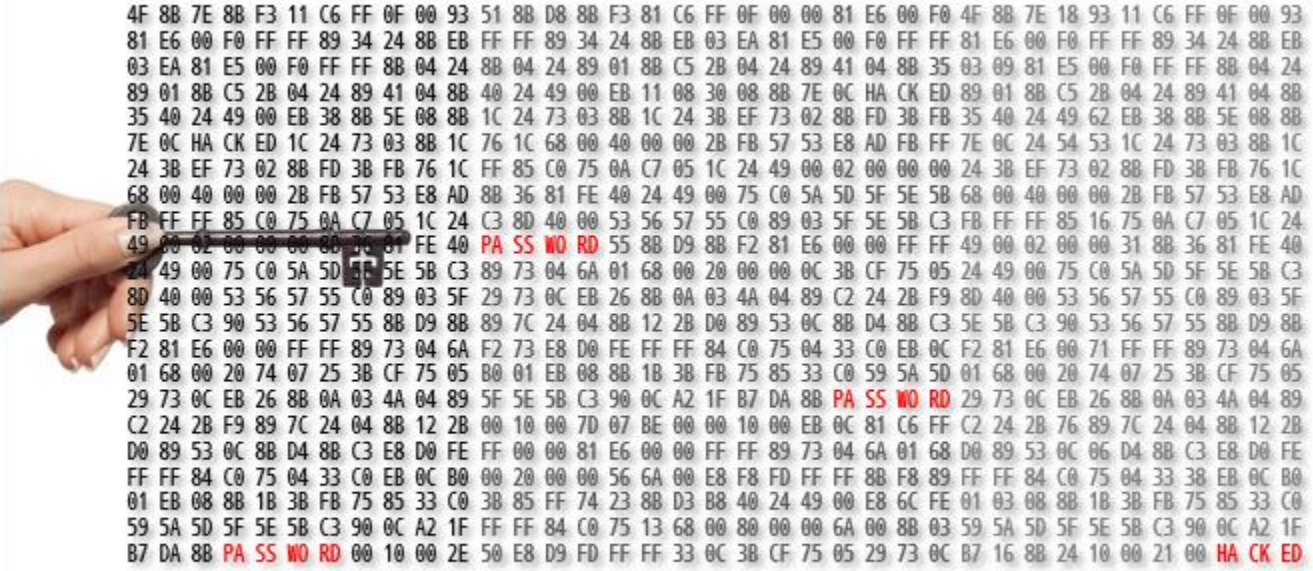
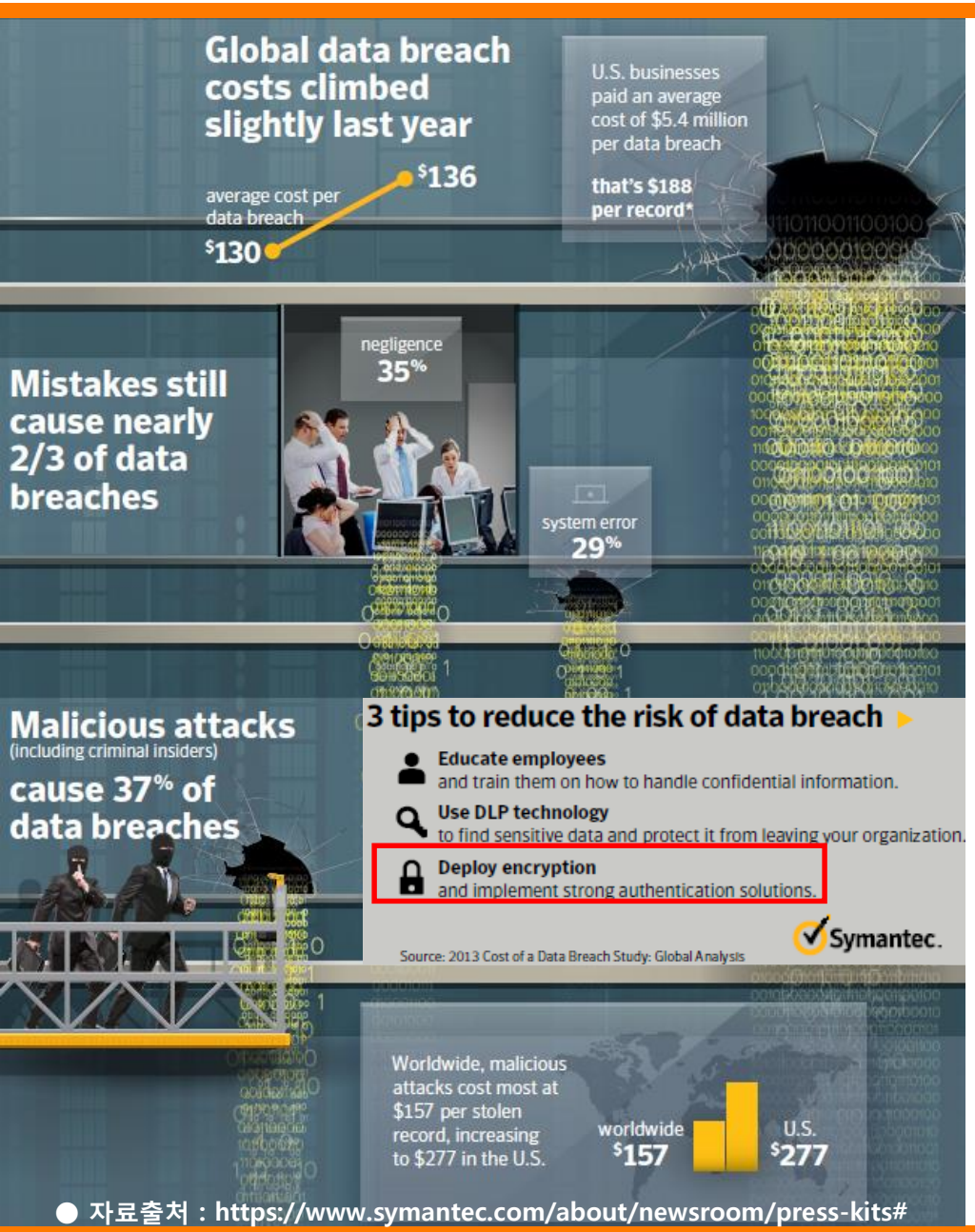
Security Features for SSD



