IT@Intel White Paper
Intel IT
IT Best Practices
Intel® vPro™ Technology
June 2012

Managing Intel® Solid-State Drives Using Intel® vPro™ Technology

Compared to software-based whole-disk encryption (WDE), our new hardware-based WDE solution improves user experience, increases encryption compliance, and reduces support issues.

Executive Overview

Intel IT has conducted a successful pilot project of our hardware-based whole-disk encryption (WDE) solution to replace our current software-based WDE solution on systems with self-encrypting drives. Compared to software-based WDE, our new hardware-based WDE solution improves user experience, increases encryption compliance, and reduces support issues. This new solution is based on two Intel technologies: self-encrypting Intel® solid-state drives (Intel® SSDs) and Intel® Active Management Technology (Intel® AMT), part of Intel® vPro™ technology.

Hardware-based WDE addresses our encryption challenges in the near term and offers the following benefits:

- Performance improvements, which can lead to greater employee productivity and job satisfaction
- Integration with our client build process, which helps us achieve our goal of 100-percent mobile platform encryption
- Fewer Service Desk calls because the encryption process is fast and easy-to-use, and users can recover their own systems
- Increased return on investment for Intel technologies already in use, and the potential for significant reduction in software license fees

The main components of our custom solution are Intel AMT-configured laptops with self-encrypting Intel SSDs and a password-management application. On the server side, the system comprises a secure password database for master passwords and other necessary data, a self-service system recovery portal, the Service Desk intranet portal, and manageability web services.

Our long-term encryption and data protection roadmap includes Opal-compliant drives and solutions. The Opal standard, published by the Trusted Computing Group, offers a set of mechanisms and protocols for self-encrypting drives (SEDs), including encryption, authentication, configuration, and policy management. While we expect to eventually deploy Opal-compliant drives and standard management software, the Opal-compliant ecosystem, including out-of-the-box solutions, is immature. In the near term, our new hardware-based WDE solution offers valuable benefits until Opal-compliant drives and software become available.

Ziv Balshai
AMT Firmware and Software Engineering Lead, Intel Architecture Group

Oded Bar-el
Client Security Engineer, Intel IT

Doug DeVetter
Technology Evangelist, Intel IT

Efi Kaufman
Client Security Product Manager, Intel IT

Omer Livne
vPro AMT 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

As the workforce is becoming more mobile, sensitive corporate data and intellectual property are increasingly at risk if the proper protections are not in place. A 2010 study revealed 329 organizations surveyed lost more than 86,000 laptops over the course of a year.[1] However, a 2009 study indicated that the costs associated with a lost laptop with encryption was almost USD 20,000 less than the cost associated with a lost unencrypted laptop.[2]

Intel IT has taken proactive steps to protect one of Intel's most critical assets—our intellectual property. Our goal is to install whole-disk encryption (WDE) on every laptop at Intel to protect the laptop's data if it is lost or stolen. In pursuit of this goal, in 2009 we deployed a software-based encryption solution. While this solution greatly improved data security, it posed several operational and business challenges.

Challenges Associated with Software-based Encryption

After deploying the software-based encryption solution on more than 70,000 systems and realizing the security benefits, we continued working to resolve the following challenges:

- **User experience.** Users perceived a noticeable performance impact because continuous encryption and decryption activity required a significant portion of the CPU computing capacity. The deployment of high-performance Intel® solid-state drives (Intel® SSDs), such as the Intel® SSD 320 Series and Intel® SSD 520 Series, mitigated the overall performance impact of using software-based WDE. However, users with PCs with software-based WDE still experienced slower performance than without encryption. In addition, the encryption set-up process was complicated and lengthy. To complete it, employees downloaded an application, performed a series of steps to set a passphrase, and then initiated the disk encryption, which could take several hours to complete and was prone to failures caused by various system errors.
- **Compliance issues.** With at least 91,500 Intel employees—the majority of which are required to have a WDE solution on their system—we found it challenging to verify that each system not only had the encryption software installed, but also that the user had completed the encryption process. And this situation is not rare, according to a 2011 Ponemon Institute survey of IT professionals, 40 percent believe employees of their organizations routinely turn off their laptops' security protection, often in violation of company policy.[3] In addition, monitoring the exact encryption state of a lost system was often not a simple task, making it difficult to tell if it was fully encrypted or not.
- **Support issues.** Because the software-based encryption solution required installing multiple software layers, problems arose during the encryption process that could be hard for IT staff to troubleshoot. Support could also be problematic if an encrypted drive became corrupted because the third-party pre-boot authentication layer added complexity to the troubleshooting process.

