White Paper
May 2015

IT@Intel

Deploying Intel® Solid-State Drives with Managed Hardware-Based Encryption

Our new solution speeds up encryption and decryption activation, taking just a few seconds instead of over an hour.

Oded Bar-El
Client Security Lead Engineer, Intel IT

Shahar Rand
Client Security Engineer, Intel IT

Executive Overview

To gain the security benefits of centrally managed hardware-based encryption and to better protect Intel's intellectual property, Intel IT is deploying the Intel® Solid-State Drive (Intel® SSD) Professional Family combined with McAfee® Drive Encryption[1] 7.1.

Our encryption journey began in 2009 with the deployment of Intel SSDs and software-based encryption. As technology matured, we moved to a more stable software-based encryption solution that was integrated with the already deployed McAfee® ePolicy Orchestrator software—providing a "single pane of glass" view for all McAfee security products we were using. Later, we developed a custom hardware-based encryption management solution. These solutions provided incremental improvements for both users and IT employees.

Our current centrally managed hardware-based solution offers additional advantages:

- There is no noticeable impact on laptop performance.
- Encryption and decryption activation now takes just a few seconds, whereas software-based encryption took over an hour.
- Integration with McAfee ePolicy Orchestrator software enables us to track encryption compliance and generate encryption reports.
- The solution is easily scalable to accommodate growth in our PC fleet.

Our environment includes some older solid-state drives that still require software-based encryption. McAfee Drive Encryption provides the same user interface for both types of encryption and can automatically and transparently detect whether to use software-based or hardware-based encryption, depending on drive type.

Intel SSDs and McAfee Drive Encryption work in tandem to provide a more secure, higher-performing solution than either the latest encryption or SSD technology alone could.

[1] McAfee Drive Encryption is available as a key component of the McAfee Complete Data Protection Suites. Please visit www.mcafee.com/dataprotection for more information.

Contents

1 Executive Overview
2 Background
– Initial Software-Based Encryption (2009)
– Improved Software-Based Encryption (2010)
– Custom Hardware-Based Encryption (2011)
4 Solution: Managed Hardware-Based Encryption
– Managing a Mixed Encryption Environment
– Reprovisioning Opal-Activated SSDs
6 Next Steps
7 Conclusion

Contributors

John Mahvi, Client Product Manager, Intel IT

Roy Ubry, Client Engineering Staff Engineer, Intel IT

Doug DeVetter, Solutions Architect, Non-Volatile Memory Solutions Group

Acronyms

AFR annualized failure rate
SED self-encrypting drive
SSD solid-state drive
TPM Trusted Platform Module

Background

Intel IT helps protect Intel's intellectual property and employees' personally identifiable information by encrypting data stored on employees' laptops. Our goal has always been seamless, centrally managed hardware-based encryption, but until recently this was not technically feasible. As technology has evolved, our approach to encryption has changed, enabling us to get closer to our goal in recent years (see Figure 1). At each step of our multiyear encryption journey, we examined our options and picked the best one for us each time. Each technology choice, although best-in-class at the time, did have disadvantages. But each step brought us closer to deployment of the centrally managed Opal-compliant[2] self-encrypting drives (SEDs), such as Intel® Solid-State Drive (Intel® SSD) Pro 1500 Series and Intel® SSD Pro 2500 Series, which are currently part of the Intel® SSD Professional Family.

Initial Software-Based Encryption (2009)

We deployed our first software-based encryption solution in 2009. Initially we deployed it on traditional hard drives, which resulted in unacceptable drive performance, because the encryption software used a significant amount of CPU cycles and battery life. During the same period, we began transitioning our mobile PC fleet to Intel SSDs.

The software-based encryption's negative performance impact was far less noticeable on laptops equipped with an SSD. By tying together our encryption solution and our standardization on Intel SSDs, we were able to achieve

[2] The Opal standard, published by the Trusted Computing Group, offers a set of mechanisms and protocols for self-encrypting drives, including encryption, authentication, configuration, and policy management.

