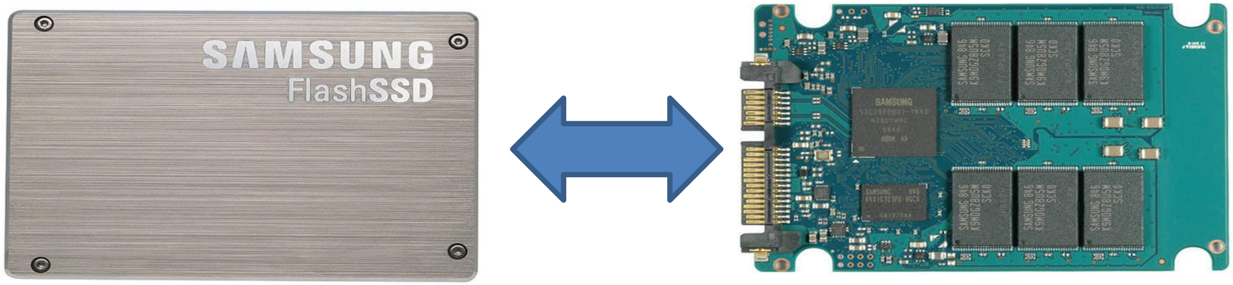


2nd Annual NSA TRUSTED COMPUTING Conference & Exposition

Using COTS Technologies to Deliver Decisive Defensive Advantage

Solid-State Drives with Self-Encryption:
Solidly Secure

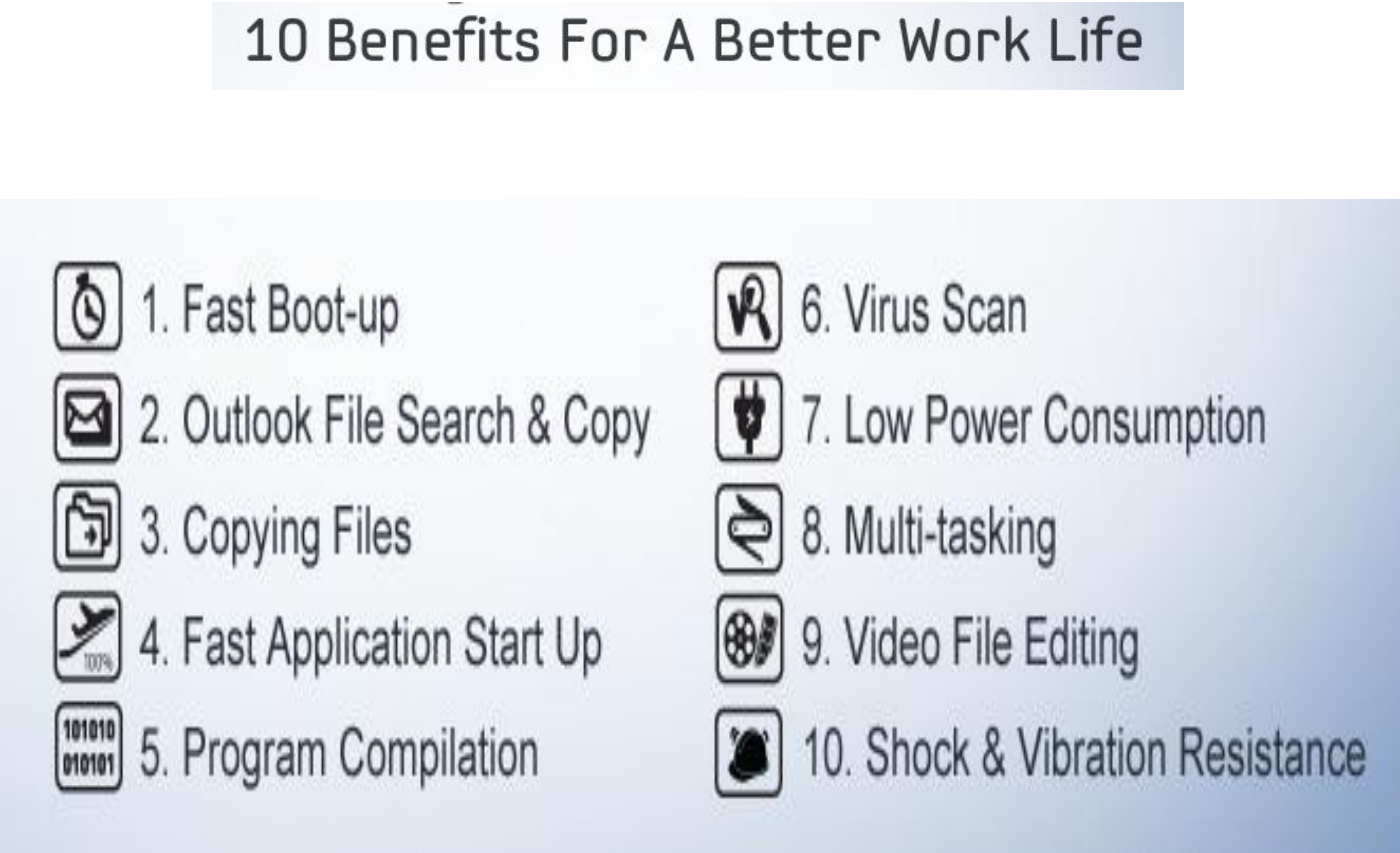
Michael Willett

Storage Security Strategist

SAMSUNG

09/22/2011

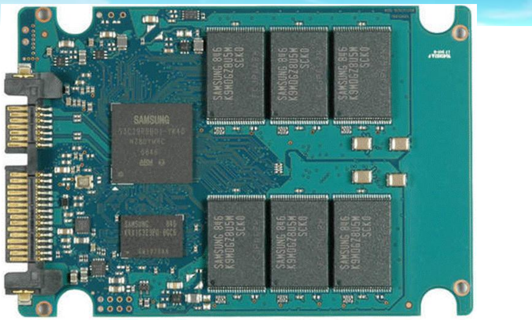
SOLID STATE DRIVES



