IT@Intel White Paper

Intel IT
IT Best Practices
Intel® Solid-State Drives
June 2012

The Full Mobile Deployment Benefits of Intel® Solid-State Drives

Our Intel® Solid-State Drives deliver compelling employee benefits related to productivity, reliability, security, lifecycle, and total cost of ownership.

Doug DeVetter
Technology Evangelist, Intel IT

John Mahvi
IT PC Fleet Manager, Intel IT

Executive Overview

Intel IT has reached its goal of deploying virtually 100 percent of our approximately 91,000 mobile business PCs with Intel® Solid-State Drives (Intel® SSDs). Intel SSDs deliver compelling benefits related to employee productivity, reliability, security, lifecycle, and total cost of ownership. In fact, Intel SSDs deliver such improved performance and endurance that we now manage the SSD fleet independently from our mobile business PCs to maximize their value. By aggressively deploying the latest generation of Intel SSDs, we are realizing even greater reliability and also improving security.

Our transition to SSDs began more than four years ago, and during that time we have documented in several white papers the gains in user productivity and reductions in IT support costs. Benefits that we have recently documented include:

- Excellent reliability as evidenced by an annualized failure rate of less than one percent.
- Superb endurance – 98 percent of the Intel SSDs that have been in service from zero to four years have a 90 percent or better remaining life.
- Faster encryption performance through the introduction of Intel SSD 320 Series with hardware-based encryption.
- Improved security options and manageability through the deployment of Intel SSD-equipped mobile business PCs based on the Intel® Core™ vPro™ processor family.
- Excellent reuse benefits based on the long life of these drives and the ability to perform a secure erase in just seconds.

Based on these and other benefits realized over the years with Intel SSDs, Intel IT remains committed to maintaining our 100-percent deployment of Intel SSDs in mobile business PCs. Our goals moving forward include increasing our use of Intel® vPro™ technology to manage and secure our fleet of Intel SSD-equipped mobile business PCs, increasing the percentage of mobile business PCs with hardware-based encryption capabilities, and planning the addition of SSD-equipped Ultrabook™ devices as one of our key PC fleet offerings.

Contents

Executive Overview 1

Business Background 2

Results of Intel® Solid-state Drive Deployment 3
- Reliability 3
- Endurance 4
- Security 4

Best Practices for Reuse and Data Recovery 5
- Erasing SSDs to Prepare for Reuse 5
- Data Recovery 6

Firmware Updates and Manageability Considerations 6
- Manageability for Compliance and Policy Enforcement 6

Conclusion 7

For More Information 7

Acronyms 8

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.

BUSINESS BACKGROUND

Intel has more than 91,500 employees in 164 sites in 62 countries. Intel IT manages over 109,000 PCs and more than 80 percent of them are mobile business PCs. Starting in 2008, we began to look into the use of Intel® Solid-State Drives (Intel® SSDs) to improve data security, user productivity, and reduce total cost of ownership (TCO). After several successful pilot deployments, in 2009 we began full-scale deployment through the purchase of mobile business PCs equipped with Intel SSDs and retrofits of existing units during rebuilds and OS updates.

SSDs are data storage devices that use flash memory to store data. As a drop-in replacement for a SATA hard disk drive (HDD), SSDs can easily replace HDDs in many applications and have many advantages over them (see Table 1).

Our experience over the last five years shows that Intel SSDs help increase the productivity of Intel's highly mobile workforce through improved system performance, lower energy consumption for extended battery life, and greater drive reliability.[1]

Other advantages of SSDs include more rapid system startup and launch of OSs and applications, both of which help employees increase their productivity. Intel internal measurements show that mobile business PCs with Intel SDDs provide an average annual time savings of 27 hours per employee over those equipped with HDDs on the time taken for such tasks as booting systems, loading applications, and putting systems into standby and then awakening them.[2]

[1] A more complete discussion of Intel® Solid-State Drive (Intel® SSD) user productivity benefits and their IT advantages can be found in the IT@Intel white papers "Enterprise-wide Deployment of Notebook PCs with Solid-State Drives" and "Accelerating the Deployment of Intel® Solid-State Drives throughout the Enterprise." The latter paper provides a performance comparison that shows the 4x improvement in I/O performance that can be achieved with an Intel® Core™ vPro™ processor-based system with an Intel SSD compared to a similar system equipped with a hard disk drive. Such enhanced responsiveness is an important contributor to user experience and productivity.

