IT@Intel White Paper

Intel IT
Data Protection
November 2013

Improving Data Protection with McAfee Drive Encryption

McAfee Drive Encryption safeguards Intel's corporate data and intellectual property—as well as employees' personal information—while improving the user experience and boosting productivity.

Executive Overview

Intel IT is deploying McAfee Drive Encryption, an integral component of new McAfee security products such as McAfee Complete Data Protection - Advanced software suite. McAfee Drive Encryption provides a hybrid agent that can automatically and transparently detect whether software- or hardware-based encryption is needed.

This hybrid approach is an important aspect of encryption manageability for Intel IT because our environment includes an installed base of laptops with Intel® Solid-State Drives (Intel® SSDs) and non-Opal-compliant, self-encrypting drives (SEDs), which require software-based encryption. Our environment also includes Opal-compliant drives, such as the Intel® SSD Pro 1500 Series, which support hardware-based encryption.

We experienced a number of benefits with McAfee Drive Encryption, such as the following:

- Deployed on more than 40,000 systems with zero data loss to date
- 100-percent integration with existing products and processes
- One central management console (a "single pane of glass") that can generate enterprise-wide reports for multiple security solutions, with detailed compliance reporting
- Significantly faster resume from hibernation than our previous software-based encryption solution[1]

McAfee Drive Encryption safeguards Intel's corporate data and intellectual property—as well as employees' personal information—while improving the user experience and boosting productivity. We expect to complete the migration to McAfee Drive Encryption across Intel's laptop fleet by mid-2014.

Oded Bar-El
Client Security Engineer, Intel IT

Efi Kaufman
Client Security Product Manager, Intel IT

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

The quantity and sophistication of information security threats continue to increase for enterprises because of the rapid growth of social media, cloud computing, IT consumerization, and mobile technology. By implementing our "Protect to Enable" security strategy Intel IT is helping to increase protection while continuing to support the flow of information and the adoption of new technologies.

To help protect Intel's intellectual property and employees' personal information, in 2009 we deployed software-based encryption on corporate-owned laptops provided to employees. We encrypted the entire drive—including data, applications, the OS, and free space. If a system was lost or stolen, unauthorized individuals could not access the data stored on the drive.

While the solution we deployed greatly improved data security, it posed operational and business challenges:

- **Performance.** Employees perceived a performance impact because continuous encryption and decryption activity required a significant portion of the CPU compute capacity—even on Intel® Solid-State Drives (Intel® SSDs). Also, passphrase recovery required assistance from an IT Help Desk technician.
- **Compliance and manageability.** We found it challenging to verify that each system had the encryption software installed and that each employee had completed the encryption process.
- **Reliability.** We experienced reliability issues associated with passphrase recovery; in some cases, employees lost all data stored on the laptop.

We continually monitor innovations in information security technology and evolve our data protection techniques as technology changes and matures. The development of the Opal standard, published by the Trusted Computing Group, led us to formulate a long-term encryption roadmap in 2012. This roadmap includes Opal-compliant drives (see sidebar, "McAfee Drive Encryption and the Opal Standard") as well as standard encryption-management software.

Because Opal-compliant drives were not generally available in 2012, we developed a near-term hardware-based encryption solution using self-encrypting drives (SEDs)

McAfee Drive Encryption and the Opal Standard

The Opal standard, published by the Trusted Computing Group (TCG), defines a set of mechanisms and protocols for self-encrypting drives (SEDs), including encryption, authentication, configuration, and policy management. The TCG is a not-for-profit organization formed to develop, define, and promote open, supplier-neutral industry standards for trusted computing building blocks and software interfaces across multiple platforms.

SED solutions based on the Opal standard enable integrated encryption and access control within the protected hardware of the drive. SEDs provide the industry's preferred solution for drive encryption, protecting data when the machines or drives are lost, stolen, repurposed, under warranty repair, or at end-of-life. The Opal standard provides multi-vendor interoperability, allowing application vendors to manage SEDs from multiple providers.