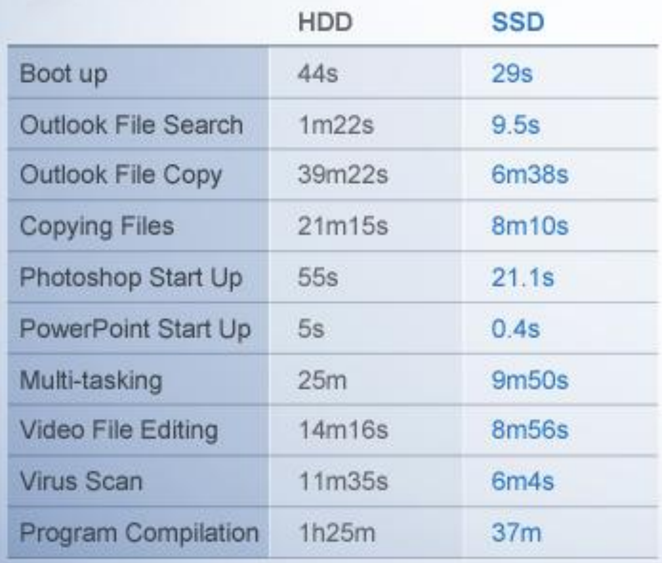
10 Benefits For A Better Work Life

1. Fast Boot-up
2. Outlook File Search & Copy
3. Copying Files
4. Fast Application Start Up
5. Program Compilation
6. Virus Scan
7. Low Power Consumption
8. Multi-tasking
9. Video File Editing
10. Shock & Vibration Resistance

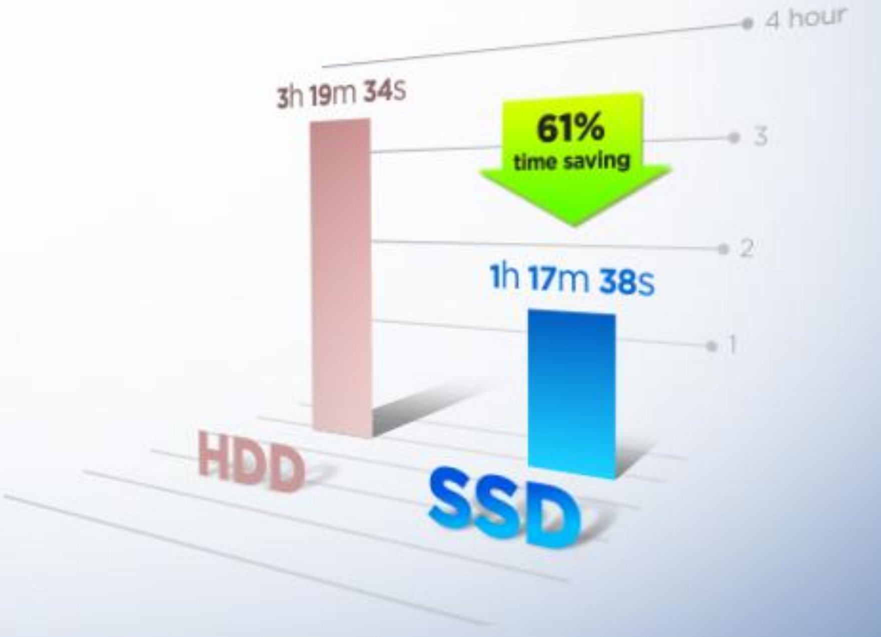
For a Better Work Life



SSD can save up to 61% of your work hour.



