Challenges Managing Self-Encrypting NAND Flash Devices

Sandler Rubin

Senior Product Manager,

Symantec Corp.

Agenda

1. Business Case for Encryption
2. What’s Wrong with Self-Encrypting Flash?
3. Understanding Enterprise Requirements
4. A Hybrid Future?
5. Conclusion & Questions

Mobility: Potential for Data Loss

47% of corporate data resides on mobile devices

43% of employees lost a device with company data

32% of employees didn't report the loss or theft in a timely fashion

***Source**: Ponemon Institute*

Risk Increasing Dramatically

~200M laptops sold in 2009
637K laptops lost in US airports

Nearly 440M smartphones by 2013
59% rate smartphone data as important

250M flash drives sold in 2009
65% capacity growth per annum

Majority of data breaches are internal
180M desktops and laptops retired annually

__Source__: Gartner, iSuppli, Ponemon Institute, SANS Institute

Steep Financial Impact

Compliance

Increased penalties, notifications

- 46 state laws plus 5 federal bills
- HIPAA, HIPSA, SOX, GLBA, PCI-DSS, etc.
- Data Protection Act (UK), EU Directive 95/46/EC

Intangible Costs

Disclosure is mandatory

- Diminished market valuation
- Damaged brand & credibility
- Loss of customer confidence

Tangible Costs

Data loss is expensive

- Cost per breached record: $204
- Average cost per incident: $6.75 million
- Typical IP value per laptop: Up to $8.8 million

1/15th as expensive to prevent

Source: *Gartner, Ponemon Institute*

Steep Financial Impact

Compliance

Increased penalties, notifications
- 46 state laws plus 5 federal bills
- HIPAA, HIPSA, SOX, GLBA, PCI-DSS, etc.
- Data Protection Act (UK), EU Directive 95/46/EC

Intangible Costs

Disclosure is mandatory
- Diminished market valuation
- Damaged brand & credibility
- Loss of customer confidence

Tangible Costs

Data loss is expensive
- Cost per breached record: $204
- Average cost per incident: $6.75 million
- Typical IP value per laptop: Up to $8.8 million

Encryption is the only "safe harbor"