SK hynix

Why Storage Security is Important ?



● 자료출처 : https://www.symantec.com/about/newsroom/press-kits#

Dilemmas !

" A secret known by two is no longer a secret "

Sheer magnitude of breaches

Data is more vulnerable than ever, however. The Chronology of Data Breaches, which tracks compromises of personal information, reports:

4,817

Data Breaches

made public since 2005 with 898,584,384 RECORDS BREACHED in total. Examples of such incidents, which often lead to identity theft, legal action and brand damage, include:

1. **Nationwide Building Society**
   Missing notebook containing data of 11 million customers
2. **Humana**
   Company laptop stolen, along with a file containing customer information
3. **University of California**
   Laptop computer theft with graduate student application information including Social Security numbers
4. **UCLA Health**
   Valuable data on password -protected discs was apparently being handled by junior employees

The consequences can be devastating to businesses and individuals. Ponemon Institute reported in 2015:

$3.8M Average total cost of data breach

$154 Average cost per lost/stolen record

22% Likelihood of a business being breached in the coming 24 months

● 자료출처 : https://trustedcomputinggroup.org/work-groups/storage/

Why focus on the DAR(Data At Reset) and DARE(DAR Encryption) ?

3 States of data

- Data is everywhere, and when is broadly categorized, three states of data exist

Data in Motion

- Network
- Multi-Channel : e-mail, Messaging, P2P, Web, FTP, etc

• Anytime a user uploads or downloads data from a cloud server or data is in transit while being shared, that's data in motion. When that same data is simply existing in the cloud or on an endpoint device, the data is at rest.

