Encrypted Storage: Self-Encryption versus Software Solutions

Dr. Michael Willett
Storage Security Strategist

Independent Consultant
• The Trusted Computing Group has defined and standardized Self-Encrypting Storage/Drives (SED) and the whole drive industry, including HDD and SSD, has implemented those standards. SEDs are steadily replacing non-SEDs in customer storage-requisition cycles. Such customers are weighing the relative merits of hardware-based self-encryption versus software-based solutions. Practical experience and the pro/con of making the transition to SEDs will be shared in this session.

• Learning Objectives

♦ Review compliance requirements for stored-data encryption
♦ Understand the concept of self-encryption
♦ Compare hardware versus software based encryption
♦ Examine practical experience implementing stored data encryption
Encrypted Storage: WHERE is the crypto engine?

AES Software

CPU

Storage Drive

...OR...

AES Hardware

encrypt/decrypt
Encryption can be done in a number of places:

- Host middleware
- Host HBA (h/w adapter)
- Application
- Switch
- “Bump in the wire” appliance
- Array controller
- Drive (HDD, SSD)
Encryption can be done in “layers of indirection”

Host middleware
Host HBA (h/w adapter)

Application

DIFERENT THREAT SCENARIOS (Possibly)

“Bump in the wire” appliance

Array controller

Drive (HDD, SSD)
Corporations spend millions to protect their networks, devices & data…

- Physical security, firewalls, intrusion detection, etc…

…But don’t always understand the risk posed by internal misplacement, re-purposing, and disposal processes.

Front Door  Back Door!!
Use Case: Stored Data Protection
The Problem…

2005-2013: over 864,108,052 records containing sensitive personal information have been involved in security breaches

In 2013, U.S. businesses paid an average cost of $5.4 million per data breach; that’s $188 per record

$5.4 Million Per Incident

http://www.privacyrights.org/ar/ChronDataBreaches.htm
2005-2013: over 864,108,052 records containing sensitive personal information have been involved in security breaches. In 2013, U.S. businesses paid an average cost of $5.4 million per data breach; that's $188 per record.

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

“... any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person...”

Encryption “safe harbor”
Why Encrypt Data-At-Rest?

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

- Compliance
  - 48+ U.S. states have data privacy laws with encryption “safe harbors”, which exempt encrypted data from breach notification¹

- EU: Data Protection Directive 95/46/EC (27 countries) replaced with European Data Protection Regulation ⁴: requires breach notification³

- Exposure of data loss is expensive ($6.65 Million on average per incident²)

- Obsolete, Failed, Stolen, Misplaced…
  - Nearly ALL drives leave the security of the data center
  - The vast majority of retired drives are still readable

². Ponemon Institute, Annual US Cost of Data Breach Study – www.ponemon.org
Approach: Self-Encrypting Drive (SED)
Trusted Storage Standardization

Published Storage Specifications

Self-Encrypting Drives (SED)
What is a Self-Encrypting Drive (SED)?

Trusted Computing Group
SED Management Interface

...OR...

AES Hardware Circuitry
- Encrypt Everything Written
- Decrypt Everything Read
Why Put Security Directly in Drive Storage?

3 Simple reasons

› Storage for secrets with strong access control
  • Inaccessible using traditional storage access
  • Arbitrarily large memory space
  • Gated by access control

› Unobservable cryptographic processing of secrets
  • Processing unit “welded” to storage unit
  • “Closed”, controlled environment

› Custom logic for faster, more secure operations
  • Inexpensive implementation of modern cryptographic functions
  • Complex security operations are feasible
Client Security: Pre-Boot Authentication

- Transparency: Master boot record and OS are unmodified
- Protected from malicious software: Authentication occurs before OS (and any malicious software) is loaded
- The master boot record can’t be corrupted: The entire drive, including the master boot record, is encrypted

1. BIOS attempts MBR read; drive redirects to pre-boot area
2. Drive loads pre-boot OS
3. User enters authentication credentials for drive to verify
4. If authentication successful, drive loads original MBR
5. Normal operation commences
Authentication in the Drive

1. Correct AK?
   - Yes
   - No

2. Clear AK decrypts DEK
   - Unlock HDD
   - Unlock SDD

3. DEK encrypts and decrypts User Data

- AK: Authentication Key
- DEK: Data Encryption Key

Hashed AK
Encrypted DEK
Clear Data
Hash AK
Pre-boot Authentication

Drive does NOT respond to Read or Write Reqs
Crypto 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

