Intel processors for business clients 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 PTT and Intel Platform Protection Technology with Boot Guard support Windows 8 secure boot for a safe environment before loading 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 data on the go.
- Intel vPro Technology helps reduce the effort and cost of threat prevention and remediation.

All these built-in technologies, available only in systems based on Intel processors for business clients, 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
White Paper: Enterprise-Class Protection with Intel® Processors for Business Clients

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

2. 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 Intel® processor manufacturer for more information. For more information, visit http://www.intel.com/go/virtualization.

3. 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.

4. 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.

5. 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 vary. Contact your system manufacturer for more information.

6. Intel® OS Guard requires an Intel® 4th generation Core™ processor, Intel® software and OEM-enabled BIOS, Intel® vPro™ processor, and an capable operating system. Consult your system manufacturer for more information.

7. No computer system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, and firmware, and software, and participation in the system. 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://intel.com.

8. KVM Remote Control (Keyboard Video Mouse) is only available with Intel® vPro™ processor. Intel® software and OEM-enabled BIOS, and an Internet connection. Solid-state drive (SSD) or equivalent may be required. Depending on system configuration, your results may vary. Contact your system manufacturer for more information.


10. No system can provide absolute security under all conditions. Requires an Intel® Trusted Execution Technology-enabled processor, an Intel® TXT-enabled processor, chipset, BIOS, Authentic Code Modules and an Intel® TXT-compatible measured launched environment (MILE). Intel® TXT also requires the system to contain a TPM v1.2. For more information, see http://www.intel.com/technology/security.

11. Intel® Identity Protection Technology-enabled system, including a 2nd, 3rd, or 4th gen Intel® Core™ processor, enabled chipset, firmware, and software, and participation in the system. 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://intel.com.

12. Advanced Encryption Standard – New Instructions (AES-NI) requires a computer system with an AES-NI-enabled processor, 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.

13. No system can provide absolute security. Requires an Intel® Secure Key enabled PC with a 4th gen Intel® Core™ vPro™ processor and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.

14. 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/management/amt.

15. 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.


17. 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.