[2] For full details on this study, see the Intel IT white paper "Enterprise-wide Deployment of Notebook PCs with Solid-State Drives."

Table 1. Hard Disk Drives versus Solid-State Drives

Hard Disk Drives	Solid-State Drives
▪ More fragile due to rotating platters and mechanical arms	▪ More rugged because there are no moving parts
▪ Reduced battery life due to high energy consumption	▪ Longer battery life and cooler machines due to reduced energy consumption
▪ Decreased performance as file fragmentation increases	▪ Consistent performance because fragmentation is not an issue
▪ Greater risk of data loss and hard disk failure when transported	▪ More resistant to the bumps and drops expected from mobile users
▪ Slower responsiveness and performance due to drive spin-up time and mechanical arm movement	▪ Faster responsiveness and performance due to no drive spin-up time, no mechanical arm movement, and minimal latency

Our deployment of mobile business PCs with Intel SSDs consisted of four phases.

- **Phase 1 - Early Intel SSD introduction and funded upgrades.** This phase involved our initial research and benchmarking, as well as a pilot deployment.
- **Phase 2 - Initial proliferation.** This stage started with the distribution of 8,000 units and a refined study of their TCO benefits. From this study, we found that Intel SSDs did indeed reduce TCO, which led us to expand their deployment and make them a key element of our standard configuration. We also made Intel SSDs a key enhancement in our retrofits during OS upgrades to Microsoft Windows* 7.
- **Phase 3 - Standardization.** Based on the successes of the two previous phases, we specified Intel SSDs in all new mobile business PCs and made them a part of any rebuild related to breakage or repair. In this phase, nearly 40,000 Intel SSDs were deployed.
- **Phase 4 - Full deployment.** This phase, with the goal of 100-percent deployment, completed our transition to Intel SSDs. Moving forward, our plan is to continue deploying mobile business PCs with Intel SSDs, taking advantage of each new generation as it becomes available, with an increased interest in leveraging the security and manageability features of these products.

Currently, Intel IT supports 61 make and model combinations of mobile business PCs from 10 unique hardware suppliers. We equip 100 percent of our mainstream mobile business PCs with an Intel SSD, and these PCs are also equipped with Intel® vPro™ technology for improved manageability and security.

RESULTS OF INTEL® SOLID-STATE DRIVE DEPLOYMENT

We find the inclusion of an Intel SSD in an Intel® Core™ vPro™ processor-based mobile business PC produces a platform popular with employees for its performance, responsiveness, and overall productivity benefits. In addition, these platforms deliver compelling IT advantages, particularly with regard to reliability, endurance, and security—all of which help contribute to a lower TCO.

Reliability

Reliability is a key factor in realizing reduced TCO from SSDs in a mobile platform. With no moving parts, SSDs bring a natural resistance to failure due to impact or vibration, making shock-sensor software and its performance overhead and tuning requirements unnecessary. We found that the compute-quality NAND (short for "NOT AND") and validated firmware met our needs to provide stable, predictable performance and consistent data integrity for our users.

Based on our studies, the reliability of Intel SSDs resulted in fewer support calls and out-of-warranty drive replacements, which translated into direct IT savings. In our experience, Intel SSDs consistently reduce downtime compared to HDDs. Recently we investigated drive reliability through an industry-standard measure: annualized failure rate (AFR). A lower AFR can help reduce TCO, as reliability increases user uptime and saves IT the time and expense in troubleshooting and rebuilding laptops. We estimate each drive failure can cost IT from two to 12 hours of repair time and can involve several support calls to answer user questions about the initial failure and the reconfiguration process.

Benefits of Standardization on a Single Solid-State Drive Supplier

From an IT standpoint, standardizing on a single drive supplier has many advantages, particularly with regard to streamlining selection, testing, and support. By standardizing on Intel® Solid-State Drives, Intel IT realizes the following benefits:

- Common drive management and firmware update tools and techniques
- Reduced drive compatibility testing in our supported PC models
- Easier validation and management of drive encryption
- Easier troubleshooting because of established familiarity with the product
- Logistics benefits related to inventory management and handling
- Easier testing for everything from performance to remaining drive life

Our results, based on two years of monitoring, show excellent Intel SSD reliability as evidenced by an AFR of less than one percent over the two-year span. This is far better than the AFR for HDDs of 4.85 percent that we calculated for our mobile business PCs in 2007.[3]

In cases of possible failure, we use a proprietary set of tools to analyze the drive. If analysis detects a failure, we log the cause and destroy the drive. If a drive passes, we log the test, then wipe and reuse the drive. SSD health can also be monitored through the Intel® Solid-State Drive Toolbox (Intel® SSD Toolbox), a free toolset available at www.intel.com/go/ssdtoolbox.

