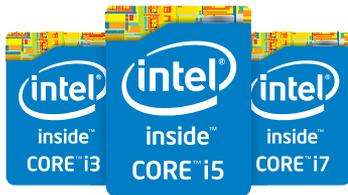


Breakthroughs in Zero Impact Data Protection

Help stop data loss while maintaining user productivity



In an increasingly mobile world, your company's data is as well-traveled as you are. Gone are the days when information resided in one locked room. Now your data jumps across an expanse of potentially defenseless devices, operating systems, and Internet-ready locations.

Your IT department works hard to implement protection solutions in anticipation of an attack compromising your highly sensitive data. Unfortunately, many of these solutions can significantly impair user productivity due to their intense CPU drain. As a result, users might either temporarily disable or completely uninstall the software, leaving enticing data vulnerable. Now, you must remediate and enforce compliance. You want to minimize interruption in performance and productivity, and you want to feel confident that data is protected across all endpoints. You need speedy software that delivers both high-level security and user satisfaction.

Boost Data Protection

Imagine a solution that does not force you to sacrifice protection in favor of user productivity. The benefits are threefold: deep data security, optimized device performance, and restoration of user output and satisfaction. All this while rolling your initial security investment into an enhanced tool that's as easy to install as a plug-in—a small, incremental step to your current, or future, McAfee® ePolicy Orchestrator® (McAfee ePO™) deployment.

The solution is McAfee® Complete Data Protection Suites powered by Intel® Core™ vPro™ processors. McAfee Complete Data Protection Suites offer:

- Drive encryption
- File and removable media protection
- Management of native encryption (for Apple Mac* devices)
- McAfee ePO Deep Command

When you deploy endpoints powered by Intel® Core™ processors, you also get Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI),¹ which accelerates encryption for efficient protection with faster performance. You get an encryption solution that is not only extremely fast, but also that is FIPS 140-2 and Common Criteria EAL2+ certified for the Intel AES-NI implementation.

Use Your Existing Infrastructure

McAfee Complete Data Protection Suites are administered by McAfee ePolicy Orchestrator. There's no new interface to stumble through, no ramp-up time to bog down your increasingly busy IT team, and no expensive systems to upgrade. With McAfee ePO, you have the advantage of single-console management and the convenience of dashboard reporting to help with compliance and security posture reporting.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)¹ is an instruction set found in Intel® Core™ processors and latest-generation Intel® Atom™ processors that increases encryption and decryption performance and reduces processor load. Intel AES-NI forms the secure backbone of McAfee® Endpoint Encryption technologies by helping users maintain productivity while protecting data on PCs, network files, removable USB storage devices, and CD/DVDs. Full integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) software lets you to centrally manage deployments, policies, password recovery, reporting, and auditing for consistent protection and lower total cost of ownership (TCO).

Encryption without Burden

Your users’ various tasks demand varied levels of hardware performance. To illustrate what impact the McAfee encryption solution has on performance, benchmarks were performed by using SYSmark 2012 on a system with and without encryption. SYSmark 2012 is an application-based benchmark that reflects usage patterns of business users in the areas of office productivity, data and financial analysis, system management, media creation, 3-D modeling, and web development.

Results from the SYSmark 2012 benchmark (Figure 1) indicate there is minimal to no discernable impact to the end user when McAfee encryption is enabled.

Users Focus on Work, Not Start-Up Times

In addition to fast computation for specific tasks, users also demand speedy boot ups and minimal time required for laptops to enter standby. These functions, although not occurring as frequently as application tasks, are an element of end-user satisfaction and lead to the perception of how well their system performs. Figure 2 shows that hardware-enhanced encryption keeps devices humming. Performance studies where McAfee encryption is installed reveal minimal user-perceptible lag in boot time and minimal impact when laptop lids are closed.

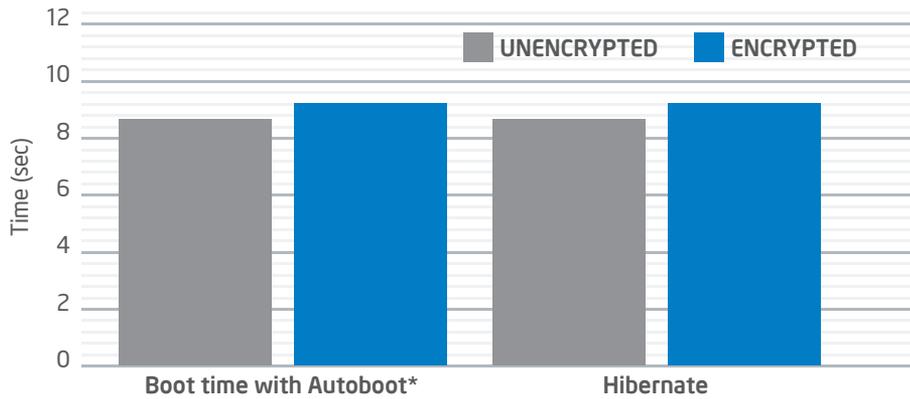
SYSmark 2012* Performance Benchmark Results