The software-based encryption solution was by far better than no encryption at all—its benefits outweighed these operational difficulties. However, we began to investigate newer encryption technologies that would mitigate these problems.

[1] Claburn, Thomas. "Lost Laptops Cost Billions." InformationWeek, December 02, (2010).

[2] Ponemon, Larry. "The Cost of a Lost Laptop." Ponemon Institute (2009). www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Cost%20of%20a%20Lost%20Laptop%20White%20Paper%20Final%203.pdf (PDF)

[3] Ponemon Institute, "Perceptions about Self-Encrypting Drives: A Study of IT Practitioners." (2011). www.trustedcomputinggroup.org/files/static_page_files/67318BEF-1A4B-B294-D00BDAD736433305/TCG_Ponemon_SED_Survey_Report.Final.pdf (PDF)

Hardware-Based Encryption with Remote Management

Recent technological advances in self-encrypting drives (SEDs) provided the opportunity to address the operational and business challenges we were experiencing with software-based WDE. SEDs employ an encryption engine on the drive circuitry, completely offloading the data encryption/decryption task traditionally performed by the CPU—thereby avoiding the performance overhead associated with software-based encryption.

The Security Subsystem Class: Opal, published by the Trusted Computing Group, offers a set of mechanisms and protocols for disk-drive encryption, authentication, configuration, and policy management. While waiting for the industry to develop the Opal-compliant ecosystem, which will allow us to deploy that solution—including Intel SSDs and ISV management application—we needed a solution that could manage the SSDs currently in use at Intel. These SSDs—Intel® SSD 320 Series and Intel® SSD 520 Series—are not Opal-compliant. That is, although they provide hardware-based encryption capabilities, they don't support the standard management software interface required by Opal. Therefore, we needed to develop a custom SSD management solution for hardware-based encryption.

A COMPLETE WHOLE-DISK ENCRYPTION SOLUTION USING TWO KEY INTEL TECHNOLOGIES

Almost 25 percent of Intel mobile business PCs are equipped with self-encrypting Intel SSDs. Our deployment roadmap specifies that all new mobile business PCs will be equipped with this type of drive, and the goal is to have self-encrypting Intel SSDs on at least 40 percent of our systems by the end of 2012. In addition, Intel® Active Management Technology (Intel® AMT), a component of Intel® vPro™ technology, is already 100-percent deployed on our mobile business PC fleet.

By using these two Intel technologies, we can take advantage of our existing investments, while enhancing encryption compliance across the enterprise, reducing the Service Desk support load associated with encryption, and improving the user experience.

Solution Requirements

When designing our new WDE solution, it had to be deployable on systems with self-encrypting Intel SSDs and Intel AMT.
In addition, the new solution needed to:

- Work seamlessly with existing applications and processes
- Support as many power states as possible
- Include enterprise-level recovery, support, and compliance capabilities
- Not interfere with forensics or eDiscovery processes and tools
- Comply with international export controls and local government encryption policies

In addition the solution needed to be simple for the end user to use.

Self-Encrypting Intel® Solid-State Drives (Intel SSDs)

How Self-encrypting drives (SEDs) Work: SEDs, such as the Intel® SSD 320 Series and Intel® SSD 520 Series, have a drive controller that automatically encrypts all data to the drive and decrypts all the data from the drive. The disk encryption key is never present in the computer's processor or memory, where it could be accessed by hackers. The key used to encrypt and decrypt is securely stored only on the drive. Because the disk encryption key is encrypted with the ATA (Advanced Technology Attachment) passwords, the key is made accessible to the drive only after successful user authentication; without the key the data remains encrypted on the media.

Authentication of the user is done within the SED by supplying the ATA user password, which is isolated from the OS. Therefore, attacks on OS vulnerabilities cannot affect an SED's pre-boot process.