Revision 1 of U.S. NIST SP800-88: Guidelines for Media Sanitization under way to support Crypto Erase

No Performance Degradation

Encryption engine speed
Matches
Port’s max speed

The encryption engine is in the drive electronics

Scales Linearly, Automatically

All data will be encrypted, with no performance degradation
All Drives are Eventually Retired
  - End of Life
  - Returned for Expired Lease
  - Returned for Repair / Warranty
  - Repurposed

50,000 drives leave data centers daily
Exposure of data is expensive - $6.65 million on average
90% of retired drives are still readable (IBM study¹)

Needed: A simple, efficient, secure way to make retired drive data unreadable

How the Drive Retirement Process Works

People make mistakes

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

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

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)

Disposal Options Are Riddled with Shortcomings

Formatting the drive or deleting the data
- Doesn’t remove the data - data is still readable

Over-writing
- Takes hours-to-days
- Error-prone; no notification from the drive of overwrite completion

Degaussing the disk drive
- Difficult to ensure degauss strength matched type of drive
- Very costly; error-prone; dependent on technicians who have other duties
- Loss of investment

Shredding
- Very costly; time-consuming; dependent on technicians who have other duties
- Environmentally hazardous
- Loss of investment

Smashing the disk drive
- Not always as secure as shredding, but more fun
- Environmentally hazardous
- Loss of investment

Disposing via professional offsite services
- Costly
- No guarantee of disposal
- Drive is exposed to the tape’s falling-off-the-truck issue
How the Drive Retirement Process Works

Drive Retirement is:

- Expensive
- Time-consuming
- Error-prone

People make mistakes which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007¹

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)

Drive Retirement: Self-Encrypting Drives

Self-Encrypting Drives

- Retire Drive
- Replace
- Repair
- Repurpose
- Remove ALL drives
- Send even “dead” drives through
- Queue in secure area
- Transport Offsite
- Queue in secure area

Power Off = Locked/Encrypted = Secure

Added “insurance”: Crypto Erase

- 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
Key Management Simplification

Encryption key never leaves the drive. No need to track or manage...

BUT, YOU STILL MANAGE THE AUTHENTICATION KEYS (drive locking), to protect against loss or theft (for just crypto erase, no authentication key needed)

- To recover data from a drive:
  - *Only need the Authentication Key and the drive*
  - Don’t need to track encryption key storage separate from data storage
- Don’t need to be concerned with interoperability of encryption key storage and data
# Performance Comparisons: HDD and SSD, software versus SED

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup</td>
<td>7.90</td>
<td>6.97</td>
<td>7.99</td>
<td>82.50</td>
<td>47.90</td>
<td>95.33</td>
</tr>
<tr>
<td>App Loading</td>
<td>7.03</td>
<td>5.77</td>
<td>5.71</td>
<td>48.33</td>
<td>30.77</td>
<td>60.37</td>
</tr>
<tr>
<td>Modest size file test</td>
<td>6.13</td>
<td>5.00</td>
<td>5.28</td>
<td>41.13</td>
<td>26.77</td>
<td>50.40</td>
</tr>
<tr>
<td>Large Scale Data Read</td>
<td>84.67</td>
<td>52.88</td>
<td>82.75</td>
<td>178.00</td>
<td>70.23</td>
<td>169.33</td>
</tr>
<tr>
<td>Large Scale Data Write</td>
<td>79.60</td>
<td>49.50</td>
<td>50.31</td>
<td>170.80</td>
<td>63.60</td>
<td>164.50</td>
</tr>
</tbody>
</table>

‘Hurdles’ to Implementing Encryption…

| Key management / data loss       | • Tracking and managing encryption keys  |
|                                  | • Tracking and managing authentication keys (passwords for unlocking drives) |
| Complexity                      | • Data classification                  |
|                                  | • Impact on OS, applications, databases |
|                                  | • Interoperability                     |
| Performance                     | • Performance degradation; scalability |
| Cost                            | • Initial acquisition costs            |
|                                 | • Deployment costs                     |
## SED: Addressing the Hurdles…