REACHING NEW LEVELS OF RELIABLITY WITH NEXT GENERATION INTEL SOLID-STATE DRIVES

Our SSD AFR results were from a previous generation Intel SSD. Analyzing the results, we traced most of the issues we experienced to NAND failures and unplanned system power losses. These potential points of failure have been addressed through product improvements incorporated in the Intel SSD 320 Series. These improvements include the use of the latest compute-quality Intel 25nm NAND flash memory, plus a design that enhances reliability through the use of an array of extra NAND flash memory. If the controller on one of these drives encounters a faulty NAND array, the drive can automatically reconfigure itself to reduce the potential for data loss and drive failure. In addition, to protect against data loss when a system loses power unexpectedly the Intel SSD 320 Series is designed with capacitors that provide enough stored energy for the SSD to write cached data to the NAND.

Based on our analysis of these improvements, we are deploying Intel SSD 320 Series for new PCs and replacement of lower capacity drives. We expect to realize increased reliability over the great reliability we have experienced with the earlier generations of Intel SSDs.

Endurance

In all drives, endurance is a key aspect of reliability and TCO. The longer a drive is useful, the more value an organization gains from it. The main factors determining the life span of HDDs are mechanical. The most frequent life-ending event is a head crash where the actuator arm physically contacts the disk platter causing data loss. Over time, other components simply wear out: platters vibrate due to bearing wear, actuators lose precision, and lubricants evaporate. The result is more retries, more corrupted data requiring error correction code recovery, higher drive temperatures, greater power draw, and eventually failure.

In our experience, with no mechanical parts Intel SSDs are so reliable they can outlast the productive life of our mobile business PCs. In other words, when it becomes time for Intel IT to refresh a PC to take advantage of the productivity and manageability advances of a next generation processor, the SSD still has lots of life in it. Intel IT typically refreshes mobile business PCs on an approximately two- to four-year refresh cycle.

To monitor SSD wear, Intel IT uses E9 Self-Monitoring, Analysis and Reporting Technology (SMART). Commonly known as the Media Wearout Indicator, SMART's wearout indicator starts at a normalized value of 100 when the SSD is new and decreases in value as the NAND erase cycles increase toward the maximum-rated cycles. A variety of diagnostic tools are available to read SMART attributes. For Intel SSDs, SMART attributes can be read using the Intel SSD Toolbox.

Based on our use of the Media Wearout Indicator, we show that 98 percent of the Intel SSDs that have been in service from zero to four years have a remaining lifetime of 90 percent or better.

Because of the long life of Intel SSDs, we have started to manage them separately from the original PC in which they were purchased or deployed. This facilitates our reuse of them and our tracking of their useful lives through the Media Wearout Indicator as they move from one machine to another. The long life of the SSDs and our reuse of them help us amortize their cost over a longer period of time in comparison to HDDs. The result is an ever greater effect in helping us reduce the TCO of our mobile business PC fleet.

Security

To enhance security and better protect one of Intel's most critical assets—our intellectual property (IP)—in 2009 Intel IT began deploying software-based whole-disk encryption (WDE) on our mobile business PCs with SSDs. The faster I/O performance of SSDs over traditional HDDs helped mitigate the performance impact of this advanced security method. We conducted benchmark tests in 2010 comparing a mobile business PC based on an Intel Core vPro processor and equipped with an Intel SSD against the same system equipped with a HDD, both performing WDE. Results for the PC equipped with an Intel SSD showed a 4x advantage in I/O performance.

We achieved further improvement in encryption and decryption when we began using the Intel SSD 320 Series, which provides higher I/O performance, and Intel® processors supporting Intel® Advanced Encryption Standard - New Instructions (Intel® AES-NI). Intel AES-NI, introduced with previous generation Intel Core processors, accelerates encryption and decryption to minimize application performance concerns inherent in cryptographic processing.