• Data in transit is often an easy target for cyber criminals, who can position themselves between where data is stored and where it's going to syphon off information in transit. If this data in motion is not encrypted, there's nothing stopping the cyber criminal from gaining access.

Data at Rest

- Discovery, Analysis, Protection & Control
- PC, Server, HDD, SSD, Other Media

• There's a misconception that data at rest is more secure than data in motion; the truth is they're both vulnerable. Outside of physical device theft, where any unsecured data at rest could become vulnerable, if data at rest isn't outfitted with access rights controls, nothing is stopping an end user from downloading an app and unwittingly providing it permission to access that file on their device.

• **Data leakage through stolen/lost laptop or storage device**

• **End of life and disposal**

Data in Use

• Integrity
• End Point, Network Interface

• Data in use could include anything from a file being copied between folders to files being edited to data being transferred from a laptop to a thumb drive. While it might be easier to steal data in motion, data in use (and data at rest) must always be secure as well.

Encryption at Rest in Google Cloud Platform

Google's default Encryption Policy

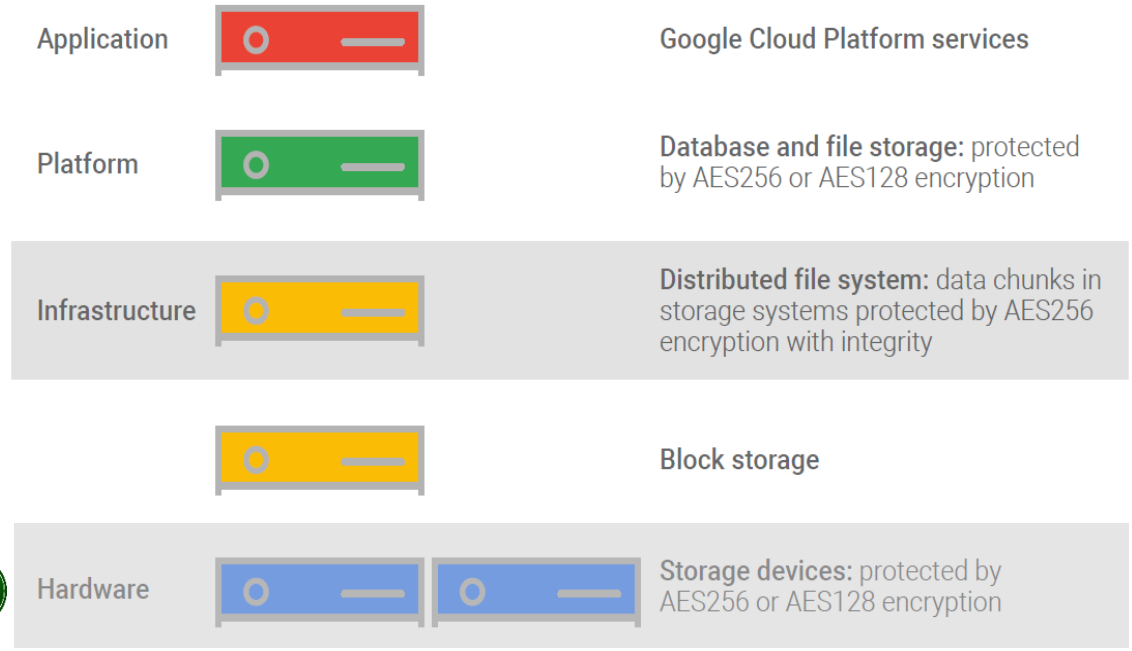


Figure 1

• Several layers of encryption are used to protect data stored in Google Cloud Platform. Either distributed file system encryption or database and file storage encryption is in place for almost all files; and storage device encryption is in place for almost all files.