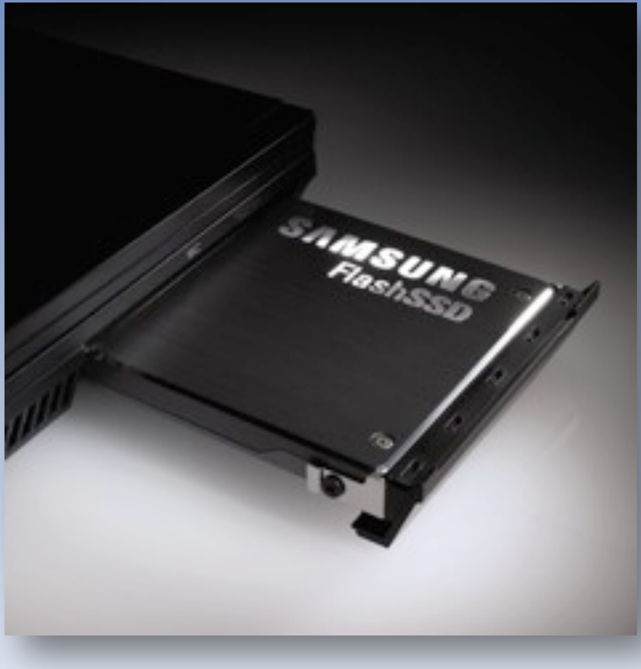
1/15th as expensive to prevent

Source: *Gartner, Ponemon Institute*

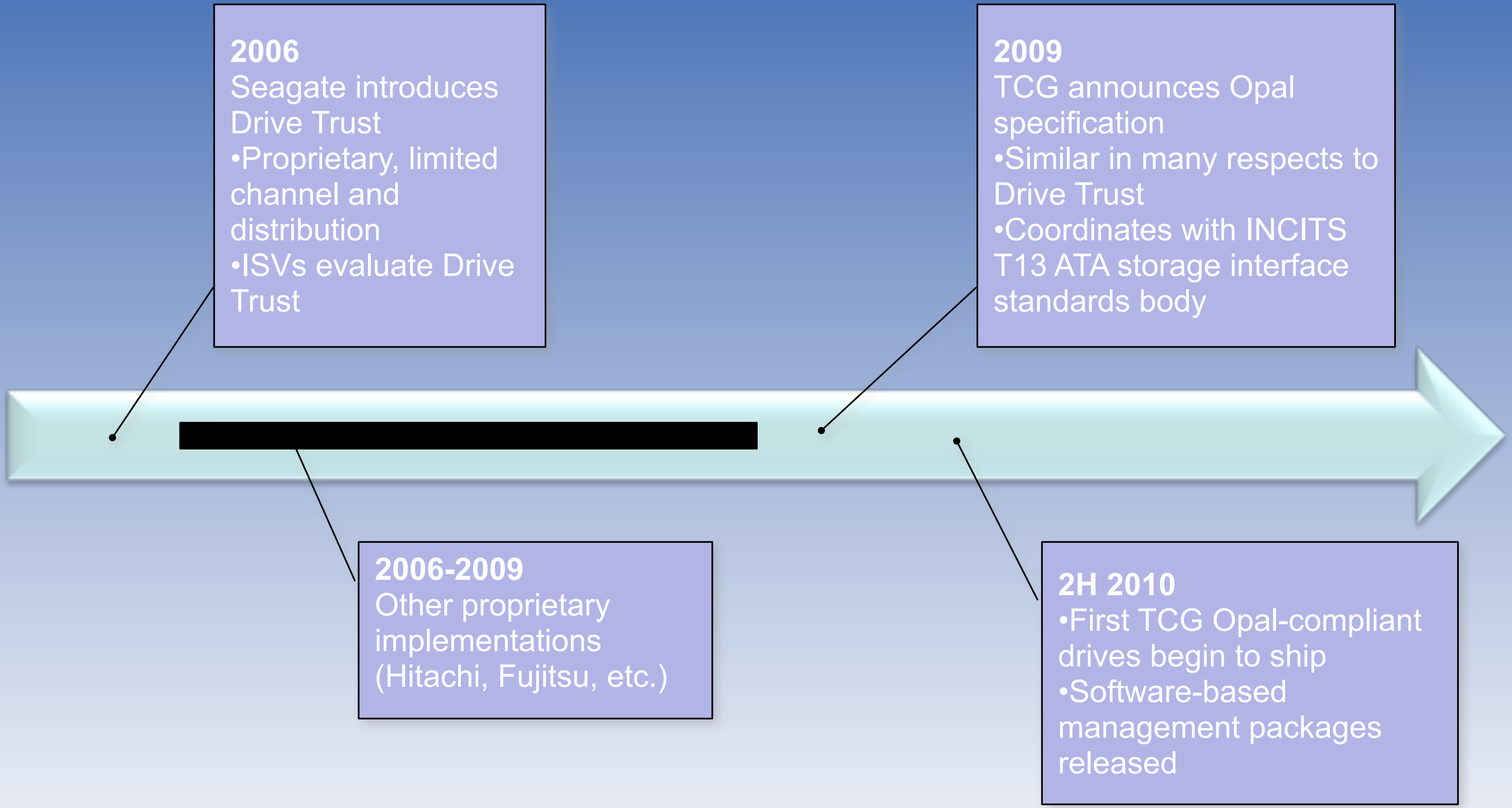
Emerging Self-Encrypting Devices

Secure, Removable Flash Storage

Self-Encrypting SSD



History of TCG Opal



2006
Seagate introduces Drive Trust

- Proprietary, limited channel and distribution
- ISVs evaluate Drive Trust

2006-2009
Other proprietary implementations (Hitachi, Fujitsu, etc.)

2009
TCG announces Opal specification

- Similar in many respects to Drive Trust
- Coordinates with INCITS T13 ATA storage interface standards body

2H 2010

- First TCG Opal-compliant drives begin to ship
- Software-based management packages released

Benefits of Self-Encrypting Devices

TCG Opal

- Cross-vendor compatibility
- Hardware-based, always-on drive encryption
- Full data bus performance
- On-board key generation and storage
- Standard interface for application developers
- Support for user and administrator accounts
- NIST-approved secure drive erase