Benefits of SEDs: SEDs offer the rugged reliability, responsive performance, long battery life, and flexibility and scalability of all Intel solid-state drives, with the added benefit of securing data. Their built-in encryption circuit alleviates the performance impact associated with a software-based WDE solution. Both the Intel® 320 Series and the Intel® 520 Series of SEDs use the Advanced Encryption Standard (AES) with 128-bit encryption, which is equal to the encryption strength of the majority of software-based WDE solutions, and complies with the widely accepted FIPS 197 industry standard.

Table 1. Components of Our New Hardware-Based Whole-Disk Encryption Solution

Component	Description
Client system	PC equipped with Intel® vPro® technology and a self-encrypting Intel® solid-state drive, such as the Intel® SSD 320 Series
Self-encrypting drive (SED) password-management application	Verifies the password's strength and enables the setting of user and master passwords on the BIOS. The application uses the user password to lock the encryption key on the Intel SSD.
Secure password database	Stores master passwords, drive serial numbers, and various statistics about the client system, security state, and data access log. Passwords in the database are encrypted. The database is hosted in the high-trust zone for maximum security.
System recovery portal	Allows employees to remotely unlock their systems through self-service.
Service Desk intranet portal	Enables Support Desk agents and other authorized personnel to perform remote actions on the managed systems as well as to retrieve data from the database.
Intel IT manageability web services	Are performed by Intel® AMT Generic Redirection Tool (Intel GRT) and are used to connect to Intel® Active Management Technology on the client PC to perform various manageability tasks. These web services are hosted on dedicated Intel IT servers. The Intel GRT provides an easy, intuitive way to perform Intel AMT tasks using very simple XML scripts. Our scripts are written for the specific BIOS types we support and probably would need customization to work on other makes and models of PCs.¬

¬ The Intel® AMT General Redirection Tool (Intel GRT) is publicly available at http://communities.intel.com/docs/DOC-6283.

Solution Components

Table 1 describes the primary components of our new hardware-based WDE solution.[4]

Key to our solution are two passwords: the user and master, which are part of the Advanced Technology Attachment (ATA) standard, used on Intel SSDs (for more details, see the sidebar on page 3). The user password is selected by the user and unlocks the PC's drive during normal use. Master passwords are system-generated strong passwords that are stored on the secure password database and used by Intel IT to unlock the drive if the user forgets the password.

How the Solution Works

Figure 1 illustrates how the solution components work together. Because the self-encrypting drive (SED) password-management application is part of our standard client build, it is typically already installed on an employee's PC. The SED application has an easy-to-use interface that explains how the password-setup process works and its requirements. For

[4] The solution can be engineered for any platform equipped with Intel® vPro technology, supported versions of Intel® AMT, and self-encrypting Intel® SSDs; we've limited our implementation to the most common platforms in use at Intel.