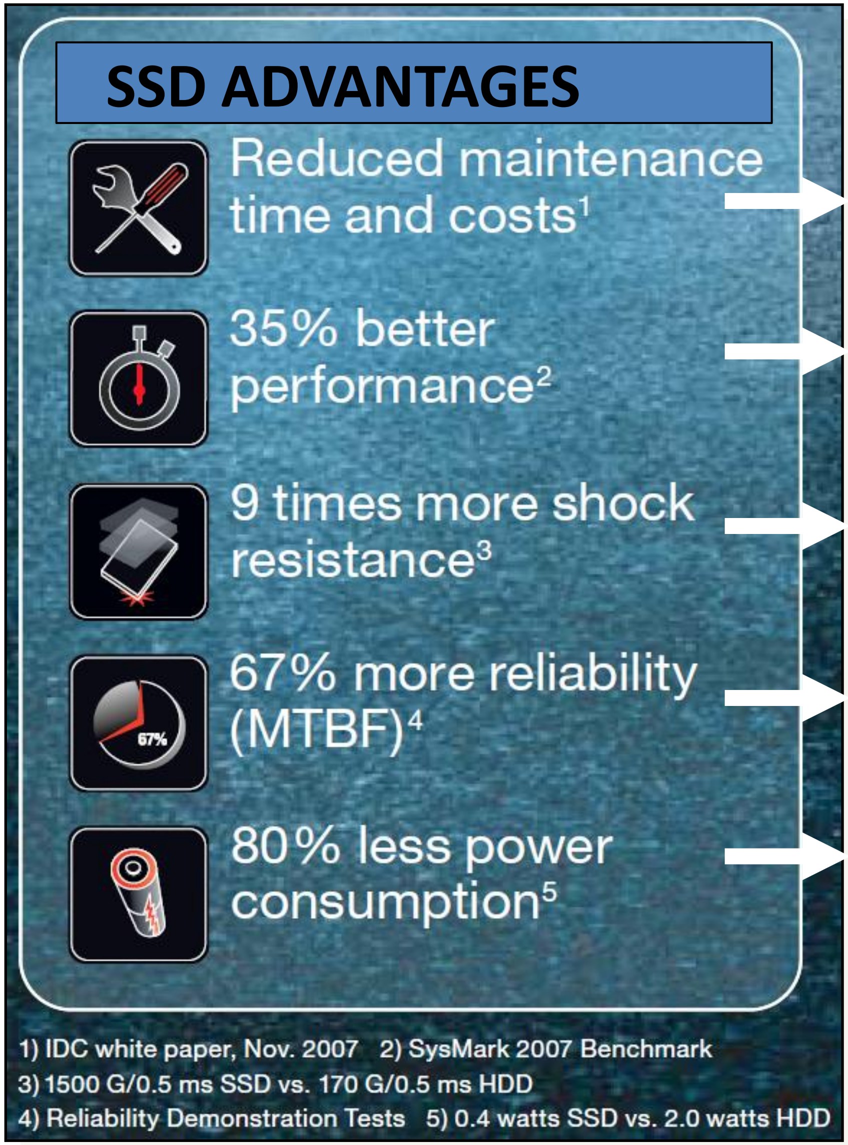
	HDD	SSD
Boot up	44s	29s
Outlook File Search	1m22s	9.5s
Outlook File Copy	39m22s	6m38s
Copying Files	21m15s	8m10s
Photoshop Start Up	55s	21.1s
PowerPoint Start Up	5s	0.4s
Multi-tasking	25m	9m50s
Video File Editing	14m16s	8m56s
Virus Scan	11m35s	6m4s
Program Compilation	1h25m	37m



Test Environment : Windows Vista, Intel Core2Duo 2.4GHz, 2GB DDR2, ICH9M-E

Solid-State Drives

SOLID STATE DRIVES



SSD ADVANTAGES

- Reduced maintenance time and costs[1]
- 35% better performance[2]
- 9 times more shock resistance[3]
- 67% more reliability (MTBF)[4]
- 80% less power consumption[5]

[1] IDC white paper, Nov. 2007 [2] SysMark 2007 Benchmark

[3] 1500 G/0.5 ms SSD vs. 170 G/0.5 ms HDD

[4] Reliability Demonstration Tests [5] 0.4 watts SSD vs. 2.0 watts HDD

Save $$ on IT cost (TCO)

+

Faster booting and application launching

+

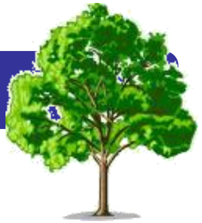
Shock proof

+

Fewer drive crashes

+

Energy efficient and Green



=

Right Solution

IDC Study
Reduced Cost of an SSD-based PC

True cost of an IT asset = direct + indirect costs over the life span

Cost factors:

- **Acquisition**
- **Deployment**
- **Performance**
- **Support and maintenance**
- **Retirement**

Example savings: SSD-based notebook PC: **improved reliability** = 35%, or **$30 per user per year**, reduction in lost productivity. Improved reliability **reduces the annual IT labor costs** to evaluate, fix, and/or replace failed or improperly working disks. The cost savings over HDD-based PCs is estimated to be 80%, or **$16 per user per year**.

Cost savings result from:

- **increased user productivity**
- **higher reliability**
- **reduction of costs associated with support**
- **maintenance and retirement**
- **power savings**

adding all of these cost benefits together….

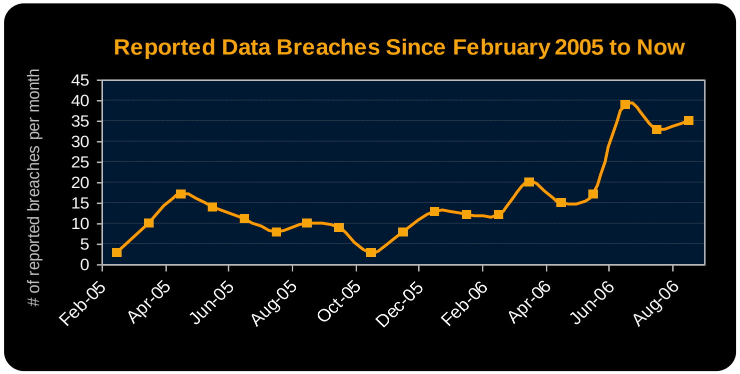
Annual cost reduction up to $176/user annually

http://www.samsung.com/global/business/semiconductor/products/flash/ssd/2008/down/evaluating_total_cost.pdf

WHY ENCRYPT STORED DATA?