Deploying SSDs with software-based WDE helped us met our information security objectives and still provide better overall system performance compared to an unencrypted HDD. As of July 2012, we had almost all eligible mobile business PCs with Intel SSDs deployed with software-based WDE.

Software-based WDE continues to be a good practice for mobile business PCs because it keeps data safe in an unintelligible form

[3] Reliability results from a study completed in May 2012 of 69,000 Intel® Solid-State Drives installed in our mobile business PC fleet. This is an update to the study documented in the IT@Intel brief "Validating the Reliability of Intel® Solid-State Drives."

should the PC be lost or stolen. However, there are some limitations with software-based WDE. These include:

- **Consumption of a portion of the CPU computing capacity.** The extra processor workload diminished to some extent the high data transfer rates of SSDs that contribute to its higher user productivity. Our users perceived an I/O performance impact from the continuous encryption and decryption activity.
- **A complicated and time-consuming setup process.** Employees who were issued a new PC had to download software, set up a passphrase, and start an initial encryption of the drive that could take several hours.
- **Difficulty checking and maintaining employee compliance with our encryption policy.** Since an employee could turn off the encryption feature, it was difficult to ensure compliance.
- **Difficulty in troubleshooting.** The software-based encryption solution required installing multiple software layers. This sometimes led to problems during the encryption process that were difficult for IT staff to troubleshoot. Support could also be problematic if an encrypted drive became corrupted because of the complexity that the third-party pre-boot authentication layer added to the troubleshooting process.

IMPLEMENTING HARDWARE-BASED WHOLE DISK ENCRYPTION

To mitigate performance, compliance, and manageability issues with encryption, we investigated hardware-based encryption and remote management capabilities. Our first step was to perform a pilot study using two Intel® technologies: self-encrypting Intel® SSDs and Intel® Active Management Technology (Intel® AMT), a key component of Intel vPro technology.[4]

The Intel SSD 320 Series offers a hardware-based SSD encryption feature implemented using the Advanced Encryption Standard (AES). The Intel SSD 320 Series' 128-bit AES encryption works right out of the box. There's nothing to download or configure.

The advantage of hardware-based encryption is that the drive controller instead of the processor encrypts and decrypts all data. This eliminates the CPU overhead related to encryption and decryption. An added advantage of offloading the encryption and decryption to the drive controller is that it can extend the life of the computer's battery by lowering CPU utilization. This gives our highly mobile workforce more flexibility in where and how long they work.

A custom management solution based on Intel AMT was used to automate the password management process, including setup, provisioning, verification, and retrieval.

This pilot proved a success. Hardware-based WDE preserved SSD performance benefits and made encryption fast, automatic, and transparent. Intel IT is now deploying our hardware-based WDE solution on newly deployed, eligible systems. We currently have about 20,000 eligible mobile business PCs deployed and will migrate these systems to the new solution in stages. An important advantage of this solution is that the user is prevented from disabling the ATA (Advanced Technology Attachment) user password, thus users cannot disable the encryption. Deploying this solution will help us reach our goal of 100-percent encryption compliance across our mobile business PC fleet.

BEST PRACTICES FOR REUSE AND DATA RECOVERY

The reliability, durability, and endurance of Intel SSDs have presented Intel IT with a unique opportunity to further reduce the TCO of our mobile business PCs through reuse of our Intel SSDs.

Because of the IP and other sensitive information on each drive, the safe reuse and eventual disposal of these drives require the development and adherence to a number of best practices.

Intel has a "no drive leaves Intel" policy. For internal reuse, drives must be reliably wiped clean of all data so that nothing previously on the drive is recoverable. The ability to wipe a disk clean for reuse extends the value of the drive. With many Intel SSDs in service now for four years or more, and the mobile business PCs they're in being refreshed or retired, we now have the opportunity to reuse these SSDs within the organization. We're currently reusing or considering reusing these drives in a number of ways.

- Replacement drives for mobile business PCs
- Special projects
- Lab use
- Desktop retrofits or supplementary drives

To safely reuse these SSDs, we do the following:

- Manage and track SSDs independent from the mobile business PC in which they start out.
- Assess drive wear through the Media Wearout Indicator. If testing reveals a suboptimal drive for any reason, we shred the SSD as we do all failed drives.
- Wipe all reusable drives (see next section) to clear them of all previous data before any type of internal reuse.