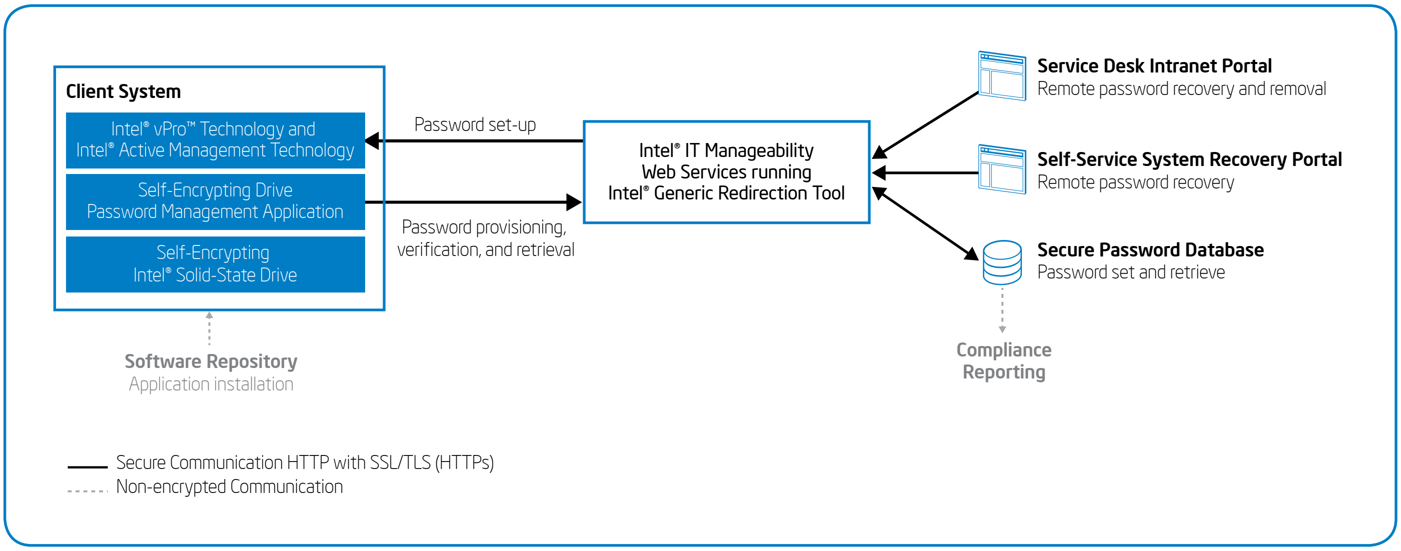

Client System
Intel® vPro™ Technology and Intel® Active Management Technology
Self-Encrypting Drive Password Management Application
Self-Encrypting Intel® Solid-State Drive
Password set-up
Password provisioning, verification, and retrieval
Intel® IT Manageability Web Services running Intel® Generic Redirection Tool
Service Desk Intranet Portal
Remote password recovery and removal
Self-Service System Recovery Portal
Remote password recovery
Secure Password Database
Password set and retrieve
Compliance Reporting
Software Repository
Application installation
Secure Communication HTTP with SSL/TLS (HTTPs)
Non-encrypted Communication

Figure 1. Our custom hardware-based whole-disk encryption solution uses two existing Intel technologies: self-encrypting Intel® solid-state drives and Intel® Active Management Technology.

example, the instructions state that the PC must be directly connected to an Intel network and not a virtual private network and that the PC must be plugged in (not on battery) during the initial setup. The application checks to see that these requirements are met before proceeding with the process.

Usually, users initiate the password setup process when they are issued their PCs in the PC Service Center. Users launch the SED password-management application and follow the steps including entering their passwords. The application verifies that the user-provided password adheres to Intel's information security and password complexity guidelines. Then, the SED application calls the Intel IT manageability web services, which communicate between the client PC and the secure password database, and sets the password in the PC BIOS. Setting the password locks the encryption key, part of the internal drive security scheme, on the client's SSD.

If a user forgets the password, the user can access a self-service system recovery portal and unlock the system remotely (similar to what a Service Desk agent would do). The user can then reset the password.

The Intel® AMT Generic Redirection Tool (GRT) interacts with the client system's BIOS to set up the user and master passwords. The Intel IT manageability web services provide an interface to the GRT and to the secure password database. The database is hosted in the high-trust zone (HTZ) for maximum security. Passwords are securely transferred using the Intel AMT serial-over-LAN interface over a Secured Sockets Layer (SSL)/Transport Layer Security (TLS) channel. No password is ever exposed.

Pilot Project

After validating the WDE capabilities in a proof of concept, we conducted a pilot project in Q1 2012. The pilot lasted six weeks and involved 200 PCs across the company worldwide. The PCs were from multiple OEMs and had either Intel SSD 320 Series or Intel SSD 520 Series. We tested all of the capabilities, including

Intel® vPro™ Technology

As shown in Figure 2, Intel® vPro™ technology—part of the latest generation of Intel® Core™ vPro™ processors—is a combination of processor technologies, hardware enhancements, management features, and security technologies that allow remote access to the PC—including monitoring, maintenance, and management—independent of the PC's OS or power state.

Intel vPro technology includes many useful features, some of which include Intel® Active Management Technology (Intel® AMT), Intel Trusted Execution Technology (Intel TXT), Intel® Virtualization Technology for Directed I/O (Intel® VT-d), and Intel® Virtualization Technology (Intel® VT-x).