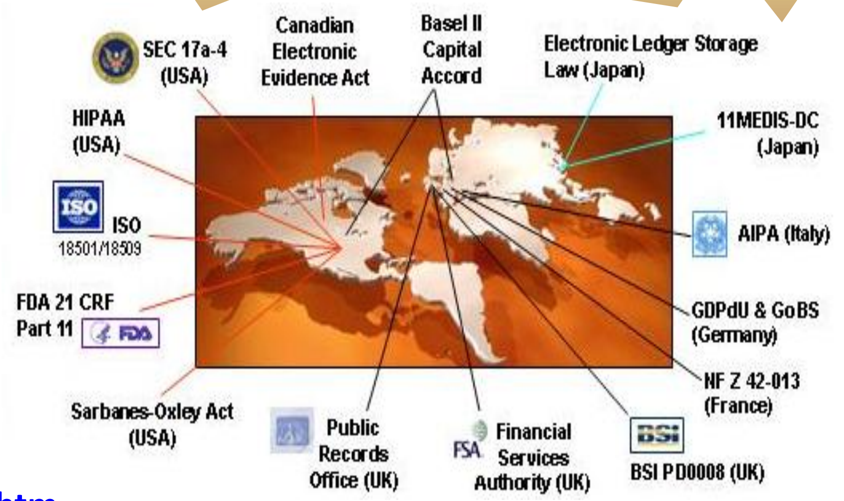
The Problem…

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches



In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record)

$6.65 Million Per Incident



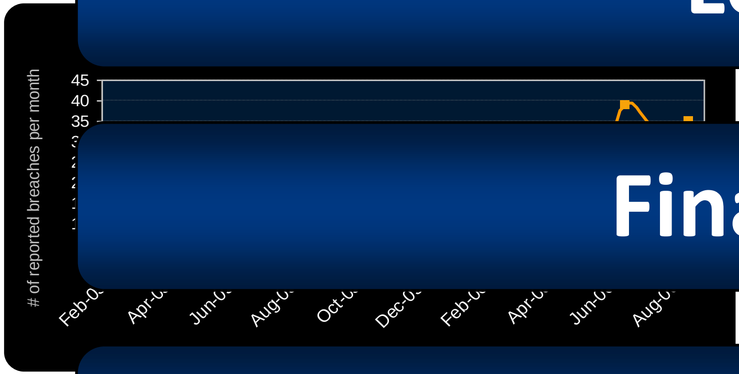
http://www.privacyrights.org/ar/ChronDataBreaches.htm

WHY ENCRYPT STORED DATA?

The Problem…

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches

Legal



…was $6.65 million per affected corporation ($202 per record)

…ident

Financial

SEC 17a-4 (USA)
Electronic Evidence Act
Capital Accord
Electronic Ledger Storage Law (Japan)
11MEDIS-DC (Japan)
AIPA (Italy)
GDPdU & GoBS (Germany)
NF Z 42-013 (France)
BSI
BSI PD0008 (UK)
FSA
Financial Services Authority (UK)
Public Records Office (UK)
Sarbanes-Oxley Act (USA)
FDA 21 CRF Part 11
FDA

Reputation

http://www.privacyrights.org/ar/ChronDataBreaches.htm

WHY ENCRYPT STORED DATA?

Threat scenario: stored data leaves the owner's control – lost, stolen, re-purposed, repaired, end-of-life, …

- Compliance
  - **46+ states have data privacy laws with encryption safe harbors**
  - **New federal data breach bills + EC breach notification directive**
- Data center and laptop drives are mobile (HDD, SSD)
- Exposure of data loss is expensive ($6.65 Million on average per incident[1])
- Obsolete, Failed, Stolen, Misplaced…
  - **Nearly ALL drives leave the security of the data center**
  - **The vast majority of decommissioned drives are still readable**

[1] Ponemon Institute, Fourth Annual US Cost of Data Breach Study – Jan 2009 www.ponemon.org

Self-Encrypting Drives (SED)

- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cuts Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent

