



# STORAGE VISIONS® 2011

AN ENTERTAINMENT STORAGE ALLIANCE™ EVENT

January 4-5, 2011 Riviera Hotel-Casino, Las Vegas, NV, USA



ENTERTAINMENT  
STORAGE  
ALLIANCE™



**Michael Willett, Storage Security Strategist, Samsung**

## TITLE

## ABSTRACT

Solid-State Drives (SSD) are gaining in popularity, both for the laptop and the data center, due to their superior properties in a number of areas:

- Reduced TCO (total cost of ownership): SSDs cost more than HDDs today, but the cost margin is steadily dropping. However, the initial cost is only part of the story. SSDs make up most of the difference in life-cycle costs
- Increased productivity: SSDs do everything faster, from power-on, to downloads, to computations, to return-from-hibernate, etc; less waiting throughout the workday creates more productive employees
- Better Performance: near-instantaneous access to data (reads and writes); no waiting for media rotations
- More shock resistance: no moving parts; operates in broader ranges of ruggedness, shock, and temperature; ideal for the 'road warriors' of business travel
- Better reliability: much bigger 'mean time to failure' numbers; HDDs are 'electro-mechanical'; SSDs have only the 'electro-' component
- Less power use: gives you longer battery life and a 'greener' device

The same users - for example, military, police, government agencies, but also gamers, intense and serious users and the frequent-traveler 'road warriors' of any company - who demand the higher reliability and performance of SSDs also demand robust security, especially protection of their stored data.

Traditionally, laptop encryption has been provided by software-based platform solutions. But, the storage industry has recently standardized (Trusted Computing Group) the concept of Self-Encrypting Drives (SED). All the major drive manufacturers cooperatively created the SED specifications and all are now providing products designed to those specs. SEDs satisfy the encryption 'safe harbor' exemption in most breach notification laws. Lost, stolen, or misplaced data must be reported publicly (expensive, embarrassing). But, auditable encryption negates the requirement for public notification.

Self-encryption has numerous superiority properties when compared to software encryption:

- Transparency: SEDs come from the factory with the encryption key already generated on-board and the drive already encrypting; always encrypting; software-based keys are provisioned by the user
- Ease of management: No encrypting key to manage externally; how does software-based encryption protect the encryption key? In software?
- 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, erasing the on-board encryption key rapidly renders the encrypted data unreadable; the "clean" drive can be re-used, disposed, or shipped out for warranty repair; software-based encryption often relies on lengthy data-overwriting procedures or even destruction of the drive itself
- Re-encryption: With SED, there is no need to ever re-encrypt the data; software-based encryption key changes require whole drive re-encryption
- Performance: No degradation in SED performance; hardware-based
- Standardization: The whole drive industry is building to the TCG/SED Specifications; software is proprietary
- No interference with processes, like compression, de-duplication, or DLP (data loss prevention); software encryption is necessarily upstream from storage and can interfere with such processes

The dynamic duo of SSD and SED provide an attractive and cost-effective combination, satisfying business requirements for both dependability and security.

## BIOGRAPHY

Dr. Michael Willett received a Bachelor of Science degree from the US Air Force Academy (Top Secret clearance) and a Masters and PhD in mathematics from NC State University. After a career as a university professor of mathematics and computer science, Dr. Willett joined IBM as a design architect, moving into IBM's Cryptography Competency Center. Later, Dr. Willett joined Fiderus, a security and privacy consulting practice, subsequently accepting a position with Wave Systems. Recently, Dr. Willett was a Senior Director at Seagate Research, focusing on security functionality on hard drives, including self-encryption, related standardization, product rollout, patent development, and partner liaison. Currently, Dr. Willett serves as a consultant on the marketing of storage-based security. Presently, Dr. Willett is working with Samsung as a storage security strategist, helping to define their self-encryption strategy across Samsung's portfolio of storage products.