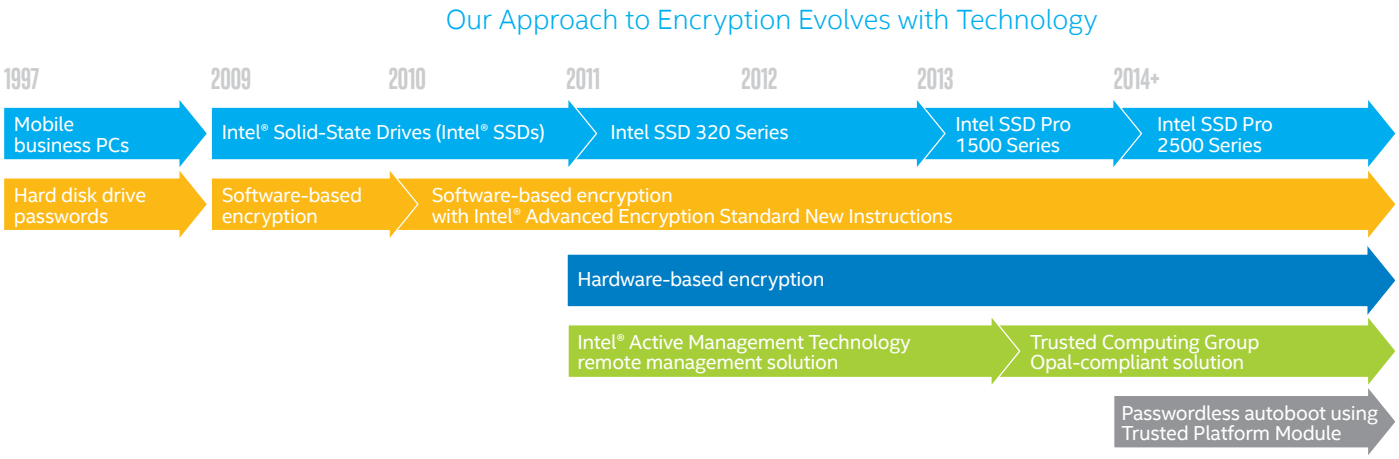

Figure 1. Intel's approach to drive encryption has evolved as technology has matured.

optimal results. However, the software-based encryption solution posed compliance manageability and reporting problems for IT: users sometimes did not complete the lengthy encryption process, we had no way to reliably determine how many SSDs were actually encrypted, and the management console was not integrated with the rest of our security solutions.

In 2010, we transitioned to a McAfee software-based encryption solution.

Improved Software-Based Encryption (2010)

The following year we transitioned to a McAfee software-based encryption solution, McAfee® Endpoint Encryption for PC. This solution supported Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), which improved encryption/decryption performance. It also included a central management system that provided a single view of all McAfee security solutions in use at Intel, such as virus scanning and intrusion-prevention tools.

Although drive performance was better than before, it was still slower than unencrypted drives. It also consumed CPU resources and shortened battery life. And, like the previous software-based encryption solution, the encryption and decryption process was still lengthy, making initial deployment and certain support actions slow and inefficient for IT technicians and Intel employees.

Custom Hardware-Based Encryption (2011)

In 2011, we began deploying SEDs, such as the Intel® SSD 320 Series and Intel® SSD 520 Series. SEDs have a drive controller that automatically encrypts all data to the drive and decrypts all data from the drive, improving the speed at which encryption and decryption occurs. These drives were not Opal-compliant, so we internally developed a hardware-based encryption management solution that took advantage of Intel® Active Management Technology, a component of Intel® vPro™ technology.[3]

The custom hardware-based encryption solution enabled us to improve the user experience (by improving performance and extending battery life), increase encryption compliance, and reduce support issues. However, the internally developed management solution was high-maintenance and resource intensive, making it impractical to scale across the enterprise.

[3] See the Intel IT white paper "Managing Intel® Solid-State Drives Using Intel® vPro™ Technology."

Solution: Managed Hardware-Based Encryption

Our current encryption solution combines two products that, working together, improve data protection at Intel:

- **Hardware-based encryption.** About 10,000 Opal-compliant Intel® SSD Pro 1500 Series are in use at Intel, and we soon will be transitioning to the Intel® SSD Pro 2500 Series.
- **Centrally managed encryption.** We are deploying McAfee® Drive Encryption 7.1[4] software integrated with McAfee ePolicy Orchestrator software.

McAfee Drive Encryption and Opal-compliant SSDs resolve the difficulties associated with our previous phases of encryption. Both users and IT staff benefit:

- **Minimal performance impact.** Laptop performance and battery life are unaffected by the presence of encryption, which can help users work more productively.[5]
- **Immediate encryption/decryption activation.** Encryption used to take an hour or more; now it can be done in just a few seconds. Users getting a new PC can leave the service center faster, and support actions take less time, increasing productivity for both users and IT staff.
- **Better compliance.** Unlike the software-based encryption process, the new process cannot be interrupted, so now we can be confident that during the build process the encryption is completed and the drive remains encrypted.
- **Better reporting.** Because McAfee Drive Encryption software is integrated with the McAfee ePolicy Orchestrator console, Intel IT can access more than a dozen reports specific to encryption in one convenient place. These reports include the disk status, installed version, client events, and more. All reports are exportable to CSV, HTML, and PDF formats and can be sent as attachments to email messages. A sample report is shown in Figure 2. Also, the IT administrator can create custom reports to fit enterprise needs and management requirements.
- **Scalable.** As Intel's client device fleet grows and becomes more and more mobile, combining McAfee Drive Encryption with Opal-compliant Intel SSDs helps our encryption solution keep pace.
- **Enhanced security.** Because it is implemented using hardware outside of the operating system, hardware-based encryption is more effective than software-based encryption in protecting against corruption and manipulation of encryption components.

