
# Encrypted SSDs: Self-Encryption Versus Software Solutions

**Michael Willett**

**Storage Security Strategist**

**and**

**VP Marketing**

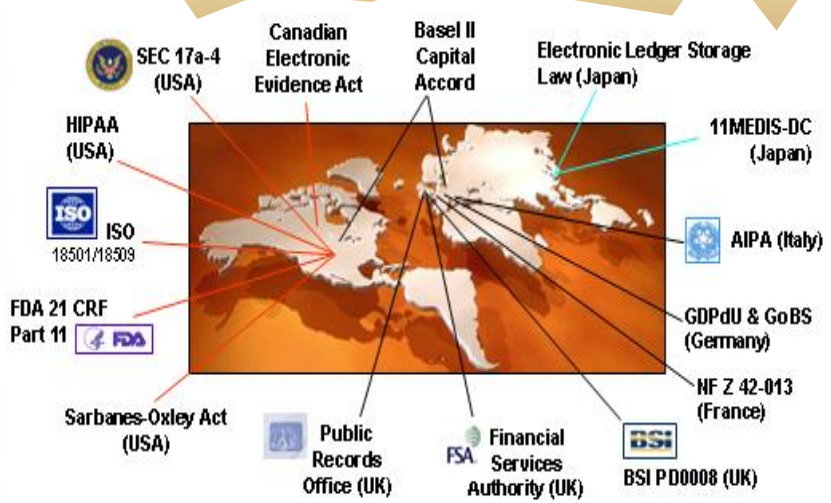
**Bright Plaza**

# 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

http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

# The Problem…

**2005-2013: over 864,108,052 records**
**contain**
**been in**

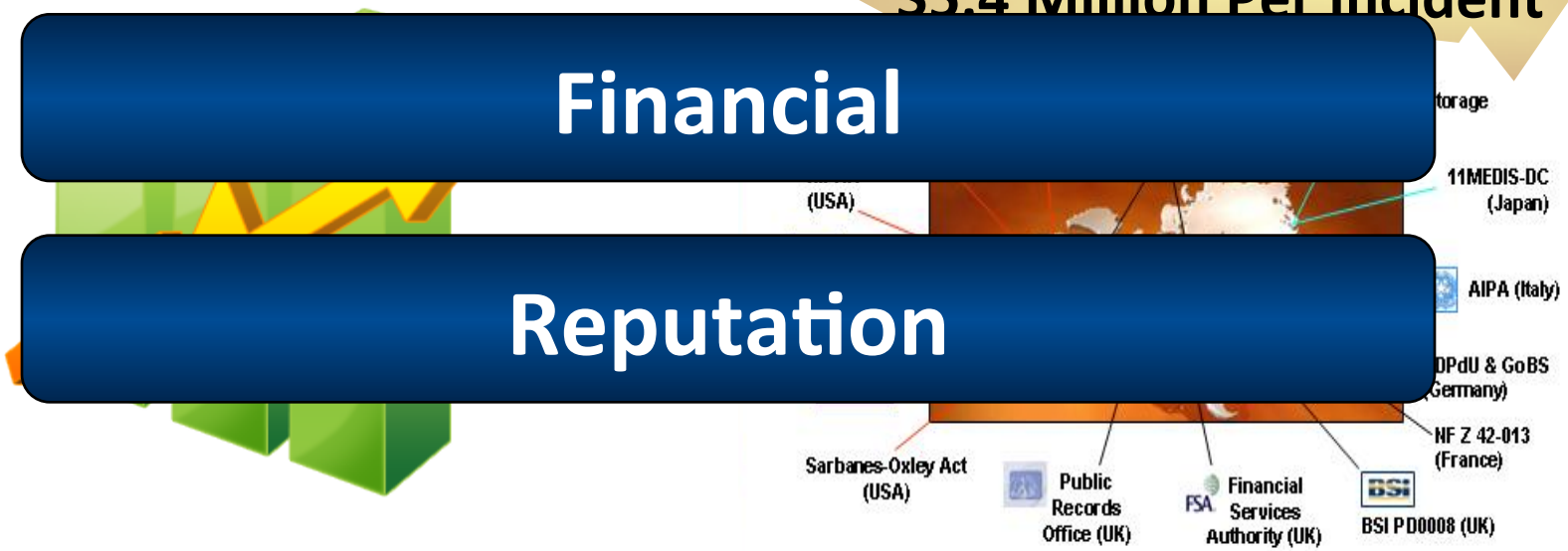
**…age cost of $5.4**
**…er record**

**$5.4 Million Per Incident**

**Legal**

**Financial**

**Reputation**




http://www.privacyrights.org/ar/ChronDataBreaches.htm
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013



3

# Breach Notification Legislation

## 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"

# Trusted Storage Standardization

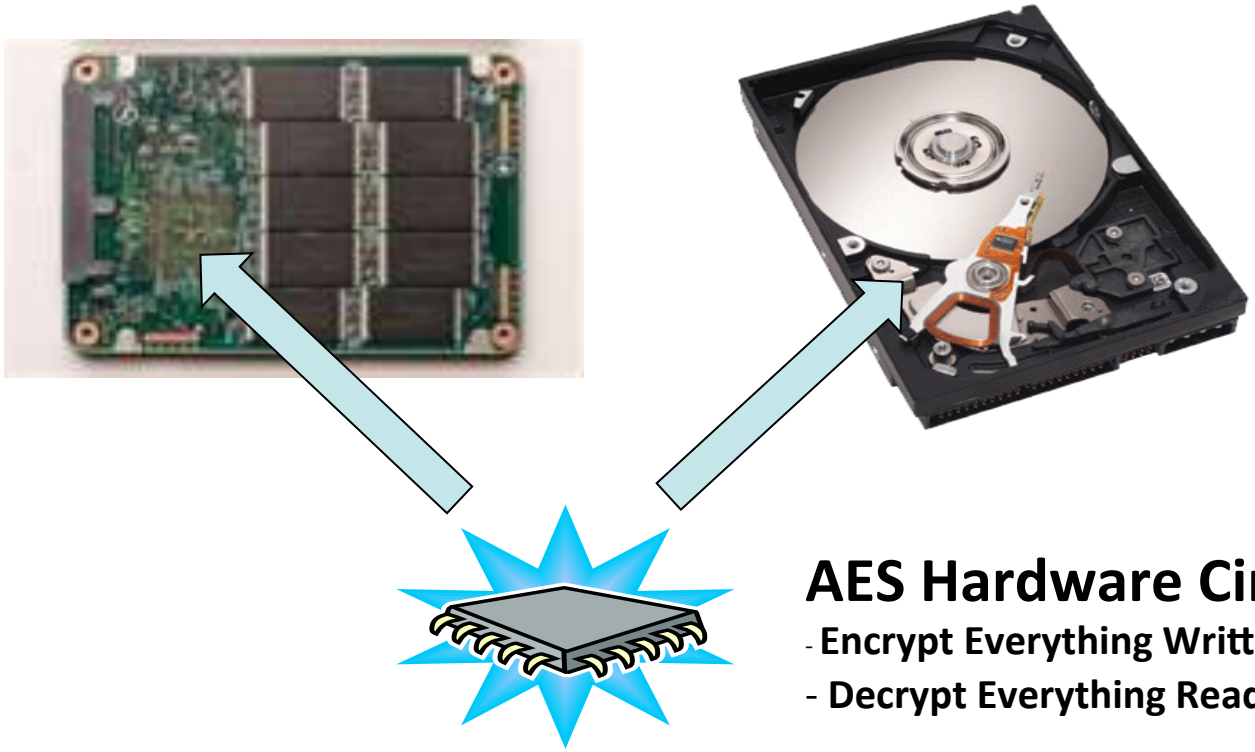


**Self-Encrypting Drives (SED)**

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

**Trusted Computing Group**
**SED Management Interface**

**I n t e r f a c e**

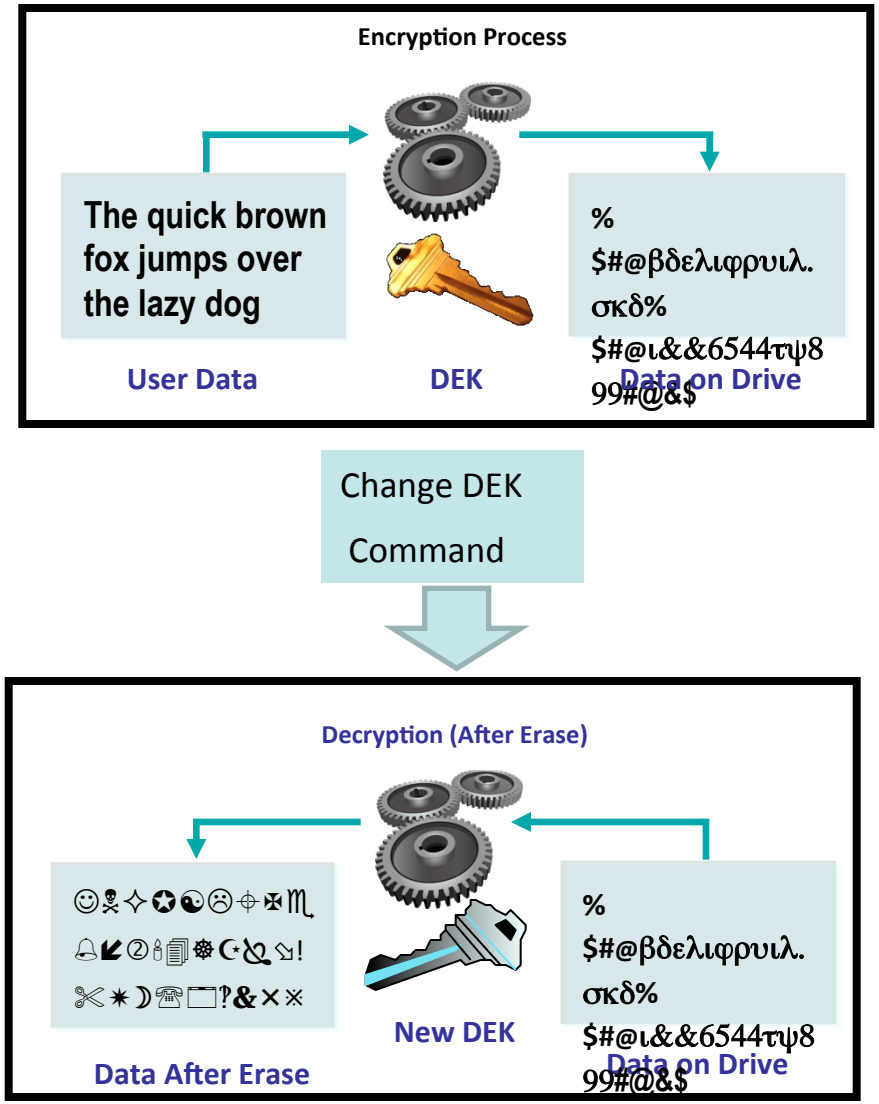


**AES Hardware Circuitry**
- **Encrypt Everything Written**
- **Decrypt Everything Read**

# 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

http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf



# No Performance Degradation

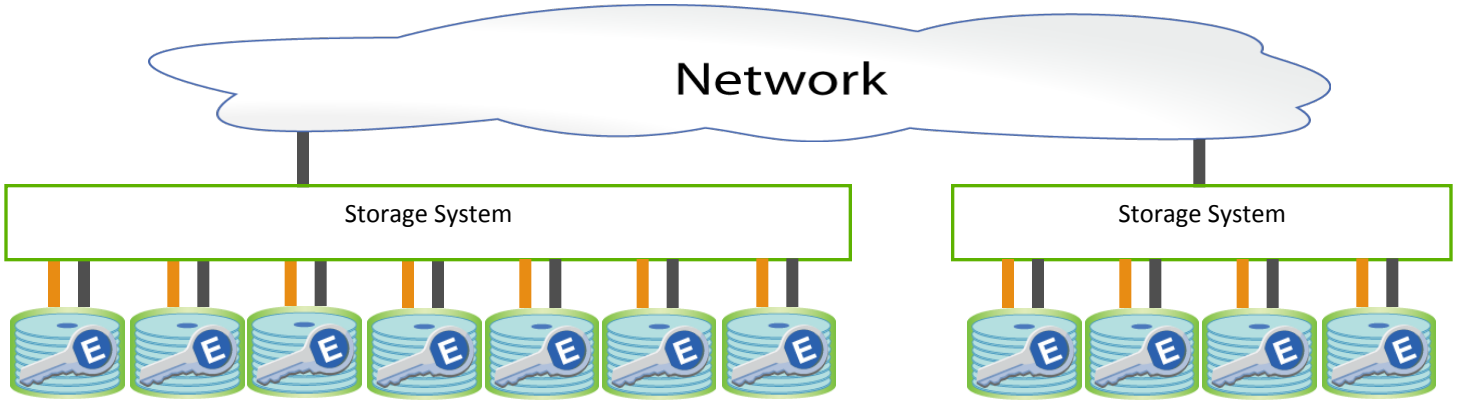
Encryption engine speed

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


# Hardware-Based Self-Encryption versus Software Encryption

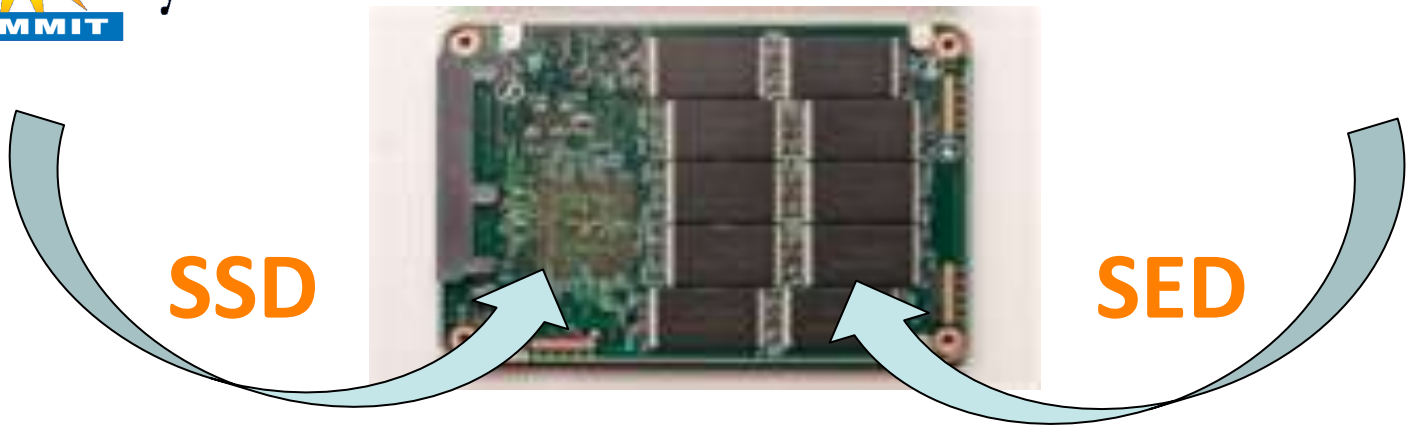
- **Transparency:** SEDs come from factory with encryption key already generated
- **Ease of management:** No encrypting key to manage
- **Life-cycle costs:** The cost of an SED is pro-rated into the initial drive cost; software has continuing life cycle costs
- **Disposal or re-purposing cost:** With 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)**

# Addressing the Hurdles…

| | |
|---|---|
| Simplifies key management to prevent data loss | ✓ Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed |
| Simplifies Planning and Management | ✓ Standards-based for optimal manageability and interoperability<br>✓ Transparent to application developers and database administrators. No change to OS, applications, databases<br>✓ Data classification not needed to maintain performance |
| Solves Performance | ✓ No performance degradation<br>✓ Automatically scales linearly<br>✓ Can change keys without re-encrypting data |
| Reduces Cost | ✓ Standards enables competition and drive cost down<br>✓ Compression and de-duplication maintained<br>✓ Simplifies decommissioning and preserves hardware value for returns, repurposing |

# Solid-State Drive + Self-Encrypting Drive




# SIMPLE SOLUTION

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

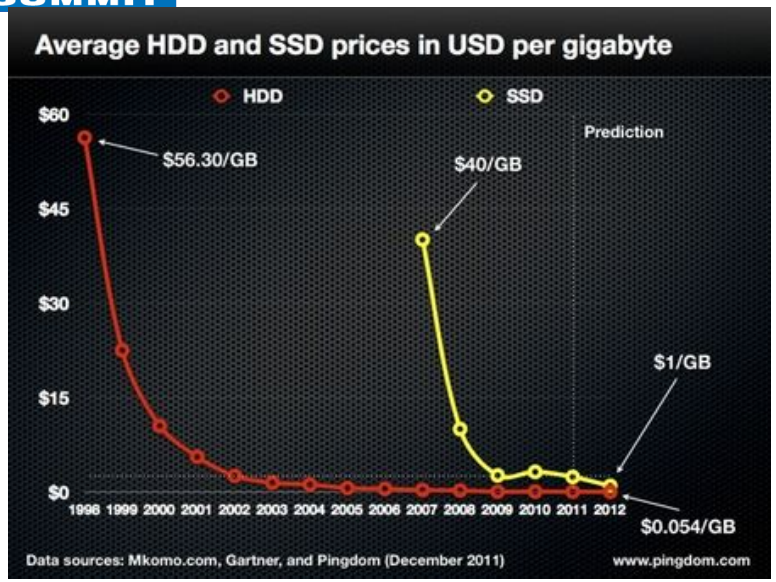
- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cut Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent

# HDD versus SSD "Cost" Comparison

Flash Memory SUMMIT

## $$$/GB




http://www.tomshardware.com/news/ssd-hdd-solid-state-drive-hard-disk-drive-prices,14336.html

"… 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.

