

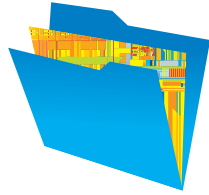


Sales Brief

Intel and McAfee 2013 Security Benefits

Intel and McAfee deliver a new level of strengthened security innovation utilizing embedded hardware security technologies for unprecedented protection and a safer computing experience across clients, data center, and the cloud.

Data Protection – Helping protect your company’s data and assets



- **Intel® Advanced Encryption Standard– New Instructions (Intel® AES-NI)** – Faster encryption protects data sooner.^{1,2,3}
- **Intel® Secure Key** – Very fast generation of high-quality, truly random numbers for encryption keys, compliant with NIST SP 800-90B/C and NIST FIPS 140-2 level 2 certified.⁴
- **Intel® Professional Series SSD** – Total disk encryption with incredibly fast performance, delivering speed and security.
- **McAfee Total Protection for Data** – Comprehensive data protection anytime, anywhere. Suite includes strong encryption, data loss prevention (DLP), policy-driven security, and a robust management platform help block unauthorized access to your sensitive information and prevent data leakage.
- **McAfee Endpoint Encryption** – Powerful and fast data encryption, utilizing Intel® AES-NI, and integrated with unique out-of-band centralized management.
- **McAfee® Data Loss Prevention** – Safeguards critical data and helps ensure regulatory compliance through multilayered protection regardless of data location.
- **McAfee Device Control** – Protects data from falling into the wrong hands via removable storage devices and media, such as USB drives, MP3 players, CDs, and DVDs.

Threat Management – Helping protect your computing environment from damaging threats across hardware environments and platforms

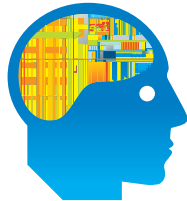


- **Intel® Trusted Execution Technology (Intel® TXT)** – Establishes a hardware-based root of trust for virtualization.⁵
- **Intel® Platform Trust Technology (Intel® PTT)** – Firmware-based trust technology supports TPM-like secure boot on Intel® Atom™ processor-based business platforms.⁶
- **Intel® Platform Protection Technology with Boot Guard** – Supports secure boot protection with TPM or Intel PTT.⁶
- **Intel® Platform Protection Technology with BIOS Guard** – Helps protect against threats targeting the BIOS firmware.⁶
- **Intel® Virtualization Technology (Intel® VT)** – Enables other protective technologies to discover potential threats beyond the OS.⁷
- **Intel® OS Guard** – Protects the OS from privileged escalation attacks.⁸
- **McAfee® Deep Defender** – Innovative hardware-enhanced endpoint security detects, blocks, and remediates advanced hidden attacks—operates outside the OS and built on the McAfee® DeepSAFE™ Technology co-developed with Intel.
- **McAfee® Total Protection** – Secures systems and data against sophisticated malware, such as botnets and zero-day attacks, and blocks noncompliant systems and unauthorized devices that attempt to access your business-critical systems and data.
- **McAfee® Application Control** – Effectively blocks unauthorized applications and code on servers, corporate desktops, and fixed-function devices; stops zero-day threats.
- **McAfee® Integrity Control** – Ensures only authorized sources can effect changes to critical infrastructure endpoints, including ATMs, kiosks, and point-of-sale devices.
- **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® Management for Optimized Virtual Environments (MOVE) AntiVirus** – Optimizes McAfee virus protection for virtual desktops and servers without compromising performance or security, helping you realize operational returns and more effective security management.
- **McAfee® Firewall Enterprise** – Defends critical assets, including regulated data repositories (customer, financial, and healthcare data), e-mail and web servers, extranets, and data centers.

ADVANCED PROTECTION
STRONG ENCRYPTION
MULTI LAYERED

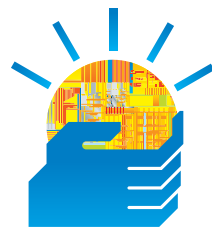


Identity and Access - Helping ensure only authorized users can access your networks and data



- **Intel® Identity Protection Technology (Intel® IPT)** - A more secure way to protect your enterprise from identity theft.⁹
- **McAfee® Cloud Identity Manager** - Enforces corporate security standards for cloud application access; improves productivity for IT and end users by relieving password reset requests; supports Intel® IPT for one-time passwords.
- **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.
- **No-Password VPN (using Intel® IPT with PKI)** - Simplifies user experience and maintains high security for corporate networks.⁶

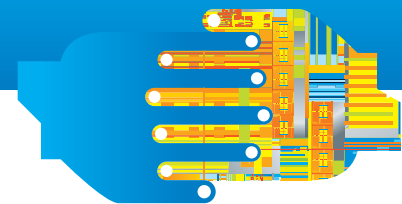
Monitoring and Remediation - Helping keep your computing environment healthy and running smoothly



- **Intel® Active Management Technology (Intel® AMT)** - Remotely diagnose, isolate, and repair an infected PC, regardless of operational state.¹⁰
- **McAfee® ePolicy Deep Command** - 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.
- **McAfee® ePolicy Orchestrator** - Centralizes and streamlines management of endpoints, networks, data and compliance solutions with a platform that integrates with and leverages your existing IT infrastructure.



A NEW LEVEL OF SECURITY



For more information on 4th Gen Intel® Core™ vPro™
visit www.intel.com/pcsecurity



¹(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>.

²(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.

³(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>.

⁴(Secure Key) 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.

⁵(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.

⁶No 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.

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(Identity Protection Technology) No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd, 3rd, or 4th 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>.

¹⁰(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.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the United States and other countries.

Copyright © 2013 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Atom, Core, vPro, and Xeon are trademarks of Intel Corporation in the U.S. and other countries. *Other names and brands may be claimed as the property of others.

Printed in USA

0513/ACH/HBD/PDF

 Please Recycle

327664-003US