Starting with version 6.2, McAfee Drive Encryption supports self-encrypting Opal-based drives on both the Unified Extensible Firmware Interface (UEFI) and BIOS. If McAfee Drive Encryption detects an incompatible or unsupported combination of an OS and Opal drive, it continues the activation process using software encryption instead of the native Opal functionality.

and Intel® Active Management Technology,[2] part of Intel® vPro™ technology.[3] This solution created an end-to-end enterprise-scale management solution for SEDs. As part of the solution, we developed a passphrase-management utility, manageability web services, and a secured database.[4]

The Opal-compliant Intel® SSD Pro 1500 Series is now available (see sidebar, "The Intel® Solid-State Drive Pro 1500 Series"). We are deploying these drives, which support hardware encryption, through our standard hardware refresh cycle. For our installed base of PCs that do not have Opal-compliant SEDs, we still require a software-based encryption solution that is more reliable than the previous software-based solution and that better meets the performance expectations of Intel employees.

SOLUTION

We are replacing our previous software-based encryption solution with McAfee Drive Encryption, which is an integral component of the new McAfee security products such as McAfee Complete Data Protection - Advanced suite.[5] We have chosen a deployment approach that minimizes the impact to employees and avoids inadvertent exposure of corporate data to attack during the encryption solution migration process.

McAfee Drive Encryption provides a hybrid agent that can automatically detect whether software- or hardware-based encryption is needed. This detection is transparent to the end user, and in either situation McAfee Drive Encryption provides drive manageability capabilities.

- If needed, McAfee Drive Encryption uses software-based encryption and takes advantage of Intel® Advanced Encryption Standard – New Instructions (Intel® AES-NI)[6]—found in select Intel® processors—to improve system performance.
- When running on a system that is equipped with an Opal-compliant drive, McAfee Drive Encryption automatically detects the drive type and offloads all the encryption and decryption processes to be executed by the Opal drive hardware, which provides maximum system performance.

McAfee Drive Encryption is now our primary drive encryption solution.

The Intel® Solid-State Drive Pro 1500 Series

The Intel® Solid-State Drive (Intel® SSD) Pro 1500 Series helps accelerate storage and lower total cost of ownership with integrated drive encryption, remote management, and high reliability. The following list summarizes some of the enterprise-level benefits associated with the Intel SSD Pro 1500 Series.

- **Flexibility**. Capacities range from 80 GB to 480 GB. Available in both thin 2.5-inch and smaller M.2 form factors, the Intel SSD Pro 1500 Series was designed for the latest Ultrabook™ 2 in 1[7] designs and can also fit into more traditional PC platforms.
- **Enhanced security and manageability.** The Intel SSD Pro 1500 Series introduces Trusted Computing Group Opal protocols[8] across the full range of supported capacities and form factors, providing industry-standard encryption-key-management capabilities. The integrated hardware-based 256-bit Advanced Encryption Standard (AES) engine seamlessly encrypts and decrypts data without compromising performance.
- **Power-efficient performance.** The Intel SSD Pro 1500 Series accelerates platform performance. Sequential I/O operations occur at 490 to 540 megabytes per second; the drive can process from 42K up to 80K random input/output operations per second (IOPS).[9] In addition to strong performance gains, the Intel SSD Pro 1500 Series extends battery life through advanced low-power modes, reducing idle power by over 90 percent in comparison to a typical hard disk drive. This reduces power usage from watts to milliwatts. When the Intel SSD Pro 1500 Series is coupled with a 4th generation Intel® Core™ vPro™ processor platform, power consumption is reduced another order of magnitude—from milliwatts to microwatts.
- **Enterprise-ready quality and reliability.** The Intel SSD Pro 1500 Series is designed to meet an annualized failure rate of less than 1 percent,[10] which can significantly reduce total cost of ownership.

Benefits of McAfee Drive Encryption

Overall, McAfee Drive Encryption improves performance, compliance and manageability, and reliability compared to our previous software-based encryption solution. The combination of these benefits helps provide enhanced information security and better business value.

PERFORMANCE

We conducted performance tests on a system with no software-based encryption, a system with McAfee Drive Encryption, and a system with our previous software-based encryption solution. All of our tests were performed on systems with the same configuration.[11] The three tests were:

- Test case 1 - Resume from hibernation with no applications running
- Test case 2 - Resume from hibernation with several common applications
- Test case 3 - Power on

In test cases 1 and 2, system performance for laptops using McAfee Drive Encryption was significantly faster than a similarly configured laptop using our previous software-based encryption solution. In addition, in test cases 1 and 3, the McAfee Drive Encryption system performed almost as fast as the system with no software encryption installed (see Figure 1).