<table>
<thead>
<tr>
<th>Simplifies Planning and Management</th>
<th>✓ Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplifies key management to prevent data loss</td>
<td>✓ Standards-based for optimal manageability and interoperability</td>
</tr>
<tr>
<td></td>
<td>✓ Transparent to application developers and database administrators. No change to OS, applications, databases</td>
</tr>
<tr>
<td></td>
<td>✓ Data classification not needed to maintain performance</td>
</tr>
</tbody>
</table>

## Solves Performance

|  ✓ No performance degradation |
|  ✓ Automatically scales linearly |
|  ✓ Can change keys without re-encrypting data |

## Reduces Cost

|  ✓ Standards enables competition and drive cost down |
|  ✓ Compression and de-duplication maintained |
|  ✓ Simplifies decommissioning and preserves hardware value for returns, repurposing |
“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
Factors Influencing Accelerated SED Adoption

1. AES/TCG in Controllers
2. All Channels/Models SED Capable
3. Diminishing/Zero Price Difference
4. Awareness: Breach Notification Exemption Compliance
SED Products Widely Available

- **Samsung**: SSD PC

- **Seagate** (Maxtor, Samsung HDDs): HDD and SSD PC and Enterprise

- **Western Digital** (Hitachi): HDD Enterprise

- **Toshiba** (Fujitsu): HDD PC and Enterprise

- **Micron**: SSD PC

- **Other HDD and SSD manufacturers**
Approach: Software-Based Encryption (CPU-based)

AES Software

CPU

encrypt/decrypt

Storage Drive
Encryption upstream can affect other processes:

- Data Compression
- Data De-duplication
- Data Loss Prevention (DLP)

Stored Data
Hardware vs Software Encryption: LOTS of Literature!

- **Data encryption's impact on network backup can be high**
  - “software-based encryption exacts perhaps the harshest performance penalty on the backup process”
  - “Software-based encryption often doesn't include data compression”

- **Hardware versus Software**
  - “Software-based encryption products address the basic need for encrypting data on computer systems where performance is not the primary concern … including communications and messaging encryption. Software-based products can also provide encryption at the file and folder level, as well as for removable storage devices.”
  - “Hardware-based encryption overcomes issues: … ease of use and system performance. Encryption built into the hard disk eliminates much of the setup and configuration complexity. … isolates the encryption functions and stores the encryption keys in the drive itself .. blocking rootkits and other malware from accessing keys and other sensitive information from the operating system. In addition, hardware encryption performance is very close to that of a non-encrypted drive”

- **Hardware-based full disk encryption**
  - “SEDs use a dual Master Boot Record (MBR) system … no other boot methods will allow access to the drive.”

- **Global Hardware Encryption Market 2015-2019**
  - “Global Hardware Encryption market to grow at a CAGR of 50.62 percent ”

MANY MORE…. 
SEDs RULE!

TOP TEN REASONS WHY...
Reason #1: Compliance

• Worldwide data protection laws and regulations continue to get more stringent on encryption, higher penalties, and more rigorous compliance evidence.
Reason #2: Performance

- Self-encrypting drives have integrated encryption hardware. The result:
  - Zero performance impact.

- Software full disk encryption/decryption is processor intensive and is performed by the main processor of the personal computer. During periods of high data usage this can have a major negative performance impact.

- For data intensive applications such as scans, backup, and large file operations, self-encrypting drives can provide much better performance than software FDE products*

- Net: Users can turn off software encryption! Bad.

Reason #3: Stronger Security

- All encryption and decryption is done in the protected hardware of the self-encrypting drive.
- Encryption keys are generated in the controller hardware of the self-encrypting drive, never leave the drive, and are not accessible outside of the drive – no management needed.

