Sales Brief

Intel and McAfee 2012 Security Benefits

Intel (with McAfee) delivers a new level of security by combining hardware with software for unprecedented protection and a safer, more worry-free computing experience across clients, data center, and the cloud.

Identity and Access – Helping ensure only authorized users can access your networks and data

- Intel® Identity Protection Technology (Intel® IPT) – A more secure way to protect your enterprise from identity theft[1]

- McAfee® Total Protection for Endpoint – Secures lost or stolen devices by blocking non-permitted access to your business-critical systems and sensitive data

- McAfee® Network Security Platform – The industry's leading next-generation scalable network intrusion prevention system for connected devices and virtualized environments

- McAfee® Data Loss Prevention – Protects critical data from unwanted access

## Data Protection – Helping protect your company's data and assets
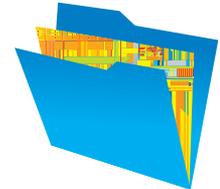
- Intel® Advanced Encryption Standard– New Instructions (Intel® AES-NI) – Faster encryption protects data sooner[2,3,4]

- Intel® Anti-theft Technology – Helps protect your data by disabling your lost or stolen laptop from anywhere[5]

- McAfee® Total Protection for Endpoint – Secures systems and data against sophisticated malware, zero-day attacks, noncompliant systems, and unauthorized devices

- McAfee® Network Security Platform – Protects network-connected devices against advanced, targeted attacks, using a combination of powerful, sophisticated defenses

- McAfee® Data Loss Prevention – Safeguards critical data and helps ensure regulatory compliance through multilayered protection regardless of data location

- McAfee® Database Security – Easily implemented real-time, reliable protection for business-critical databases from external, internal, and intra-database threats

Threat Management – Helping protect your computing environment from damaging threats

- Intel® Trusted Execution Technology (Intel® TXT) – Establishes a hardware-based root of trust for virtualization[6]

- Intel® Virtualization Technology (Intel® VT) – Protects virtual environments from malware and rootkits[7]

- Intel® OS Guard – Protects the OS from privileged escalation attacks[8]

- McAfee® Global Threat Intelligence – Correlated real-world data collected from millions of sensors around the globe delivers comprehensive protection to stop the latest threats from Internet vectors: file, web, e-mail, and network

- McAfee® Integrity Control – Ensures only authorized sources can effect changes to critical infrastructure endpoints, including ATMs, kiosks, and point-of-sale devices

- McAfee® Deep Defender – Innovative hardware-assisted endpoint security detects, blocks, and remediates advanced, hidden attacks; built on the McAfee® DeepSAFE™ Technology co-developed with Intel

Monitoring and Remediation – Helping keep your computing environment healthy and running smoothly
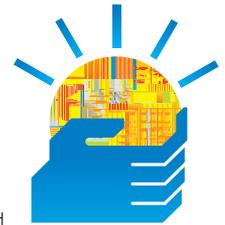
- Intel® Active Management Technology (Intel® AMT) – Remotely diagnose, isolate, and repair an infected PC, regardless of operational state[9]

- McAfee® ePolicy Orchestrator/Deep Command/Risk Advisor – With Intel® AMT, enables remote security management access to PCs, reducing security operations costs while enhancing security posture

- McAfee® Enterprise Security Manager – Enables fast, efficient management of security, threat management, and remediation across the enterprise

For more information on 3rd Gen Intel® Core™ vPro™ visit www.intel.com/pcsecurity

---

1 (Identity Protection Technology) 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 web site. 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.

2 (AES-NI) Intel® 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® Xeon® and Core™ processors. For availability, consult your reseller or system manufacturer. For more information, see http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html

3 (FTC Disclaimer) Software and workloads used in performance tests may have been optimized for performance only on Intel® microprocessors. Performance tests, such as SYSmark* and MobileMark,* are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

4 (Cross Client) Cross-client claim based on lowest performance data number when comparing desktop and mobile benchmarks. Configurations and performance test as follows: (Mobile) Comparing pre-production 3rd generation Intel® Core™ i5-3320M Processor (4T2C, 3M cache, up to 3.20 GHz), Intel Reference Board, pre-production BIOS, Memory 8 GB (2x4 GB) Micron* PC3-12800, Hitachi* Travelstar 320 GB hard-disk drive, Intel® HD Graphics 4000, Driver pre-production 8.15.10.2616, Chipset INF pre-production 9.3.0.1019. Intel® Core™2 Duo Processor P8600 (2T2C, 3M cache, 2.40 GHz, 1066 MHz FSB), HP* dv6, BIOS HP* vF.31, Memory 4 GB (2x2 GB) Micron* PC3-8500, Hitachi* 320 GB hard-disk drive, Mobile Intel® GM45 Chipset Family w/ integrated graphics Driver: 8.15.10.1749, Chipset INF 9.2.0.1030, Microsoft Windows* 7 Ultimate 64-bit 6.1 Build 7601. (Desktop) Comparing pre-production 3rd generation Intel® Core™ i5-3450 Processor (4T4C, 6 MB cache, 3.1 GHz base up to 3.5 GHz), Intel® Desktop Board DH77KC, Memory 8 GB (2x4 GB) Micron* DDR3-1600, Seagate* 1 TB, Intel® HD Graphics 2500, Driver: 8.15.10.2616 (BIOS:vSLZ7510H.86A.0033.2011.1230.1146, Chipset INF 9.3.0.1019, Intel® Core™2 Duo E8400 (2C2T, 3.0 GHz, 6 MB cache), Memory 4 GB (2x2 GB) Micron* DDR2 800 MHz, Seagate* 1TB hard-disk drive, Intel® G45, Driver: 8.15.10.2189, (BIOS:IDG4510H.86A.0135.2011.0225.1100, INF), Microsoft Windows* 7 Ultimate 64-bit 6.1 Build 7601. Encryption workload consists of SiSoftware Sandra* 2011—AES256 CPU Cryptographic subtest measures CPU performance while executing AES (Advanced Encryption Standard) encryption and decryption algorithm. For more information go to http://www.intel.com/performance.

5 (Anti-Theft) No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware, and software with disk encryption, and service activation with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Service may not be available in all countries. 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.

6 (TXT) 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, visit www.intel.com/go/inteltxt.

7 (Virtualization) Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, 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/content/www/us/en/virtualization/virtualization-technology/hardware-assist-virtualization-technology.html.

8 (OS Guard) 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.

9 (AMT) Security features enabled by Intel® 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, see http://www.intel.com/technology/vpro.

The information in this document is provided only for educational purposes and for the convenience of McAfee and Intel customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.