Erasing SSDs to Prepare for Reuse

Reliably erasing data from storage media—sanitizing the media—is a critical component of secure data management. While sanitizing entire disks and individual files is well understood for HDDs, SSDs have a very different internal architecture. In the initial phases of adopting SSDs, we were able to standardize on a single disk-wiping software product for both SSD and

[4] For the complete study, see "Managing Intel® Solid-State Drives Using Intel® vPro™ Technology."

HDD erasing. The software we used did an excellent job of rendering drives to exclude any possibility of future recovery of deleted folders and files. However, the actual disk wipe could take several hours.

We have been investigating using ATA Secure Erase, which along with Enhanced Secure Erase are part of the security features in the ATA specification, for a number of years. Because we no longer have to wipe HDDs, we can now standardize on Secure Erase as our disk sanitization solution. Intel IT plans to use a proprietary tool to perform Secure Erase, but it can also be performed using the Intel SSD Toolbox. The Secure Erase operation takes only seconds to complete.

Data Recovery

Though more reliable than HDDs, SSDs can fail for a variety of reasons. Because the technology is different that that of HDDs, data recovery on SSDs is still a new and relatively immature industry. Consequently, we rely on regular data backups for all employees from an IT-provided network backup system.

To further ensure against drive failure, Intel IT has chosen to purchase only high-quality drives with built-in reliability features. We use tools such as the Media Wearout Indicator, as described earlier, before reusing any drive in another system, and we are constantly refining our methods to proactively identify and replace potentially problematic drives.

FIRMWARE UPDATES AND MANAGEABILITY CONSIDERATIONS

Now that Intel vPro technology is fully deployed on our mobile business PC fleet, Intel IT is looking at ways to use more of Intel AMT's remote out-of-band capabilities to improve support to our worldwide customers and further reduce TCO.

Firmware is an important component of an SSD, impacting performance, reliability, and security. SSD firmware is something we check and update along with BIOS and drivers as a part of an OS build process or any time a mobile business PC comes in for support. We find that by buying systems with OEM-qualified Intel SSDs, we only need to perform SSD firmware updates if a supplier says the upgrade is due to a major defect.

Intel IT's service center support model makes it easy for an employee to bring in a mobile business PC if a firmware update is necessary. We perform a number of checks to verify the health of the PC and verify that its data is being regularly backed up on our network. We also use Intel's publicly available firmware update tool, the Intel® SATA Solid-State Drive Firmware Update Tool (available at http://downloadcenter.intel.com/Detail_Desc.aspx?agr=Y&DwnldID=18363), to ensure the SSD firmware is current. Employees can also access this tool or the Intel SSD Toolbox.

Manageability for Compliance and Policy Enforcement

The Trusted Computing Group has a new specification, the Security Subsystem Class: Opal*, which applies to storage media such as self-encrypting drives (SEDs). The Opal standard provides a set of mechanisms and protocols for SEDs, including encryption, authentication, configuration, and policy management. Currently the Opal-compliant ecosystem is in an early phase. Intel IT has begun evaluating Opal-compliant drives and standard management software, and expects to begin deployment as soon as 2013 (see Figure 1).

In the meantime, based on the pilot study we conducted and described in "Managing Intel® Solid-State Drives Using Intel® vPro™ Technology," we developed a successful custom SED management solution. The main components of the new system are Intel AMT-provisioned mobile business PCs with the Intel SSD 320 Series and an SED password-management application. On the server side, the system uses a secure database for master passwords and other necessary data, a self-service user password recovery portal, the Service Desk intranet portal, and manageability web services.