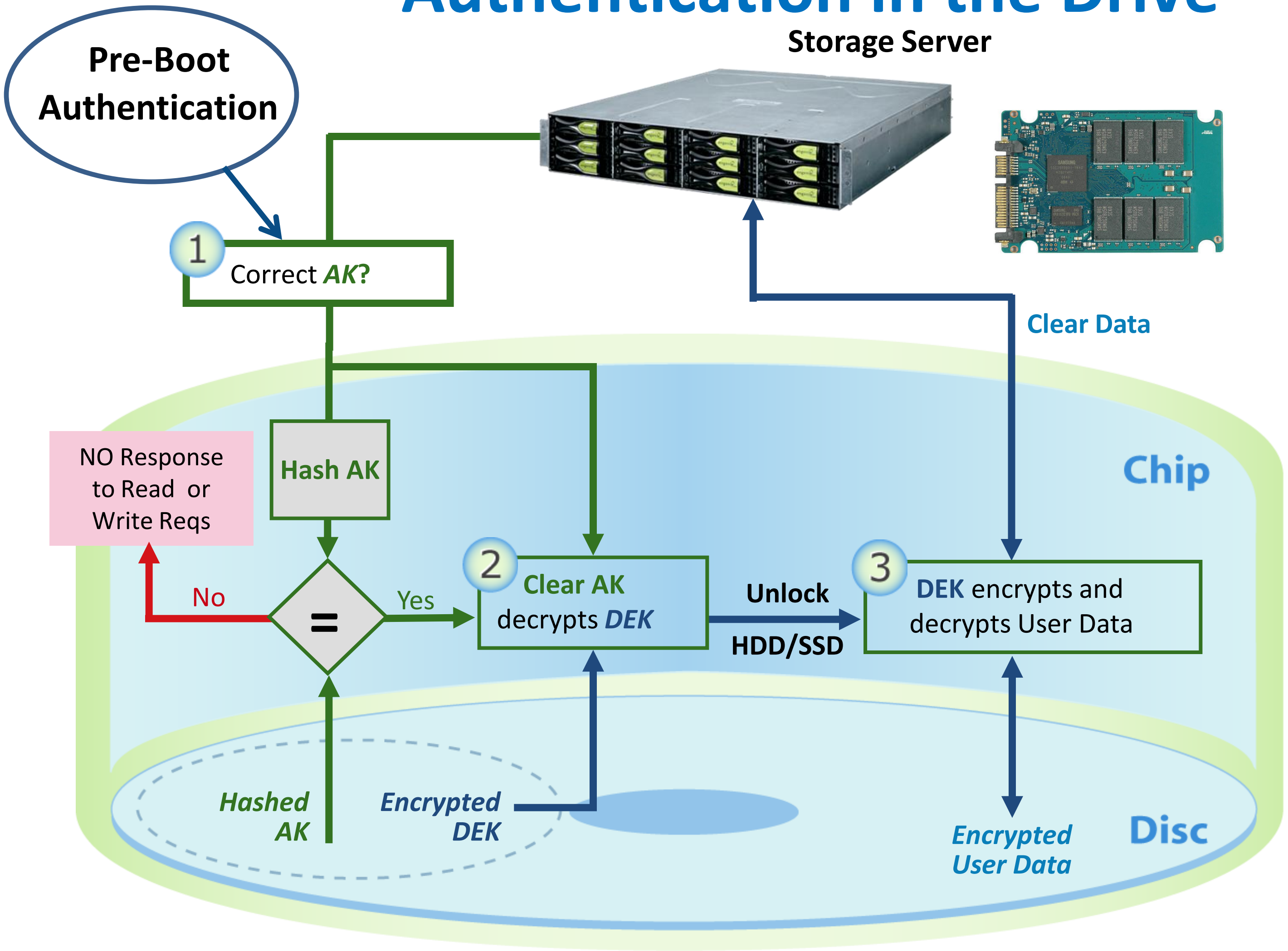
> “Many organizations are considering **drive-level security for its simplicity** in helping secure sensitive data through the hardware lifecycle from initial setup, to upgrade transitions and disposal”
>
> **Eric Ouellet**
> **Research Vice President**
> **Gartner**

Trusted Storage Standardization

TRUSTED COMPUTING GROUP™

Published Storage Specifications

Authentication in the Drive



AK
Authentication Key

DEK
Data Encryption Key

SSD Erasure – Can it be?

"… none of the existing hard drive-oriented techniques for individual file sanitization are effective on SSDs…"

"… reliable SSD sanitization requires **built-in**, verifiable sanitize operations…"

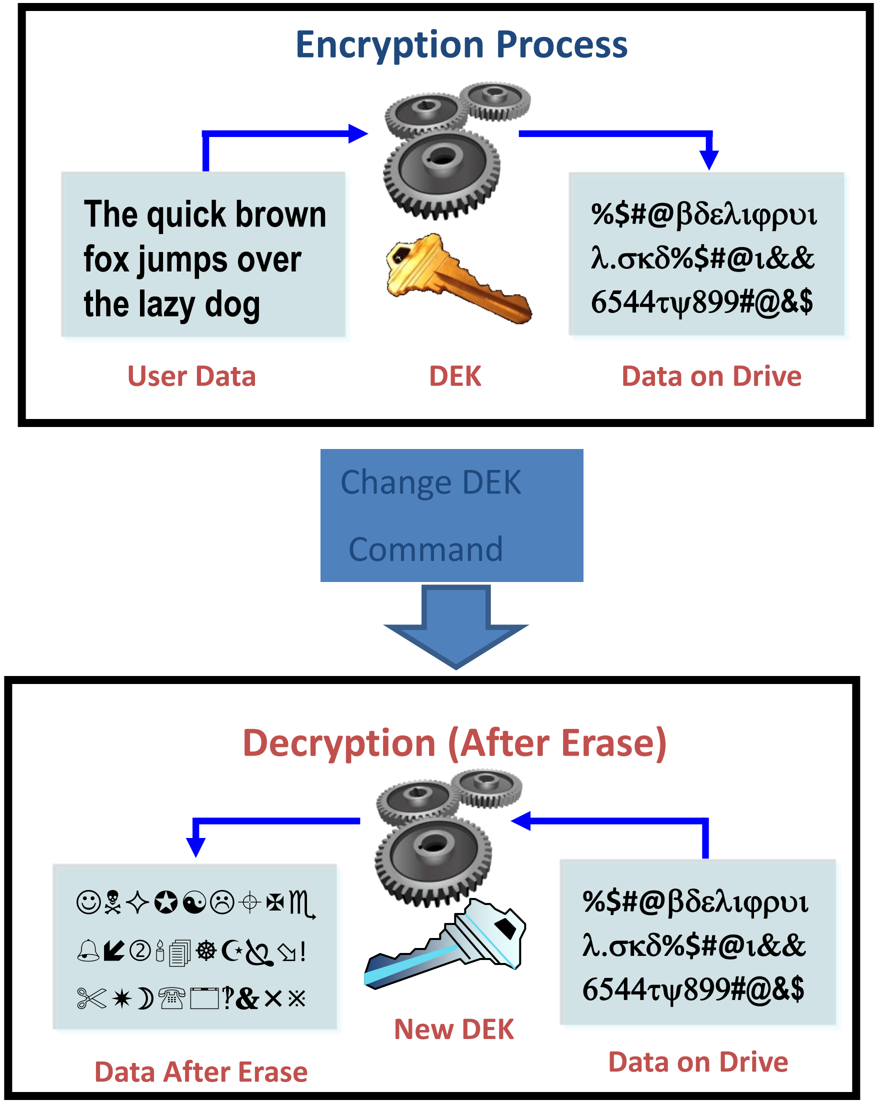
"… Flash-based solid-state drives (SSDs) differ from hard Drives (flash chips vs. magnetic disks) … maintain a layer of indirection (FTL) between the logical block addresses … and the raw flash addresses that identify physical storage. The FTL enhances SSD performance and reliability, but it can also produce copies of the data that are invisible to the user but that a sophisticated attacker can recover… "