	Unencrypted	Encrypted	Encryption Perf. Impact (%)
Overall Rating	113	112	0.99
Office Productivity	110	109	0.99
Media Creation	106	105	0.99
Web Development	103	102	0.99
Data/Financial Analysis	131	132	1.01
3-D Modeling	109	108	0.99
System Management	120	117	0.98

SYSmark 2012 did not see significant performance degradation in encrypted versus unencrypted drive test cases (within 2 percent)

Figure 1. Results from the SYSmark 2012 benchmark show there is little or no discernable impact to the end user when McAfee encryption is enabled for the types of usages noted (<http://bapco.com/products/sysmark-2012>).^{2,3,4}

Boot and Hibernate Times



Impact on boot and hibernate times with encryption enabled were minimal using a standard hard disk drive storage device

Figure 2. For boot and hibernate times, the effect of enabling McAfee is very small, which results in minimal impact to the end user.^{2,6,7,8}

Protect Your Endpoints with Comprehensive Remote Management

McAfee Complete Data Protection Suites add McAfee ePO Deep Command as a plug-in to your already existing McAfee ePO configuration. Administrators can quickly discover and provision Intel® Active Management Technology (Intel® AMT)⁹ enabled PCs with Intel® vPro™ technology,¹⁰ even when client devices are off premises. The additional power of McAfee ePO Deep Command lets security administrators configure and remediate hard-to-manage endpoints. McAfee ePO Deep Command utilizes Intel AMT, which enables secure remote access regardless of the PC's power or encrypted state. Therefore, security administrators can remotely remediate

compromised systems, enable energy-saving initiatives, wake systems, and apply proactive security, reducing help desk calls by remotely resetting user passwords. They can do all this using the comprehensive management and reporting provided by McAfee ePO software.

Let McAfee Make Your Job Easier

Allow the combined features of McAfee Complete Data Protection Suites with Intel Core vPro processors to make you a company hero. The joint solution provided by McAfee software running on Intel hardware means no more sacrificing security for speed. Your job just got a whole lot easier.

ENCRYPTION FEATURES

Drives

Automatically encrypt entire devices without requiring user action or training and without impacting system resources. Identify and verify authorized users by using strong multifactor authentication.

Compliance

Protect your data with an endpoint encryption solution that is FIPS 140-2 and Common Criteria EAL2+ certified for the Intel® AES-NI implementation.

Persistent File and Folder Encryption

Ensure that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved.

Optical/Removable Media

Get automatic, on-the-fly encryption for virtually any mobile storage device, company-issued or not.

Self-Extracting Files

Send encrypted email attachments and allow access to the attachment without requiring the recipient to install any additional software.

McAfee® ePolicy Orchestrator® (McAfee ePO™)

McAfee® Complete Data Protection Suites are just another plug-in for your current McAfee ePO software deployment—a small, incremental step to your existing McAfee solution.

Learn More

For more information about comprehensive hardware-based security solutions from Intel and McAfee, visit the following web sites and documentation:

- McAfee Complete Data Protection Suites
<http://www.mcafee.com/us/products/data-protection/index.aspx>
- Intel Core vPro processors
<http://www.intel.com/content/www/us/en/processors/vpro/core-processors-with-vpro-technology.html>
- Keep Your Client PCs Safer, Wherever They Go
<http://www.mcafee.com/us/resources/solution-briefs/sb-keep-your-client-pcs-safer.pdf>
- Protect Your Company's Data with Efficient Encryption and Secure Remote Management
<http://www.mcafee.com/us/resources/white-papers/wp-protect-your-companys-data-with-efficient.pdf>

¹ No computer system can provide absolute security. Requires an enabled Intel® processor and software optimized for use of the technology. Consult your system manufacturer and/or software vendor for more information.

² System under test: Lenovo IdeaPad U430 Touch* Ultrabook, Windows 8* Pro 64-bit build 6.9.9200, 4th generation Intel® Core™ i5-4200U processor 2C 4T 1,600MHz, 4 MB memory, Seagate 500 GB HDD 5400 rpm

³ Benchmark: SYSmark 2012 v1.5.1.271 (64-bit).

⁴ BAPCo SYSmark 2012 is an application-based benchmark that reflects usage patterns of business users in the areas of office productivity, data/financial analysis, system management, media creation, 3-D modeling, and web development. SYSmark 2012 features the latest and most popular applications from each of their respective fields.

⁵ Performance 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. For more information, go to <http://www.intel.com/performance>.

⁶ Boot time with Autoboot: Autoboot bypasses the McAfee authentication screen, which unlocks the encrypted drive. Enabling the authentication screen increases boot latency by approximately 5.7 seconds. Use of the authentication screen is recommended for maximum drive protection.

⁷ Encrypted and unencrypted boot times were measured from power LED on to Windows* logon screen appearance.

⁸ Hibernate times were measured from entering the command in the setting/power menu to LED powering off.

⁹ Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit <http://www.intel.com/content/www/us/en/architecture-and-technology/intel-activemanagement-technology.html>.

¹⁰ 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>.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. 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.

McAfee, the McAfee logo, McAfee ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries.

The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2013 McAfee, Inc.

Intel, the Intel logo, Intel Core, Atom, and vPro are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Printed in USA 0114/PC/PRW/PDF

♻️ Please Recycle 329926-001US