Intel AMT enables better remote management of PCs by:

- Providing full control of the power state of the entire managed fleet
- Reducing costly desk-side support visits and speeds diagnosis and repair times
- Enabling remote, out-of-band management of wired and wireless PCs, even when the OS is non-functional
- Allowing Service Desk agents to remotely manage PCs using a management console.

These capabilities reduce IT costs and improve business continuity of our highly mobile PC fleet. For more in-depth information about Intel vPro technology, refer to "For More Information" at the end of this paper.

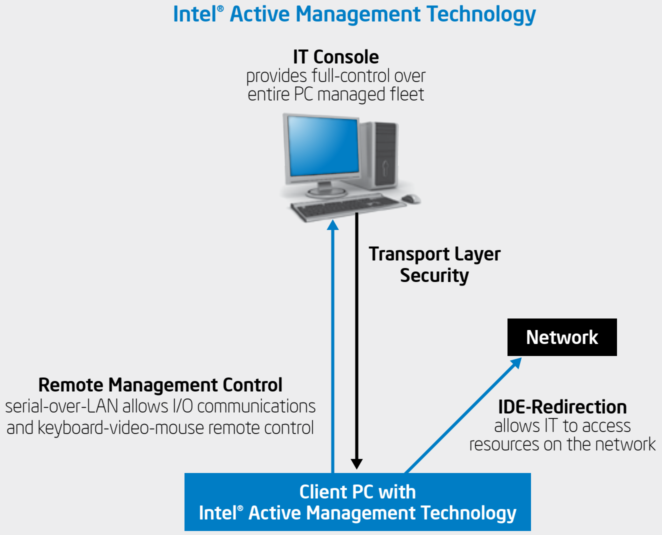

Intel® Active Management Technology
IT Console
provides full-control over entire PC managed fleet
Transport Layer Security
Network
Remote Management Control
serial-over-LAN allows I/O communications and keyboard-video-mouse remote control
IDE-Redirection
allows IT to access resources on the network
Client PC with Intel® Active Management Technology

Figure 2. Intel Active Management Technology supports efficient remote management, diagnosis, and repair.

local and remote management, use of Intel AMT, the secure database, and integration to Service Desk support tools.

Based on user feedback gathered during the pilot, we implemented several improvements. For example, we improved the user interface, and made adjustments to the SED password-management application by adding prerequisite checks, such as verifying that the client system is manageable by Intel AMT, that it is connected to the Intel network, and is plugged in to an AC power source. These checks minimize failures and errors. We also fine-tuned the XML scripts used by the Intel GRT, which may vary for each PC model.

RESULTS AND BENEFITS

Our new hardware-based encryption solution extends the functionality of Intel self-encrypting SSDs by offering a secure and manageable approach to WDE. The users appreciate the performance benefits, and we have demonstrated that the solution is technically sound and supportable.

The new solution has allowed us to avoid purchasing additional licenses and reduced our ongoing maintenance costs for our software-based encryption solution. By using existing Intel technology, such as self-encrypting Intel SSDs and Intel AMT, the new solution also increases the return on investment we've already made in these technologies.

Overall, the new solution successfully addresses our three main challenges associated with software-based WDE: user experience, compliance issues, and support issues.

User Experience

From a user's perspective, the most notable benefit of the new hardware-based WDE solution is an increase in performance of general computing tasks and of PC state transitions. For PC state transitions, for example, we measured the time it took for a system to resume from hibernation, comparing software-based WDE, SEDs, and no encryption at all on a wide variety of makes and models of PCs. A sample of this data is shown in Table 2. While software-based encryption adds approximately 20 seconds to the resume process, SEDs add no more than three seconds.

Users also appreciate how much easier this encryption process is. Once they set the password, the disk is secured instantly with no waiting for encryption to take place.

Additionally, offloading the encryption and decryption to a hardware circuit on the drive reduces the CPU load and can extend the life of the battery, enabling our highly mobile workforce more flexibility in how and where they work.

Compliance

An important advantage of self-encrypting Intel SSDs along with our new hardware-based whole-disk encryption solution is that the combination prevents security from being disabled. With SEDs and Intel AMT, users are blocked from turning off the ATA password.