http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf

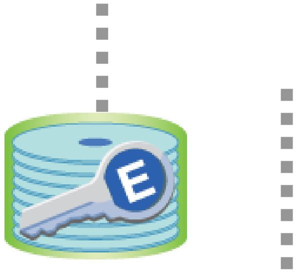
Cryptographic Erase

- Description
  - Cryptographic erase changes the drive encryption key
  - Data encrypted with previous key, unintelligible when **DEcrypted** with new key
- Benefits
  - Instantaneous "rapid" erase for secure disposal or re-purposing

- **T13/ATA: Crypto Scramble Ext (ACS-2)**
- **T10/SCSI: Cryptographic Erase (SBC-3)**


Encryption Process
The quick brown fox jumps over the lazy dog
%$#@βδελιφρυι λ.σκδ%$#@ι&& 6544τψ899#@&$
User Data
DEK
Data on Drive
Change DEK Command
Decryption (After Erase)
%$#@βδελιφρυι λ.σκδ%$#@ι&& 6544τψ899#@&$
New DEK
Data After Erase
Data on Drive

No Performance Degradation



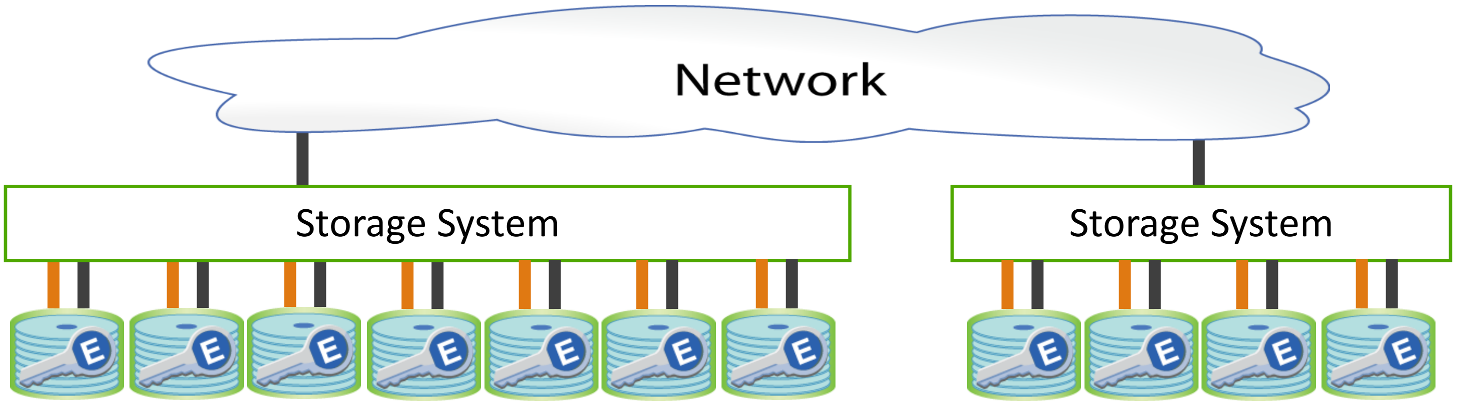
Encryption engine speed

Matches

Port’s max speed

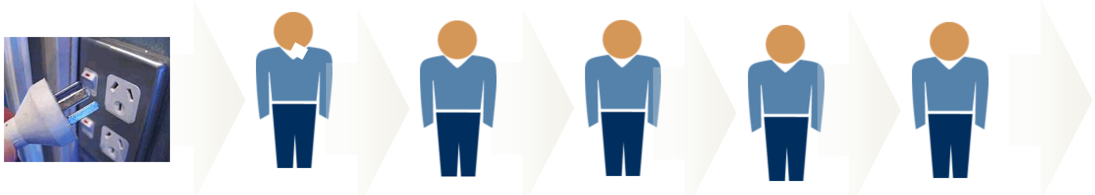
The encryption engine is in the controller ASIC

Scales Linearly, Automatically



All data will be encrypted, with no performance degradation

How the Drive Retirement Process Works



Retire Drive → Remove ALL drives → Send even "dead" drives through → Queue in Secure Area → Transport Offsite → Queue in secure area

- Replace
- Repair
- Repurpose

Retirement Options

Overwriting takes days and there is no notification of completion from drive

Hard to ensure degauss strength matched drive type

Shredding is environmentally hazardous

Not always as secure as shredding, but more fun

S E C U R E ?