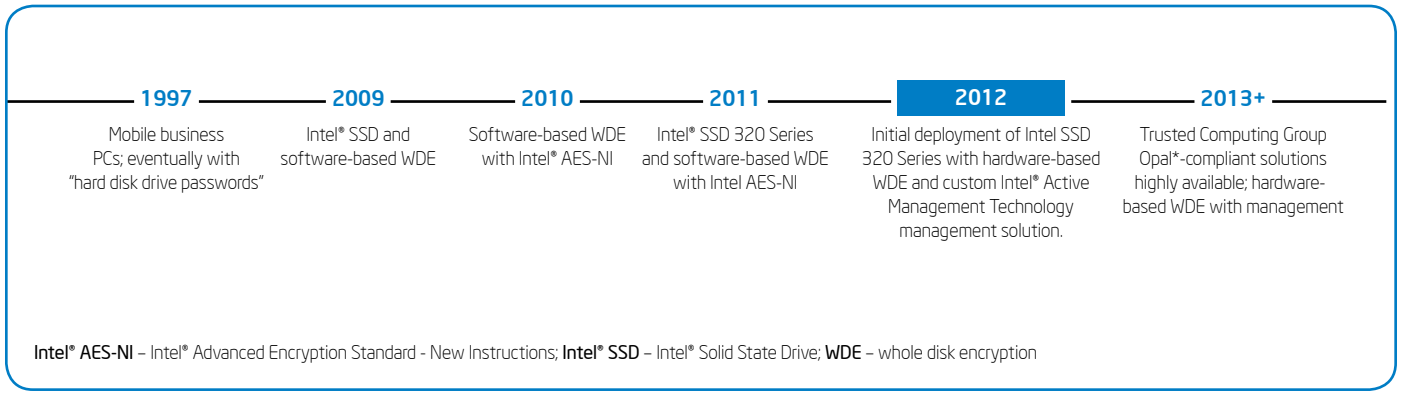

Figure 1. Timeline showing the evolution in Intel IT's deployment of solid-state drives, advanced data protection, and remote manageability for Intel's fleet of mobile business PCs.

This interim solution addresses our current manageability challenges with encryption and offers the following benefits:

- 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 passwords. Service Desk agents can also remotely unlock a user's drive in case a password is forgotten and manually unlock the system without exposing the master or user password.
- Increased return on investment for Intel® technologies already in use.
- Better compliance—with SEDs and Intel AMT, users cannot turn off the ATA password and thus are unable to disable encryption.

CONCLUSION

With virtually 100 percent of our mobile business PCs now deployed with Intel SSDs, Intel employees benefit from the productivity advantages of faster PC performance and greater reliability. Equally important, with Intel SSDs Intel IT achieves its TCO reduction goals, reaping the advantages of their high reliability, endurance, and data security features.

The latest generation of Intel SSDs, the Intel SSD 320 Series, provides especially strong reliability and security advantages. The combination of their hardware-based WDE capability and our mobile business PCs' Intel vPro technology (particularly the remote management features of Intel AMT) enables us to improve encryption compliance and performance.

While our long-term encryption and data protection roadmap includes introducing Opal-compliant drives and solutions, our current solution provides substantial advantages and we expect to deploy it in all eligible systems.

Intel SSD endurance continues to provide valuable reuse opportunities as replacement drives for mobile and desktop PCs, as well as for project and lab use. We look forward to upcoming improvements in data recovery techniques for SSDs and even greater TCO savings by the further enhancement of our remote manageability capabilities through deployment of Opal-compliant drives and greater use of Intel AMT.

FOR MORE INFORMATION

Visit www.intel.com/it to find white papers on related topics:

- "Accelerating the Deployment of Intel® Solid-State Drives throughout the Enterprise"
- "Configuration Tips for Managing Mobile PCs with Intel® vPro™ Technology"
- "Enterprise-wide Deployment of Notebook PCs with Solid-State Drives"
- "Improving the Mobile Experience with Solid-State Drives"
- "Managing Intel® Solid-State Drives Using Intel® vPro™ Technology"
- "Validating the Reliability of Intel® Solid-State Drives"

Drive Capacity

Intel IT currently issues 120-gigabyte (GB) Intel® Solid-State Drive 320 Series for new deployments to most office employees, with other employee segments receiving higher capacity drives due to business need. In our experience, employees better manage their data with smaller drive capacities, deleting unnecessary documents and other data more frequently. With large drive capacities, there is a tendency to never delete data and to simply keep accumulating it.

As the cost of solid-state drives continues to drop and data sizes grow, we will revisit our standardization on the 120-GB capacity. In addition, as cloud services grow, the need for larger capacity drives in mobile business PCs may diminish.

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

CONTRIBUTORS

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

ACRONYMS

AES	Advanced Encryption Standard
AFR	annualized failure rate
ATA	Advanced Technology Attachment
HDD	hard disk drive
Intel® AMT	Intel® Active Management Technology
IP	intellectual property
P/E	program/erase
SED	self-encrypting drive
SMART	Self-Monitoring, Analysis and Reporting Technology
SSD	solid-state drive
TCO	total cost of ownership
WDE	whole-disk encryption