Our new solution will also help us reach our goal of 100-percent encryption across our entire PC fleet. Because the encryption process is automatic, instant, and easy-to-use, and because the encryption and decryption process has almost no performance impact, employees are more likely to encrypt their disks. Also, the new solution will enhance our compliance reporting capabilities by providing better quality data about the exact encryption state of the drive—whether it is locked with user and master passwords, or not.

Support

With hardware-based encryption, the encryption process is automatic and instantaneous and one that cannot be interrupted or paused, preventing encryption from completing. We anticipate fewer Service Desk calls relating to encryption because the SED password-management application checks for prerequisite conditions, such as the client system being plugged into AC power and directly connected to the Intel network.

Also, the self-service system recovery portal enables users to unlock their client systems remotely without needing to contact the Service Desk.

We integrated the new solution into our existing back-end support tools, so that Service Desk agents can use a single console for all their support activities. We also provide training on using the solution to both employees and Service Desk agents.

Service Desk agents can remotely unlock a user's drive in case the user forgets the password, as well as reveal the master password, manually unlock a client system, and remotely remove the password from both the client PC and the database. When remotely unlocking a user's drive, the Service Desk agent is not required to expose the master or user password.

Table 2. Resume-from-Hibernation Performance Data. Intel Internal Measurements, February 2012.

Configuration	Laptop Platform A	Laptop Platform B	Laptop Platform C
Software-based Encryption	31 seconds	37 seconds	30 seconds
Self-encrypting Drive (SED)	12 seconds	16 seconds	17 seconds
No Encryption	11 seconds	13 seconds	14 seconds

NEXT STEPS

After our successful pilot, we are now ready to start deploying our hardware-based WDE solution. Currently, we have about 20,000 systems with Intel SSD 320 Series or Intel SSD 520 Series, and that number will continue to grow. We will use a phased "extended pilot" to deploy the solution.

In addition to pursuing full deployment of the solution, we are investigating several enhancements. For example, currently users can recover their passwords while disconnected from the Intel network, but are required to re-connect to the Intel network after manual recovery to finalize the process. However, as we continue our efforts to implement fast call for help (FCFH) in our Intel AMT environment, we're examining options to provide password recovery capabilities outside the Intel network.[5] The FCFH feature of Intel AMT allows Intel vPro technology platforms to initiate a secure connection to a gateway server residing in the enterprise De-Militarized Zone. Using FCFH, Intel vPro technology-based clients can be managed remotely by the IT administrator when the client system is located outside the corporate network.

Although we consider our custom hardware-based WDE solution to be highly secure, stable, and supportable, we know it is only an interim step toward our eventual goal of Opal-compliant drives and solutions. Therefore, we have chosen not to address the following technological limitations of the solution, deeming them minor enough to wait for an out-of-the-box Opal-compliant solution to be available from an ISV:

- We have to interact with the drive through the BIOS interface, rather than through direct communication with the drive. This requires writing different scripts for different PC models and sometimes even for different BIOS versions.
- Script commands, like the ones used in GRT, and timing are dependent on the BIOS version and network latency.
- Our current management capabilities using Intel AMT are limited to those exposed through the BIOS. Eventually, we want integrated inventory management and firmware update capabilities through our hardware encryption management solution.

With the knowledge we collected through our pilot project, we are continuing to collaborate

[5] Fast call for help (FCFH) is a feature of Intel® AMT that allows Intel® vPro™ technology platforms to initiate a secured connection to a gateway server residing in the enterprise De-Militarized Zone (DMZ). For more information, refer to http://software.intel.com/en-us/articles/fast-call-for-help-overview.

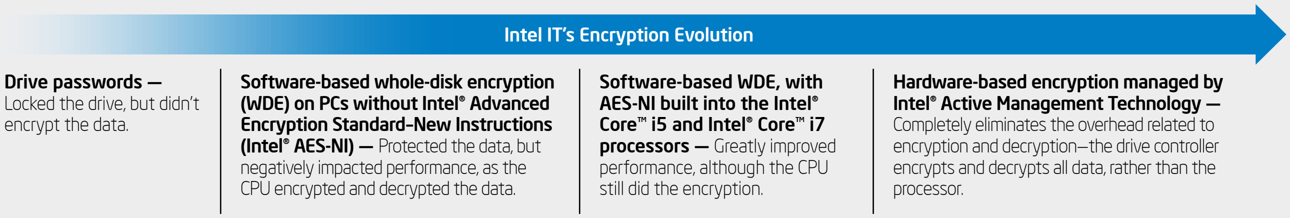
Intel IT's Encryption Evolution

Intel IT has always been committed to protecting one of Intel's greatest assets—intellectual property. As technology has changed and matured, our data protection techniques have evolved (see Figure 3), always leading to greater information security along with better business value.