People make mistakes

"Because of the volume of information we handle and **the fact people are involved, we have occasionally made mistakes**."

IRON MOUNTAIN

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

99% of Shuttle Columbia's hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

- May 7, 2008 (Computerworld)

[1] http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach_

How the Drive Retirement Process Works

Retirement Options

Retire Drive

- Repla
- Repai
- Repur

Drive Retirement is:

Expensive

Time-consuming

Error-prone

Overwriting takes days

drive

degauss

ed drive

cure

t

S
E
C
U
R
E
?

IRON MOUNTAIN

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

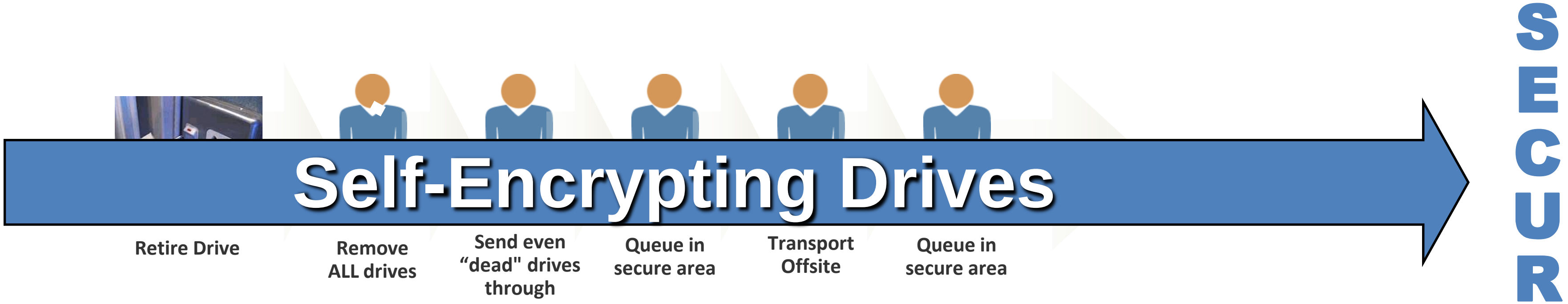
lumbia's hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

- May 7, 2008 (Computerworld)

[1] http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach_

Drive Retirement: Self-Encrypting Drives



- Replace
- Repair
- Repurpose

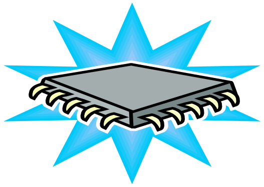
Power Off = Locked and Encrypted = Secure

- Reduces IT operating expense
  - Eliminates the need to overwrite or destroy drive
  - Secures warranty and expired lease returns
  - Enables drives to be repurposed securely
- Provides safe harbor for most data privacy laws

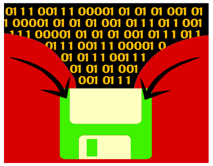
Hardware-Based Self-Encryption versus Software Encryption

-**Transparency:** SEDs come from factory with encryption key already generated

- **Ease of management:** No encrypting key to manage



- **Life-cycle costs:** The cost of an SED is pro-rated into the initial drive cost; software has continuing life cycle costs



- **Disposal or re-purposing cost:** With an SED, erase on-board encryption key

- **Re-encryption:** With SED, there is no need to ever re-encrypt the data

- **Performance:** No degradation in SED performance

- **Standardization:** Whole drive industry is building to the TCG/SED Specs

- **No interference** with upstream processes

- **User Authentication:** Pre-boot (drive based) authentication; optional TPM credential store

ISSUE: Hardware acquisition (part of normal replacement cycle)

Performance Comparisons: HDD and SSD, software versus SED

MB/Sec	HDD: no encryption	HDD: S/W encryption	HDD: SED	SSD: no encryption	SSD: S/W encryption	SDD: SED
Startup	7.90	6.97	7.99	82.50	47.90	95.33
App Loading	7.03	5.77	5.71	48.33	30.77	60.37
Modest size file test	6.13	5.00	5.28	41.13	26.77	50.40
Large Scale Data Read	84.67	52.88	82.75	178.00	70.23	169.33
Large Scale Data Write	79.60	49.50	50.31	170.80	63.60	164.50

http://www.trustedstrategies.com/

The Future: Self-Encrypting Drives

Encryption everywhere!