The agent simply checks whether the drive is Opal-compliant. If it is, hardware-based encryption is enabled. If it is not, software-based encryption is enabled.

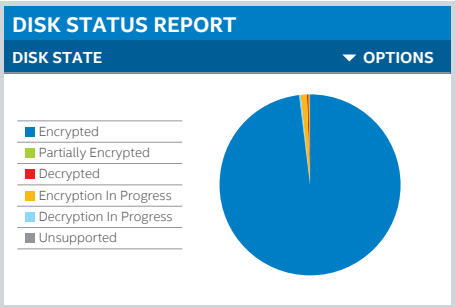

Figure 2. Integration of McAfee® Drive Encryption with McAfee® ePolicy Orchestrator software makes generating encryption reports easy. Here, the pie chart shows that the majority of drives are encrypted. FOR ILLUSTRATION PURPOSES ONLY.

[4] Previous releases of this product used the name McAfee® Endpoint Encryption for PCs.

[5] By nature, self-encrypting drives always encrypt/decrypt the information stored on them. The native performance of the drive is measured, tested, and spec'd in the encrypted state. "Encrypting the drive" is really just locking the authentication, so there is no performance change to the drive.

Managing a Mixed Encryption Environment

McAfee Drive Encryption provides a hybrid agent that can automatically and transparently detect whether software-based or hardware-based encryption should be used, depending on the configuration of the drive and on the rules that the IT administrator defines. This hybrid approach is an important aspect of encryption manageability and operations for Intel IT because our environment includes a variety of SSDs:

- Older Intel SSDs that require software-based encryption
- Non-Opal-compliant SSDs, for which we also use software-based encryption (not our custom-engineered hardware-based encryption management solution)
- Opal-compliant SSDs, such as the Intel SSD Pro 1500 Series and the Intel SSD Pro 2500 Series, which support hardware-based encryption

Because the hybrid agent runs in the background, unnoticeable to the user, the user interface and process are consistent whether the drive is using software-based or hardware-based encryption.

The hybrid agent also offers several advantages to Intel IT. First, we can simultaneously and invisibly transition from software-based to hardware-based encryption over time, using a normal refresh cycle, instead of having to purchase new hardware all at once. We can also use the same agent and the same IT image for all drives.

Finally, operating and supporting the encryption solution is simple—support staff and technicians become familiar with a single solution with a minimal learning curve between supporting software-based and hardware-based encryption.

Reprovisioning Opal-Activated SSDs

Reprovisioning SSDs with hardware-based encryption requires a different IT process than is used for software-encrypted drives. Essentially, we must take the drive out of the Opal management state and put it into a traditional management state.

Our approach is to deactivate the McAfee Drive Encryption solution using McAfee ePolicy Orchestrator, then use the Intel® Solid-State Drive Pro Administrator Tool to secure erase the drive. Even if we have lost administrative control of the drive (so that it cannot be managed), we can unlock it and securely repurpose it.

ROI for Solid-State Drives Is Increasing

When we began deploying Intel® Solid-State Drives (Intel® SSDs) in 2009, our ROI analysis identified many benefits of using solid-state drives:

- Rugged reliability with a low annualized failure rate (AFR), which can reduce total cost of ownership
- Responsive and power-efficient performance
- Longer battery life
- Flexibility and scalability due to multiple form factors and capacities
- Intel® Stable Image Platform Program, which reduces the complexity in managing a platform's lifecycle by stabilizing the variability in the key components and making the transition to the next-generation product line more predictable.

The AFR specification for the Intel® SSD Professional Family is less than 0.73 percent.[1] The observed AFR tracked by Intel is consistently less than 0.3 percent. In reviewing the Intel IT detailed incident data, we believe that the Intel SSD AFR observed by Intel IT generally falls in this same range.

[1] The AFR is based on mean time between failures (MTBF) of 1.2 million hours (1 ÷ MTBF x year = AFR). Intel SSD Professional Family AFR = 8,760 hours ÷ 1.2 million hours × 1 year = 0.73% per year.