The evolution will continue as standard management tools become more common for hardware-based encryption, leading to a fully Opal-compliant solution. However, we will continue to use the SED password-management application to support Intel® SSD 320 Series and Intel® SSD 520 Series as long as these drives are part of our computing environment.

The Opal-compliant solution will provide these additional benefits:

- Complete, managed WDE solutions from leading security software vendors (centralized management, password recovery, logging, user enrollment)
- Feature-rich pre-OS authentication
- OS-present management
- Seamless integration of SED management and software-based WDE in the same product, so that encryption has the same look-and-feel regardless of the technology being used.



Intel IT's Encryption Evolution

Drive passwords — Locked the drive, but didn't encrypt the data.

Software-based whole-disk encryption (WDE) on PCs without Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI) — Protected the data, but negatively impacted performance, as the CPU encrypted and decrypted the data.

Software-based WDE, with AES-NI built into the Intel® Core™ i5 and Intel® Core™ i7 processors — Greatly improved performance, although the CPU still did the encryption.

Hardware-based encryption managed by Intel® Active Management Technology — Completely eliminates the overhead related to encryption and decryption—the drive controller encrypts and decrypts all data, rather than the processor.

Figure 3. Intel IT's Encryption Evolution.

with the Intel SSD product development team to improve our support of self-encrypting drives. Also, we are working with ISVs and Intel product teams to test Opal-compliant software and hardware.

CONCLUSION

Based on a successful pilot project, Intel IT plans to gradually deploy a hardware-based WDE solution that will eventually replace our current software-based WDE solution on systems with self-encrypting drives. The new solution combines two Intel technologies—Intel self-encrypting SSDs, such as Intel SSD 320 Series and Intel SSD 520 Series, and Intel AMT (part of Intel vPro technology)—and addresses many of the operational and business challenges we have experienced with software-based WDE.

Some of the benefits of the new solution include the following:

- Faster data encryption and decryption, which will improve the user experience and help us reach our 100-percent encryption compliance goals
- Integration into our client build process, which will help us reach our goal of 100-percent mobile platform encryption
- Fewer Service Desk calls due to an automated, self-explanatory encryption process and self-service password recovery
- Increased return on investment for Intel technologies already in use in our environment, as well as the avoidance of purchasing additional licenses and reduction of our ongoing maintenance costs for our software-based encryption solution

Our long-term encryption and data protection roadmap includes Opal-compliant drives and standard management software. But in the near term, our new hardware-based WDE solution, including a custom approach to SED management, offers valuable benefits today and for several years to come.

FOR MORE INFORMATION

- "Configuration Tips for Managing Mobile PCs with Intel vPro Technology," Intel Corp., April 2012
- "Achieving Long-term Business Value with Intel® vPro™ Technology," Intel Corp., October 2010
- "New Security Solutions Using Intel® vPro™ Technology," Intel Corp., February 2009
- "Implementing Intel® vPro™ Technology to Drive Down Client Management Costs," Intel Corp., December 2008

CONTRIBUTORS

Yair Gopher
AMT Firmware and Software Engineer, Intel Architecture Group

Darren Lasko
Principal Storage Security Architect, Storage Technologies Group

James P. Slattery
Product Line Manager, Client SSD, Non-Volatile Memory Solutions Group

ACRONYMS

ATA	Advanced Technology Attachment
AES	Advanced Encryption Standard
FCFH	fast call for help
GRT	Generic Redirection Tool
Intel® AES-NI	Intel® Advanced Encryption Standard–New Instructions
Intel® AMT	Intel® Active Management Technology
SED	self-encrypting drive
SSD	solid-state drive
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WDE	whole-disk encryption

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

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.