[Diagram showing encryption process with the Data Encryption Key da39a3ee 5e6b4b0d 3255bfef 95601890 and Encrypted Data e3b0c442 98fc1c14 9afbf4c8 996fb924]
Reason #3 (Cont’d): Stronger Security

- Self-encrypting drives are not vulnerable to attacks such as the following:
  - Alternative boot approaches using CD or USB keys such as the Evil Maid attack
  - Memory attacks to discover encryption keys held in systems memory. Example, Princeton Cold Boot attack

- Since the security of self-encrypting drives is independent of the operating system, then software attacks on the OS, BIOS, etc. are not effective against SED security
Reason #4: Integrated Authentication

• User authentication is performed by the self-encrypting drive in order to unlock the drive
• Authentication is performed by a protected pre-boot OS which is the only software in the system when authentication of the user is performed by the drive
• Authentication cannot be separated from the drive
• SEDs support multiple users and multiple administrators, each with their own passwords or authentication credentials
• The user credentials are never in the clear anywhere inside the self-encrypting drive
Reason #5: Transparent to Software

• Self-encrypting drives operate at the hardware level, making their encryption and authentication functions completely transparent to the system software, including the operating system.

• With transparent encryption in the SED, all utilities and other software will work without modification.

• Transparency allows patch management and other operating system functions to be handled normally, since not a single bit of the operating system is changed.

• Transparency: no impact on upstream processes.
Reason #6: No Encryption Key Management Required

- **Encryption keys are**
  - Generated in the self-encrypting drive controller
  - Never leave the drive nor the data they encrypt
  - Are never exposed outside the drive

- **Result:** There is no requirement to backup, recover or store encryption keys, either locally or centrally

- **Note:** Authentication Keys are externally managed
Reason #7: Easy to Use

• With self-encrypting drives, users only have two tasks:
  ✷ Authenticate to the drive at start-up
  ✷ Change passwords/credentials, as required

❖ **Result:**
  ✷ Encryption is invisible to the user
    ❖ No training required
  ✷ Full system performance, no impact on user productivity
Reason #8: Factory Integration

• Self-encrypting drives will typically be purchased as a feature in new platforms from PC OEMs

**Benefits of Factory Integration**

› SED is system tested with all hardware and software
› Encryption is always on
› PC OEM provides single point of support for platform and encryption solution
› SED management software can be preloaded as part of factory image

*Note: SEDs can also be installed in legacy machines*
Reason #9: Easy to Deploy

- Self-encrypting drives are always encrypting, therefore, when a drive is imaged, it is immediately ready to be used.

  - Software full disk encryption solutions require the following preparation every time the drive is imaged:
    - Run Chkdsk
    - Image drive
    - Encrypt the full drive (3-23+ hours for 500 GB drive*)

Reason #10: Low Total Cost of Ownership

Self-encrypting drives provide the lowest overall cost of ownership for an encryption solution.

<table>
<thead>
<tr>
<th></th>
<th>Self-Encrypting Drives</th>
<th>Software FDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition Costs</td>
<td>Even</td>
<td>Even</td>
</tr>
<tr>
<td>Deployment</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>IT Management</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Performance</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>User Productivity</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Security/Compliance</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Total Cost of Ownership</strong></td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Bonus Reason #11: Rapid Data Destruction

- Self-encrypting drives feature ‘crypto-erase’, which provides for near instantaneous data destruction by merely deleting the encryption key, thereby rendering all data on the drive unreadable.

- A new encryption key is generated; no inventory loss
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

New hardware acquisition (part of normal replacement cycle)
Software Encryption: Does NOT Address the Hurdles…

<table>
<thead>
<tr>
<th>Simplifies Planning and Management</th>
<th>Simplifies key management to prevent data loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standards-based for optimal manageability and interoperability</td>
<td>• Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed</td>
</tr>
<tr>
<td>• Transparent to application developers and database administrators. No change to OS, applications, databases</td>
<td></td>
</tr>
<tr>
<td>• Data classification not needed to maintain performance</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solves Performance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• No performance degradation</td>
<td>• Standards enables competition and drive cost down</td>
</tr>
<tr>
<td>• Automatically scales linearly</td>
<td>• Compression and de-duplication maintained</td>
</tr>
<tr>
<td>• Can change keys without re-encrypting data</td>
<td>• Simplifies decommissioning and preserves hardware value for returns, repurposing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reduces Cost</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standards enables competition and drive cost down</td>
<td></td>
</tr>
<tr>
<td>• Compression and de-duplication maintained</td>
<td></td>
</tr>
<tr>
<td>• Simplifies decommissioning and preserves hardware value for returns, repurposing</td>
<td></td>
</tr>
</tbody>
</table>
“Reasons” FOR Software Encryption

- **Good Enough**
  - Comprehensive risk analysis needed

- **Already Installed**
  - Is it being used/bypassed? Lifecycle costs?