COMPLIANCE AND MANAGEABILITY

McAfee Drive Encryption represents enhanced manageability from several perspectives, such as integration with our existing environment and processes, improved compliance reporting, and passphrase recovery. The following sections provide more detail about each of these areas.

Integration with Our Environment and Processes

We already had McAfee security products installed in our environment, such as McAfee VirusScan® software and McAfee Host Intrusion Prevention. Therefore deploying McAfee Drive Encryption provides operational and security staff with a "single pane of glass" to run comprehensive reports about the information security status of all client PCs. A central management-and-reporting console enables IT administrators to easily set policies, demonstrate compliance, identify unencrypted laptops, and respond rapidly to loss or theft.

Additionally, our previous software-based encryption solution required a dedicated set of servers. In contrast, all management of McAfee Drive Encryption—including installation, encryption and decryption, and uninstallation—is managed solely from the McAfee ePolicy Orchestrator® (McAfee ePO™) console. Delivery of McAfee Drive Encryption is managed through McAfee Agent.

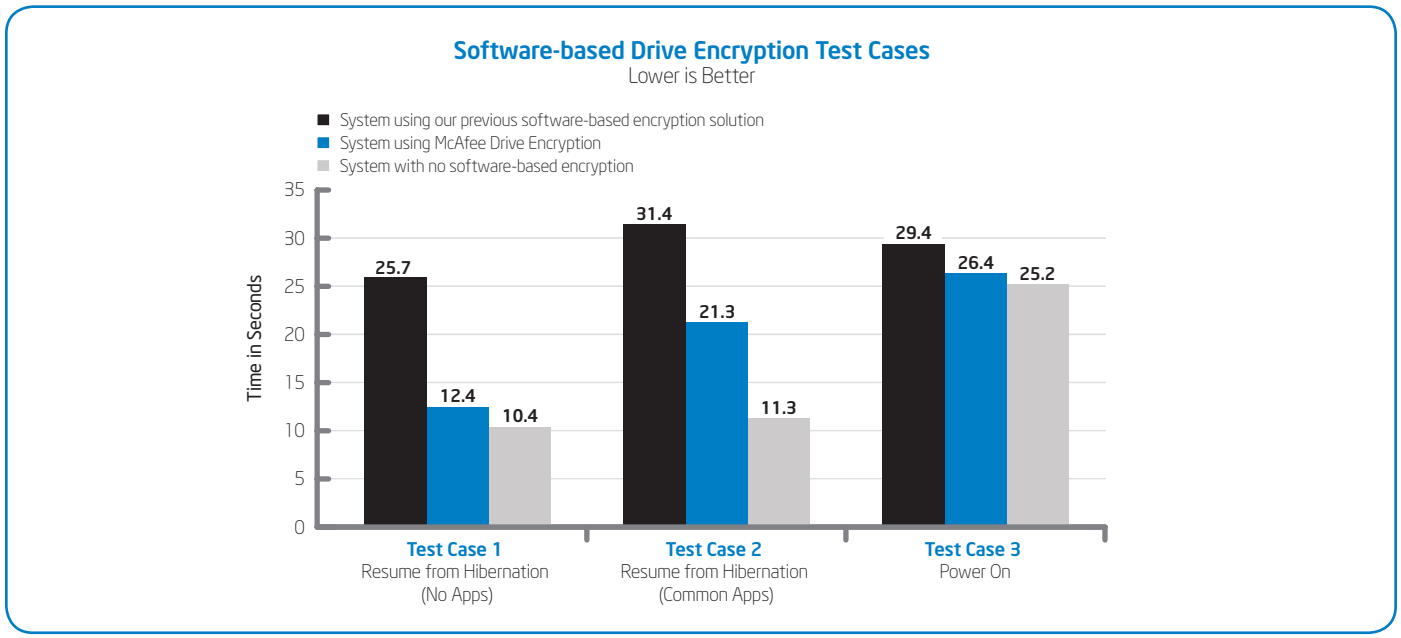

Figure 1. McAfee Drive Encryption outperforms our previous software-based encryption solution. In our tests, a system running McAfee Drive Encryption resumed from hibernation or powered on almost as fast as a system with no software encryption installed.