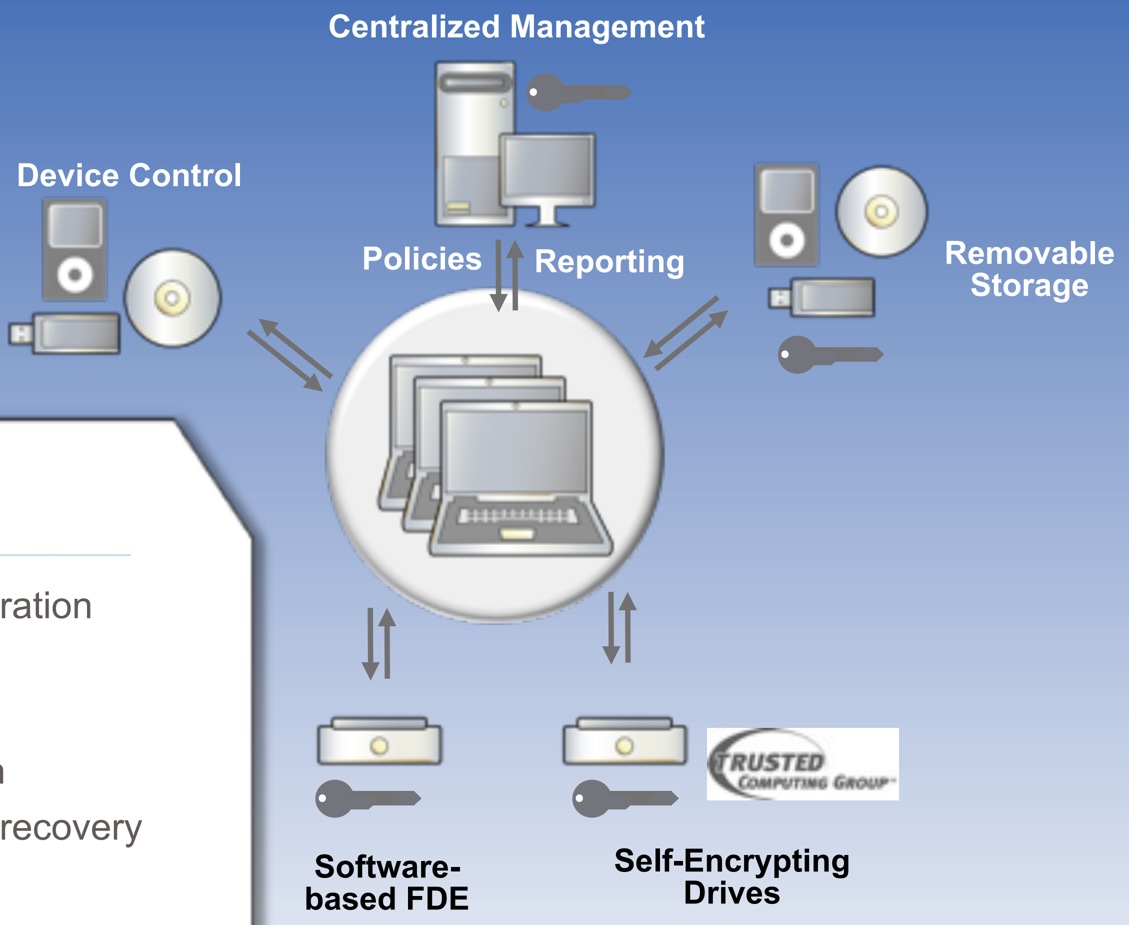
Secure USB Flash

- Highly portable
- In-built access controls
- Hardware-based, always-on drive encryption
- Excellent performance
- On-board key generation and storage
- Some vendors offer optional management

Management Challenges

- Rollout into hybrid environments
- Credential escrow and recovery
- Access recovery
- Policy management
- Reporting
- Pre-boot authentication with SSO
- Enforce usage

Enterprise Success Criteria



Key Requirements

- Policy management and administration
- Compliance reporting
- Key escrow and recovery
- Authentication with single-sign-on
- Assisted and self-service access recovery
- Directory services integration
- Lockout of non-reporting devices
- Device controls
- Integrated with existing encryption platform

Key Takeaways

- Threat landscape and data breach costs are driving the need for encryption
- Self-encrypting storage has lots of positive benefits, but insufficient on its own
- Enterprise must combine software-based management with self-encrypting storage
- Enterprises will be supporting hybrid environments for the foreseeable future

Questions?