- **Data Breaches – Not Me!**
  - All companies are susceptible! Check the literature

- **Cost of Retrofitting With SEDs**
  - Normal acquisition cycle; use life cycle costs, not just initial cost

- **Education – Do Not Understand the Alternatives**
  - Study! Lots of literature on the pro/con

- **Upper Management : Ignorance**
  - Breach protection is a “C”-level compliance requirement
  - Ignorance is not bliss!
Encryption everywhere!
- Data center/branch office to the USB drive

Standards-based
- Multiple vendors; interoperability

Unified key management
- Authentication key management handles all forms of 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
Thank You!
SSD ADVANTAGES

- Reduced maintenance times and cost
- Better performance
- More shock resistance
- More reliability (MTBF)
- Less power consumption

- Save $$ on IT cost (TCO)
- Faster booting and application launching
- Shock proof
- Fewer drive crashes
- Energy efficient and Green

Right Solution
**“... heat-assisted magnetic recording (HAMR) could push the (difference) even further...”**


**http://www.diffen.com/difference/HDD_vs_SSD**

Whereas hard drives are around $0.08 per gigabyte for 3.5", or $0.20 for 2.5", a typical flash SSD is about $0.80 per GB. This is down from about $2 per GB in early 2012.

### HDD versus SSD “Cost” Comparison

<table>
<thead>
<tr>
<th>$$$/GB</th>
<th>$$$/IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDD</td>
<td>SSD</td>
</tr>
<tr>
<td>$56.30/GB</td>
<td>$40/GB</td>
</tr>
<tr>
<td>Prediction</td>
<td>$1/GB</td>
</tr>
</tbody>
</table>

**Average HDD and SSD prices in USD per gigabyte**

Data sources: Mila.com, Gartner, and Pingdom (December 2011) www.pingdom.com

### HDD versus SSD “Cost” Comparison

<table>
<thead>
<tr>
<th>In/Out Operations per Second (IOPS – Higher is Better)</th>
<th>200~450 IOPS</th>
<th>10,000~25,000 IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequential Read/Write Speeds (MB/s – Higher is Better)</td>
<td>Read: 240MB/s Write: 210MB/s</td>
<td>Read: 510MB/s Write: 310MB/s</td>
</tr>
<tr>
<td>Random Read/Write Speeds (MB/s – Higher is Better)</td>
<td>Read: 2MB/s Write: 5MB/s</td>
<td>Read: 60MB/s Write: 210MB/s</td>
</tr>
<tr>
<td>Sound</td>
<td>Low Hum, “clicky” sounds during Read and Write</td>
<td>Sound of Silence</td>
</tr>
<tr>
<td>Heat Output</td>
<td>Moderate</td>
<td>Very Low</td>
</tr>
<tr>
<td>Power Consumption (Idle/Load)</td>
<td>14~17 Watts</td>
<td>0.5~5 Watts</td>
</tr>
<tr>
<td>Sensitivity to Shock/Vibration</td>
<td>Yes w/ Data Loss</td>
<td>None</td>
</tr>
<tr>
<td>Sensitivity to Magnets</td>
<td>Yes w/ Data Loss</td>
<td>None</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>Yes, degraded performance</td>
<td>None</td>
</tr>
<tr>
<td>Estimated Lifespan</td>
<td>1.5 Million Hours</td>
<td>2.0 Million Hours</td>
</tr>
</tbody>
</table>

**http://nutypesystems.com/rd-lab/ssd-vs-hdd-high-level/**
Solid-State Drive + Self-Encrypting Drive

SSD

SED

SIMPLE SOLUTION

- Reduced TCO
- Increased productivity
- Better Performance
- More shock resistance
- Better reliability
- Less power use
- Approaching price parity re: HDD
- Superior IOPS

- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cut Disposal Costs
- Scalable
- Interoperable
- Integrated
- Transparent
Example: SAMSUNG 840 EVO SSD SED

SAMSUNG 840 EVO SSD SELF-ENCRIPTING DRIVES

THREE TYPES OF SECURITY

- Samsung helps protect confidential information with the 840 EVO series of self-encrypting drives. All are equipped with a high-performance hardware accelerator that implements AES encryption with a 256-bit key. With a choice of three types of security, 840 EVO drives are ready to protect.