Figure 2 summarizes the process of encrypting a drive using McAfee Drive Encryption from the McAfee ePO console. With our previous software-based encryption solution, employees were required to start the encryption process themselves and could pause it, which raised compliance and security issues. With McAfee Drive Encryption, encryption starts without user intervention. The employee is prompted to create a passphrase and self-recovery answers upon first reboot after encryption has started. Similarly, employees were previously required to start the decryption process once decryption privileges had been granted. With McAfee Drive Encryption, decryption starts automatically once the system is provided with the decryption policy on the back-end.

Compliance Reporting

For compliance management, we previously relied on business group individuals who were tasked with making sure employees follow intellectual property protection guidelines. These individuals tracked which employees had enrolled in the encryption solution and completed the encryption process. With McAfee Drive Encryption, compliance is managed by the security operations staff; enrollment happens automatically.[12]

The McAfee ePO console provides approximately a dozen drive-encryption reports: drive-encryption status, installed version, tracking of client events, and more. All reports are exportable to CSV, HTML, and PDF files. Administrators can also query the ePO database using a wizard-like interface to generate customized reports as needed.

Passphrase Recovery

McAfee Drive Encryption simplifies the recovery of lost or forgotten passphrases using one of two methods—self-recovery or administrator recovery. Self-recovery is less time consuming and more efficient for employees, doesn't require phone or network access, and reduces operational costs by lowering support ticket volume.

- **Self-recovery** is based on personal information in the form of security questions, which the employee can answer without intervention from the IT Help Desk. This feature must be enabled in the ePO console; in addition, the policy must define the number of attempts after which self-recovery is invalid and the number of question to be answered (up to 10). Once the feature is enabled the employee is asked to set the answers after a successful authentication. When a passphrase is lost, the employee is prompted for the self-recovery answers and, if authenticated, is required to set a new passphrase.
- **Administrator recovery** is based on the exchange of challenge and response codes between the employee and an IT Help Desk technician. This feature must also be enabled in the McAfee ePO console. When a passphrase is lost, the employee is presented with a challenge code to be read to the support technician. The technician generates a response code using the McAfee ePO console. The employee types this response code into the McAfee Drive Encryption authentication window. As with self-recovery, once authenticated, the employee is required to set a new passphrase.

RELIABILITY

Unreliable encryption solutions can easily cause data loss. With our previous software-based encryption solution, due to problems with the encryption engine and the passphrase recovery process, about 50 employees per year lost all their data. In contrast, we now have more than 40,000 systems running McAfee Drive Encryption, and to date no data has been lost.

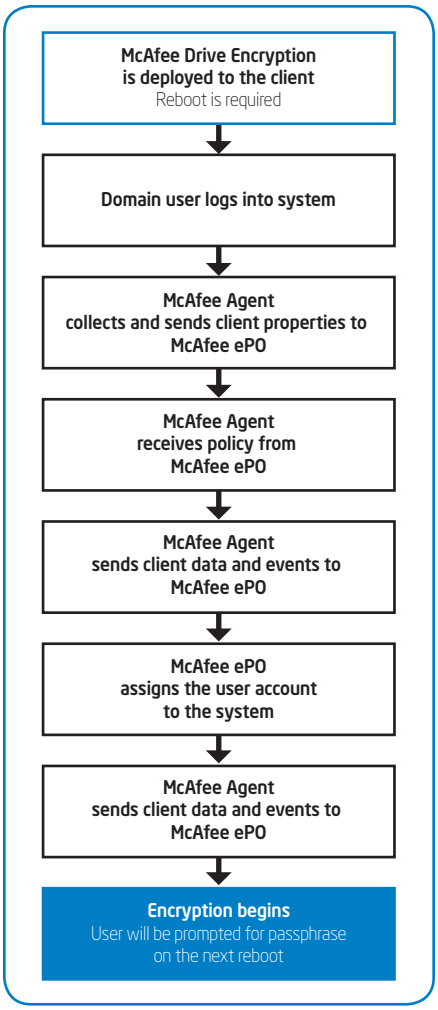

Figure 2. IT administrators manage McAfee Drive Encryption solely from the McAfee ePolicy Orchestrator® (McAfee ePO™) console.

Deployment Method

We are using passive refresh to deploy McAfee Drive Encryption as our primary encryption solution. We could have created a utility or requested that employees bring their laptops to PC Service Centers for migration. Instead we chose to deploy the new encryption solution through our standard refresh cycle—updating the encryption solution along with the hardware.