Secure erase on Intel SSDs takes less than a minute, compared to the overwrite technique used with traditional hard drives. With the Intel SSD Pro 1500 Series and the Intel SSD Pro 2500 Series, secure erase, as implemented with the Intel SSD Pro Administrator Tool, includes a block erase of the NAND flash memory and changing the cryptographic key.

Next Steps

While we have reached our intended goal of centrally managed hardware-based encryption, we continue to explore new technology that can improve user experience and IT efficiency. One such technology that we intend to soon deploy is passwordless autoboot, which stores the drive encryption password in a Trusted Platform Module (TPM) chip.[6] If during boot the system integrity is found to be retained and the system measurements remain as they were when the drive was encrypted, the drive encryption password is released automatically during the boot process.

McAfee monitors the Windows logon process. If the user enters an incorrect Windows password a certain number of times (the number is configurable by IT), the system restarts and requires the user to enter the drive encryption password after all. The drive encryption password is also required if the TPM measurements have changed since the drive was encrypted, which suggests that the drive may have been tampered with.

[6] The original equipment manufacturer must provide Trusted Platform Module (TPM) functionality, which requires TPM-supported BIOS. TPM functionality, which must be initialized, may not be available in all countries.

With passwordless autoboot, the user does not need to enter the drive encryption password; the system boots directly to Windows*. This greatly improves the user experience without significantly changing the system's security posture.

Intel® Solid-State Drive Management Tools

McAfee and Intel provide many management tools for Intel® Solid State Drives (Intel® SSDs). The following are a few examples:

- **Intel® SSD Pro Administrator Tool** is a Windows* command-line tool designed to support security and manageability settings on the Intel SSD Professional Family products.
- **Intel® Setup and Configuration Software** and related solid-state drive plug-ins help discover, enable, and manage Intel features on business client platforms that use Intel® vPro™ technology.
- **Intel® SSD Toolbox** provides information about drive properties and drive analysis.
- **Intel® Data Migration Software** assists with transitioning data from an old drive to a new Intel SSD.
- **Intel® SATA SSD Firmware Update Tool** provides the latest firmware for Intel SSDs.
- **McAfee® Drive Encryption GO** is McAfee's health-check and preflight-check tool.
- **Self-Monitoring, Analysis, and Reporting Technology (SMART)** is an industry standard that can help proactively monitor drive health.

As is often the case with maturing technology, the price of Intel SSDs has decreased significantly since 2009, making them an even better investment today. Intel provides an SSD total cost of ownership estimator at estimator.intel.com/ssdpro.

Conclusion

Our standardization on the Intel SSD Professional Family has enabled us to deploy a managed, hardware-based encryption solution that provides benefits to both users and IT. Users enjoy unimpeded performance from their laptops because hardware-based encryption does not consume CPU resources or shorten battery life. IT staff benefit because they can be confident that the encryption process is completed and that the drive remains encrypted during its lifetime.

Some older, non-Opal compliant SSDs still exist in our environment. McAfee Drive Encryption enables us to use the same agent and the same IT image for all drives—the agent checks whether the drive is Opal-compliant. If it is, hardware-based encryption is enabled. If it is not, then software-based encryption is enabled. This process is transparent to users, giving them a consistent user experience. In addition, operating and supporting the encryption solution is simple—support staff and technicians become familiar with a single solution with a minimal learning curve between supporting software-based and hardware-based encryption.

The benefits of our encryption solution include improved laptop performance, fast encryption and decryption activation, support for an environment of mixed types of SSDs, and a central console that supports compliance management and reporting. These benefits would not be possible if we relied solely on SSDs or solely on encryption management. We believe that it is the **combination** of McAfee Drive Encryption 7.1 software and Opal-compliant Intel SSDs featuring hardware-based encryption that provides the best encryption solution with which to protect Intel's intellectual property and employees' personally identifiable information.

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

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

Visit **intel.com/IT** to find content on related topics:

- Accelerating the Deployment of Intel® Solid-State Drives throughout the Enterprise paper
- Enterprise-wide Deployment of Notebook PCs with Solid-State Drives brief
- Improving Data Protection with McAfee Drive Encryption paper
- Improving the Mobile Experience with Solid-State Drives paper
- Inside IT: McAfee Drive Encryption at Intel podcast
- Managing Intel® Solid-State Drives Using Intel® vPro™ Technology paper
- The Full Mobile Deployment Benefits of Intel Solid-State Drives paper
- Validating the Reliability of Intel® Solid-State Drives brief