- Data center/branch office to the USB drive

Standards-based

- Multiple vendors; interoperability

User Authentication

Pre-boot authentication; TPM credential store

Unified key management

- Authentication key management handles all forms of self-encrypting storage

Simplified key management

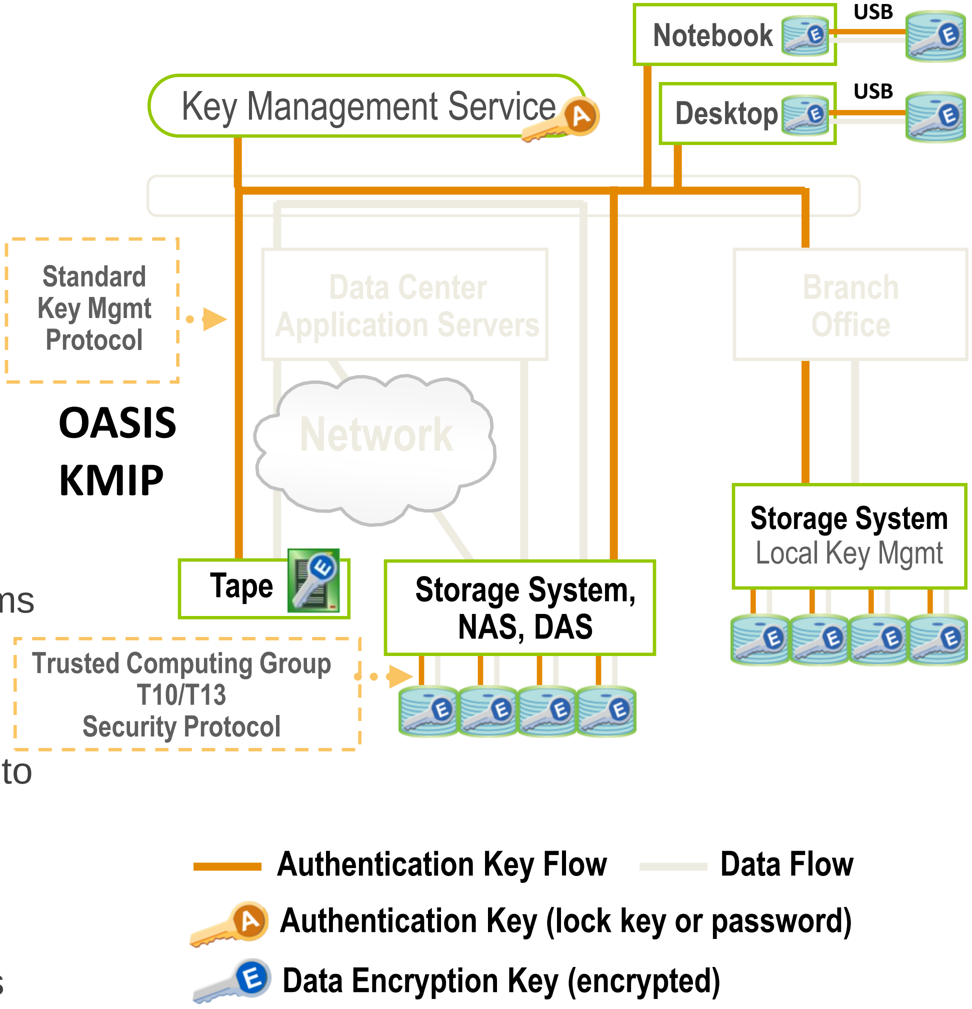
- Encryption keys never leave the drive. No need to track or manage.

Transparent

- Transparent to OS, applications, application developers, databases, database administrators

Automatic performance scaling

- Granular data classification not needed



Key Management Service

Notebook

USB

Desktop

USB

Standard Key Mgmt Protocol

OASIS KMIP

Data Center Application Servers

Network

Branch Office

Tape

Storage System, NAS, DAS

Storage System Local Key Mgmt

Trusted Computing Group T10/T13 Security Protocol

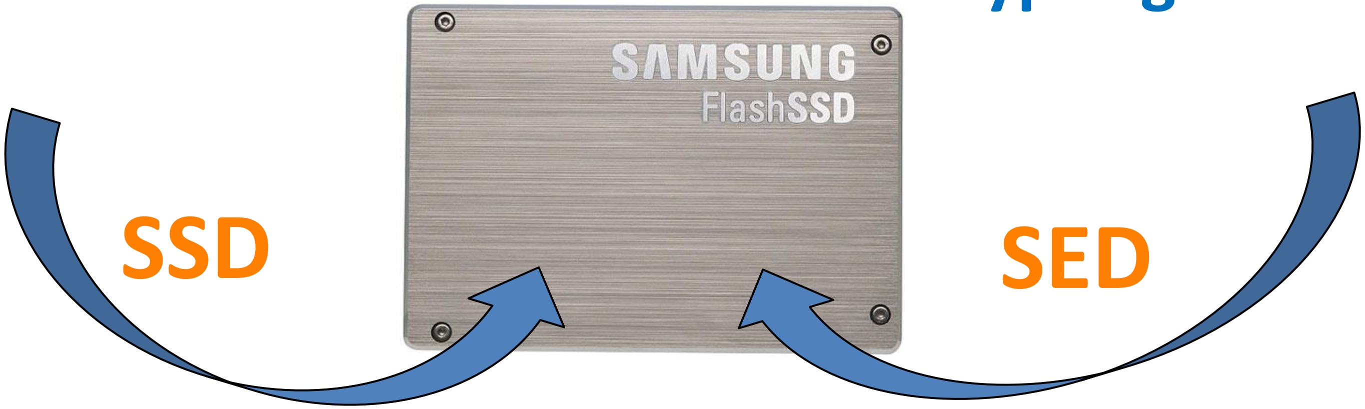
Authentication Key Flow

Data Flow

Authentication Key (lock key or password)

Data Encryption Key (encrypted)

Solid-State Drive + Self-Encrypting Drive



SIMPLE SOLUTION

- Reduced TCO
- Increased productivity
- Better Performance
- More shock resistance
- Better reliability
- Less power use
- Cost reduction up to $176

  (per user, annually)

- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cut Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent