Ten Reasons to Buy Self-Encrypting Drives

September 2010

Overview:

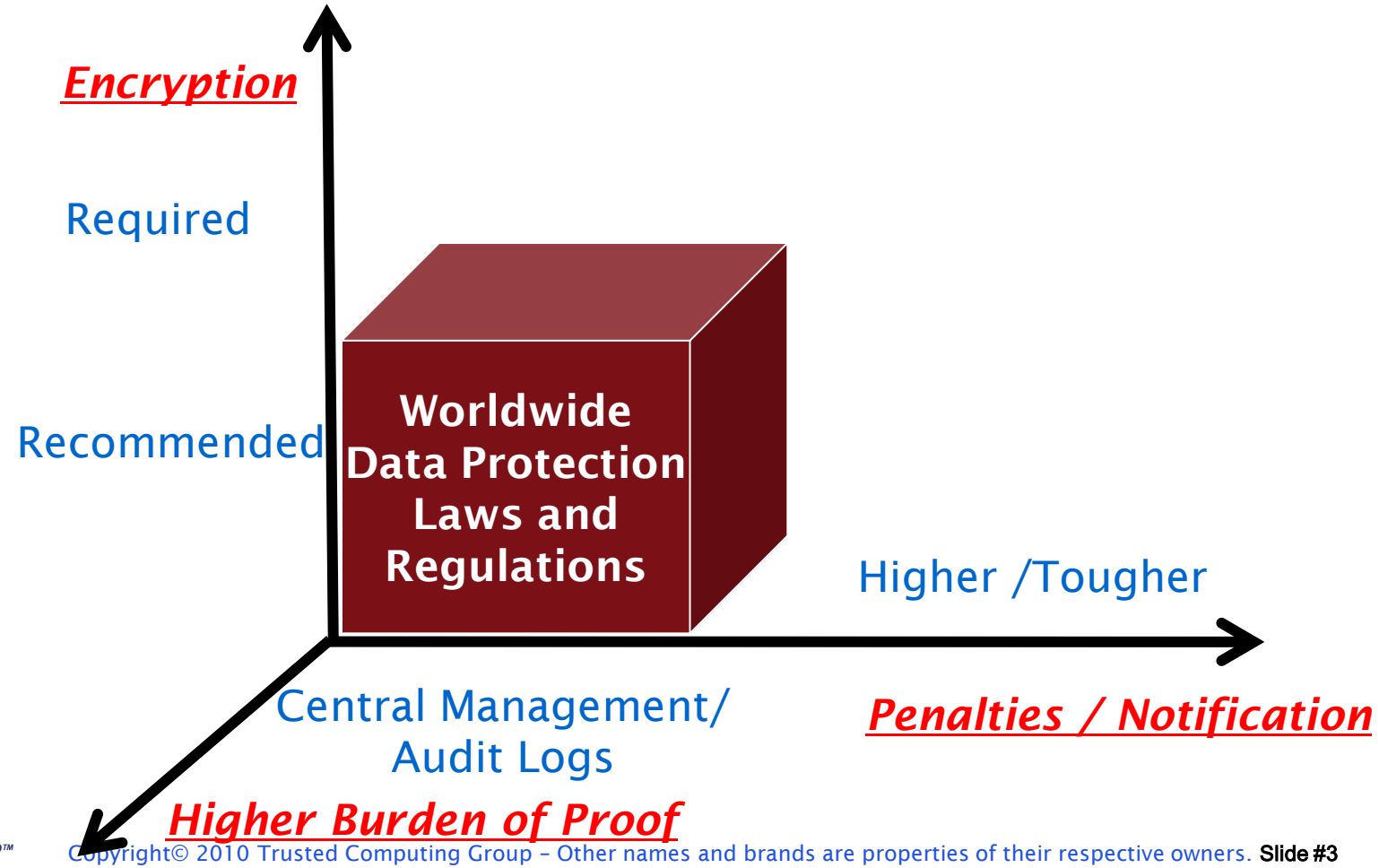
Self-encrypting drives based on open industry standards from the Trusted Computing Group provide a dramatically improved 'data at rest' solution for data protection.

Why to Buy Opal Self-Encrypting Drives

TRUSTED COMPUTING GROUP™

Reason #1: Compliance

- **Worldwide data protection laws and regulations continue to get more stringent on encryption, specify higher penalties, and require more rigorous compliance**



Reason #2: Performance

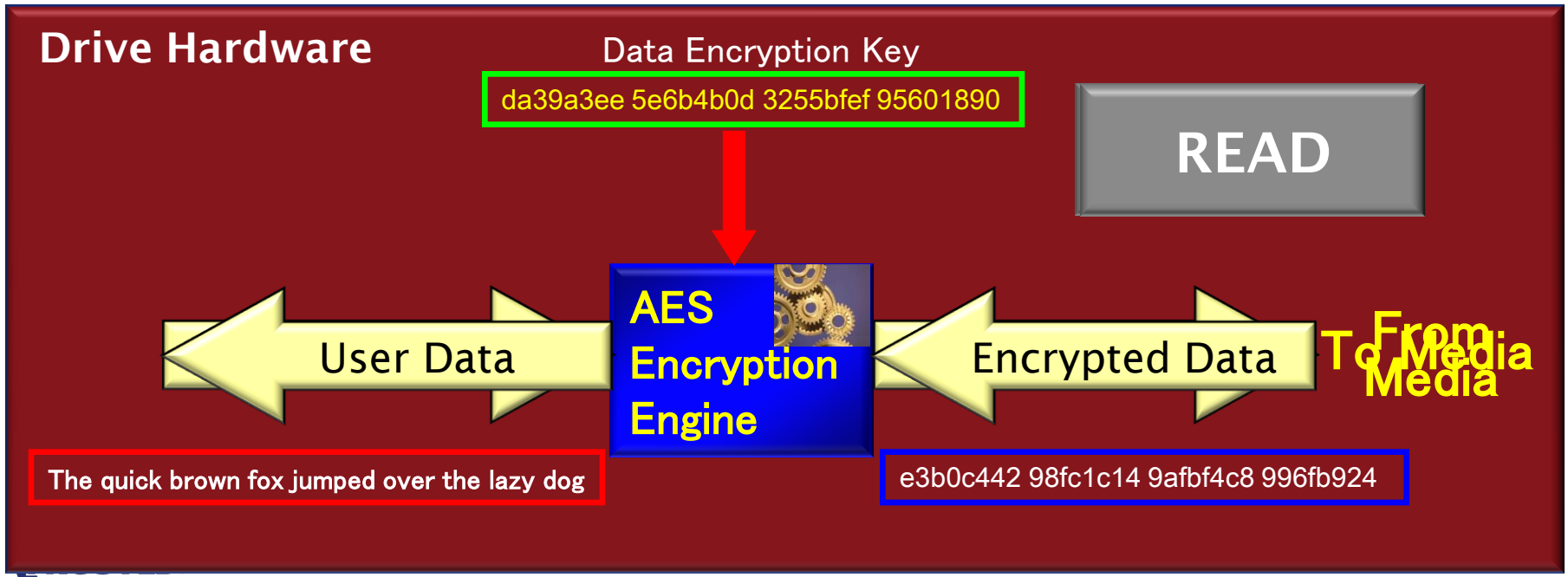
- Self-encrypting drives have integrated encryption hardware. The result: ***Zero performance impact***.
- Software full disk encryption/decryption is processor intensive and is performed by the main processor of the personal computer. During periods of high data usage this can have a major negative performance impact.
- For data intensive applications such as scans, backup, and large file operations, self-encrypting drives can provide more than double the drive performance of software FDE products*

*http://www.trustedstrategies.com/papers/comparing_hardware_and_software_fde.pdf

TRUSTED COMPUTING GROUP™

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



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
  - AES Caching attacks to discover encryption keys
- 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 provides a less complex solution

Reason #6: No Encryption Key Management Required

Encryption keys are

- Generated in the self-encrypting drive controller
- Never leave the drive and 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

However,

- Passwords and access control credentials for users to unlock the drives are still required
- Backup and recovery for these credentials is essential

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: In some cases, 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*)

* http://www.trustedstrategies.com/papers/comparing_hardware_and_software_fde.pdf

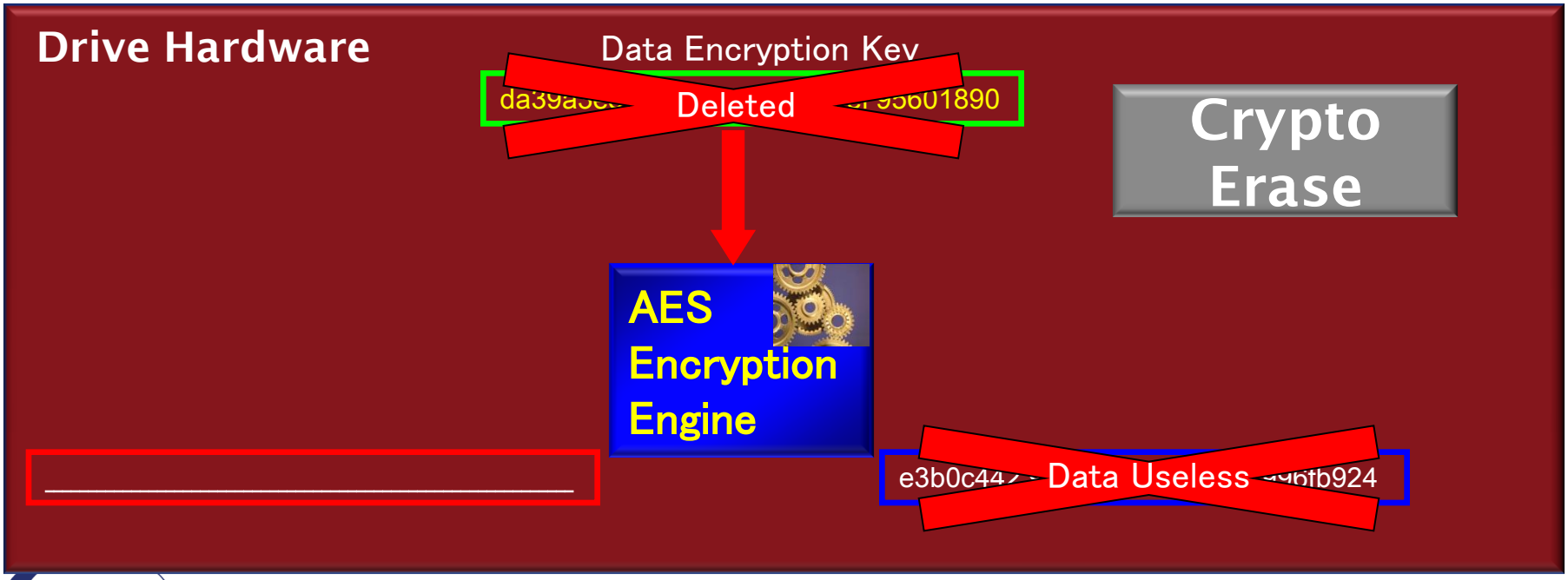
Reason #10: Low Total Cost of Ownership

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

	Self-Encrypting Drives	Software FDE
Acquisition Costs	Even	Even
Deployment	√	×
IT Management	√	×
Performance	√	×
User Productivity	√	×
Security/Compliance	√	×
Total Cost of Ownership	√	×

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 useless.
- The drive immediately generates a new encryption key.



Summary

- Self-encrypting drives represent the future of data protection

SED Benefits

- Stronger security
- Better performance
- Lower cost
- Less complex
- Easier to manage
- Easy to use