<table>
<thead>
<tr>
<th>Security</th>
<th>Default</th>
<th>How to Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCG Class 0</td>
<td>Ready to Enable</td>
<td>Set Password @ BIOS</td>
</tr>
<tr>
<td>TCG Opal</td>
<td>Ready to Enable</td>
<td>ISV Software</td>
</tr>
<tr>
<td>Encrypted Drive (eDrive)</td>
<td>Disabled</td>
<td>Change state to Ready with included Magician SW Secure Erase with Magician SW Install clean OS to automatically enable (Cannot be disabled by user)</td>
</tr>
</tbody>
</table>

Note: Only one security type may be enabled at a time.

CLASS 0

- EVO drives come ready to enable Class 0 security as a default. With Class 0, data is protected by a BIOS password. When Class 0 is enabled, Opal and eDrive security types are disabled.

OPAL

- Opal security is also a default on EVO drives. Using the Opal standard provides central control and administration and adds authentication capability, along with many other Opal features. When Opal is enabled, Class 0 and eDrive security types are disabled.

eDrive

- eDrive is disabled by default on EVO drives. It can only be enabled by a clean install of Windows 8.x Enterprise/Professional and Windows Server 2012. It cannot then be disabled by the user, and can only be disabled through the Samsung Service Center. When eDrive is enabled, Class 0 and Opal security types are disabled.

SAMSUNG 840 EVO SSD SELF-ENCRIPTING DRIVES

<table>
<thead>
<tr>
<th>Model</th>
<th>Retail</th>
</tr>
</thead>
<tbody>
<tr>
<td>MZ-7TE120BW</td>
<td>120GB 2.5&quot; Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-7TE120KW</td>
<td>120GB 2.5&quot; Samsung 840 EVO with Desktop Kit</td>
</tr>
<tr>
<td>MZ-7TE250BW</td>
<td>250GB 2.5&quot; Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-7TE250KW</td>
<td>250GB 2.5&quot; Samsung 840 EVO with Desktop Kit</td>
</tr>
<tr>
<td>MZ-7TE250LW</td>
<td>250GB 2.5&quot; Samsung 840 EVO with Notebook Kit</td>
</tr>
<tr>
<td>MZ-7TE500BW</td>
<td>500GB 2.5&quot; Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-7TE500LW</td>
<td>500GB 2.5&quot; Samsung 840 EVO with Notebook Kit</td>
</tr>
<tr>
<td>MZ-7TE750BW</td>
<td>750GB 2.5&quot; Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-7TE110BW</td>
<td>1TB 2.5&quot; Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-MTE120BW</td>
<td>120GB mSATA Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-MTE250BW</td>
<td>250GB mSATA Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-MTE500BW</td>
<td>500GB mSATA Samsung 840 EVO</td>
</tr>
<tr>
<td>MZ-MTE110BW</td>
<td>750GB mSATA Samsung 840 EVO</td>
</tr>
</tbody>
</table>

No price delta

ALL Models

3 SED MODES

2015
Saint Barnabas Health Care System: Case Study

- **Organization**
  - New Jersey’s largest integrated healthcare system
    - 25 functional facilities total
  - Provides treatment for >2M patients/year
  - 18,200 employees, 4,600 doctors

- **Environment**
  - 2380 laptops
  - Adopted SED as standard for desktops this year (2011),
    - used by healthcare professionals and executives
    - distributed across 25 functional facilities
  - Protecting PII/PHI/diagnostic information
  - HP shop using Wave-managed Hitachi SEDs
• **Barnabas Health:**
  - New Jersey’s largest integrated health delivery system
  - Implemented SEDs in 2380 laptops used by doctors, nurses, administrators and executives across 25 facilities
  - Will be encrypting 13,000 desktops used in the hospitals, via the asset lifecycle process in 4 years, 400 units expected to be done this year.

• **Key Findings:**
  - 24 hours faster deployment on average per user over previous software-based encryption
  - Negligible boot time versus up to 30 minutes to boot a PC with software encryption
Business Case

- **Identify the data protection risks/requirements**
  - Regulatory requirement for data protection
  - Safe harbor exemption
  - Intellectual property/Proprietary information protection

- **Build a business case**
  - Market place analysis
  - Embed into the asset lifecycle program to manage expense