## $$$/IOPS

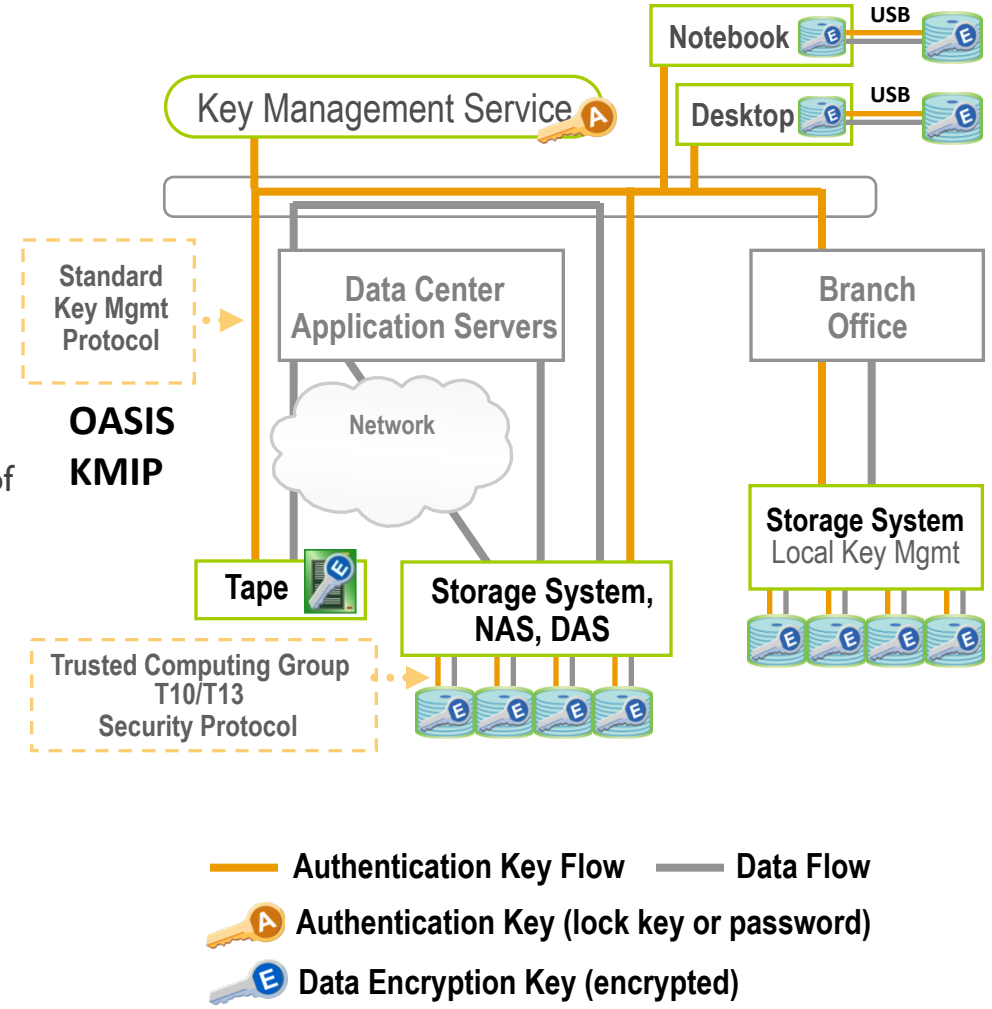
**IOPS are critical to the Enterprise**

| | Hard Drive (HDD) 1x 15,000RPM 300GB SAS | Solid State (SSD) 300GB |
|---|---|---|
| In/Out Operations per Second (IOPS – Higher is Better) | 200~450 IOPS | 10,000~25,000 IOPS |
| Sequential Read/Write Speeds (MB/s – Higher is Better) | Read: 240MB/s Write: 210MB/s | Read: 510MB/s Write: 310MB/s |
| Random Read/Write Speeds (MB/s – Higher is Better) | Read: 2MB/s Write: 5MB/s | Read: 60MB/s Write: 210MB/s |
| Sound | Low Hum, "clicky" sounds during Read and Write | Sound of Silence |
| Heat Output | Moderate | Very Low |
| Power Consumption (Idle/ Load) | 14~17 Watts | 0.5~5 Watts |
| Sensitivity to Shock/ Vibration | Yes w/ Data Loss | None |
| Sensitivity to Magnets | Yes w/ Data Loss | None |
| Fragmentation | Yes, degraded performance | None |
| Estimated Lifespan | 1.5 Million Hours | 2.0 Million Hours |

http://nutypesystems.com/rd-lab/ssd-vs-hdd-high-level/

# The Future: Self-Encryption Everywhere

- **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



# Drive Trust Alliance

- **Marketing and Open Source Development for Self-Encrypting Drives (SED)**
- Jointly with (Tom) **Coughlin Associates**
- **Mission**: promote (TCG/OPAL) SED adoption in the marketplace
- **Sponsors** benefit from cost efficiencies in:
  - marketing, on-going education, open source software for managing SEDs
- **Leadership team:** Bob Thibadeau, Scott Marks, Michael Willett
- **Client open-source software:**
  - initialize and provision a TCG/OPAL Self-Encrypting Drive (SED)
  - unlock one or more TCG ranges on that drive for reading and/or writing
- **Network agent application** for remote management of these functions using:
  - OASIS KMIP protocols or OMA protocols (in the case of mobile OS)
- **Roadmap:**
  - pre-OS boot (PBA) software and allow TCG OPAL ranges re: non-PBA use cases
- **Services can be either:**
  - broadly applicable to Sponsors or customized
- **Services include:** broad range of technical marketing support and collaboration
- **Contact:** (Gene Farrelly, COO, Bright Plaza, Inc., 919-389-3948, Gene.Farrelly@ka.je) for details on sponsoring the Drive Trust Alliance


# Thank You!