The decryption process drove this decision, because decryption can take several hours on systems that are not previously equipped with an SED. If an employee does not complete the migration process during work hours, the device could be left partially decrypted—with the data exposed—when the device is not at an Intel site or is left overnight. We wanted to avoid that possibility.

We expect the migration to McAfee Drive Encryption across Intel's laptop fleet to be completed by mid-2014.

CONCLUSION

Intel IT is chartered to protect Intel's corporate data and intellectual property—as well as employees' personal information. We are also committed to increasing employee productivity and improving the user experience. We are deploying McAfee Drive Encryption to improve performance, compliance, manageability, and reliability compared with our previous software-based encryption solution. The combination of these improvements provides a better user experience and reduces the number of calls to the IT Help Desk.

Our long-term encryption roadmap calls for deployment of Opal-compliant drives, such as the Intel SSD Pro 1500 Series. These high-performance drives support hardware-based encryption. For now, our computing environment includes an installed base of laptops with Intel SSDs and non-Opal-compliant SEDs, which require software-based encryption. McAfee Drive Encryption can automatically and transparently detect whether a drive is Opal-compliant and apply software- or hardware-based encryption as appropriate.

Over 40,000 systems are using McAfee Drive Encryption with the following benefits:

- No data loss to date.
- Easy integration with existing products and processes.
- A central management console (a "single pane of glass") with detailed compliance reporting.
- Significantly faster resume from hibernation (with and without applications running) compared to our previous software-based encryption solution.
- Systems with McAfee Drive Encryption performed almost as fast as systems with no software-based encryption in tests of power-on and resume from hibernation with no applications running.

These results demonstrate that McAfee Drive Encryption is a high-performing, reliable encryption solution with the enterprise-level, integrated manageability, and compliance reporting capabilities that we require.

For more information on Intel IT best practices, visit www.intel.com/it.

For more information McAfee Complete Data Protection - Advanced, visit www.mcafee.com/us/products/complete-data-protection-advanced.aspx.

ACRONYMS

AES	Advanced Encryption Standard
SED	self-encrypting drive

[1] 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. Configurations: All test performed on laptops based on Intel® Core™ i5 processor M540 2.53 GHz (dual core) with 4.00 GB RAM, Intel® Solid-State Drive X25-M Series. Values represent the time from when passphrase is provided to when the Alt+Ctrl+Del screen appears. Measurements were taken manually and were averaged over three samples. Common applications tested included email, spreadsheet, and web browser. All tests were performed by Intel IT. For more information go to www.intel.com/performance.

[2] Security features enabled by Intel® Active Management Technology (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, visit www.intel.com/content/www/us/en/architecture-and-technology/intel-active-management-technology.html.

[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: www.intel.com/technology/vpro.

[4] We will continue to use the self-encrypting drive passphrase-management application to support Intel® Solid-State Drive 320 Series and Intel® Solid-State Drive 520 Series as long as these drives are part of our computing environment. For more information about this solution, see the white paper "Managing Intel® Solid-State Drives Using Intel® vPro™ Technology."

[5] McAfee Drive Encryption was previously sold as a standalone product called McAfee Endpoint Encryption for PCs. This capability is no longer available as a standalone product.

[6] 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 software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.

[7] Ultrabook™ products are offered in multiple models. Some models may not be available in your market. Consult your Ultrabook device manufacturer. For more information and details, visit www.intel.com/ultrabook.

[8] Non-Opal-compliant Intel® Solid-State Drive Pro 1500 Series is also available.

[9] Performance varies slightly based on specific model. For more information, see www.intel.com/content/www/us/en/solid-state-drives/solid-state-drives-pro-1500-series.html.

[10] The annualized failure rate (AFR) is based on a mean time between failures (MTBF) of 1.2 million hours.

[11] See Endnote 1.

[12] The use of McAfee Complete Data Protection* or McAfee Complete Data Protection – Advanced* suites does not automatically guarantee compliancy or certify compliancy. IT departments should enlist the services of third-party compliancy auditing services for this. For more information, see community.mcafee.com/community/business/data/epoenc/blog/2013/05/16/mcafee-endpoint-encryption-support-for-it-governance-risk-and-compliance.