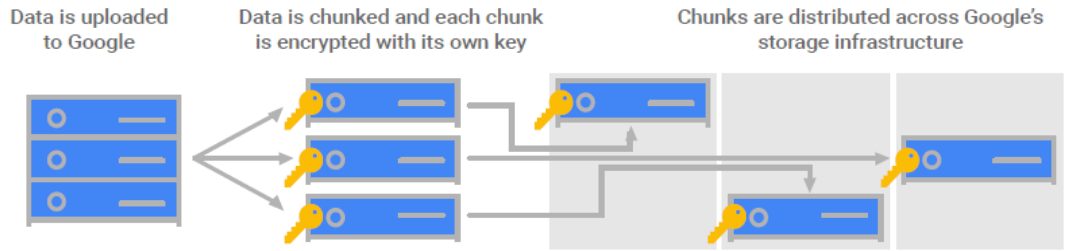


Figure 2

• Data at Google is broken up into encrypted chunks for storage.

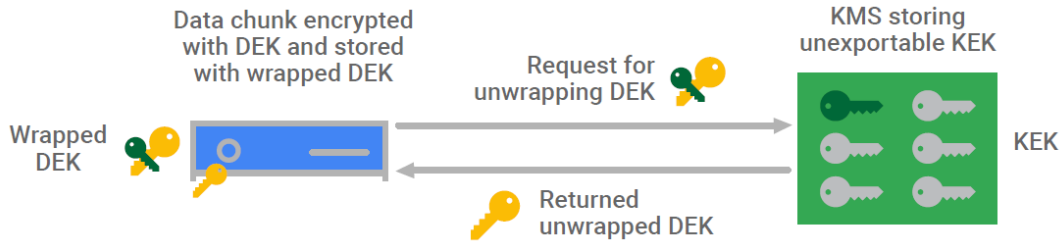


Figure 3

• To decrypt a data chunk, the storage service calls Google's Key Management Service (KMS) to retrieve the unwrapped data encryption key (DEK) for that data chunk.

Google 자료출처 : https://cloud.google.com/security/encryption-at-rest/default-encryption/

What are the Security Features for SSD ?

▪ DAR security features

▪ Without User-data Encryption

ATA Security

- Security mode feature set
- The storage device allows read/write access to the user data only after the required authority is proven
- User password / Master password
- Frozen mode supply : The storage device will abort all read/write commands until it is unlocked

TCG Pyrite

- TCG Security Subsystem Class
- Pyrite SSC does not specify encryption of user data

▪ With User-data Encryption

FDE (Full Disk Encryption)

- Encrypts an entire disk(1 Global range)
- One Key(Media Encryption Key) encrypts/decrypts the whole device

Microsoft eDrive

- MS Windows manages eDrive
- No additional Key Management solution to deploy eDrive

SED (Self Encrypting Drive)

- The Best-Kept Secret in Storage Device Encryption Security
- TCG Opal(Client) / TCG Enterprise(Enterprise)
- Encrypts Multi-ranges with Key Management scheme

What is a SED ?

Self Encrypting Drive

- **Power Off → Drive Locked / Encrypted = Secure + "Instant Crypto Erase"**
  - Hardware AES engine(AES : Advanced Encryption Standard, FIPS197)
  - Encrypt everything written
  - Decrypt everything read

AES 128/256-bit Hardware Encryption Engine → TCG OPAL2.0 → Encryption Management Application → IEEE1667 Protocol

AES256

FIPS 197 Federal Information Processing Standards AES Encryption Approved

NIST

TRUSTED COMPUTING GROUP

WINMAGIC DATA SECURITY

wave

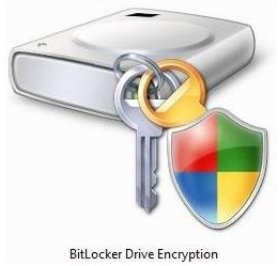
SOPHOS Community BETA

Check Point SOFTWARE TECHNOLOGIES LTD

Symantec.

McAfee

Microsoft



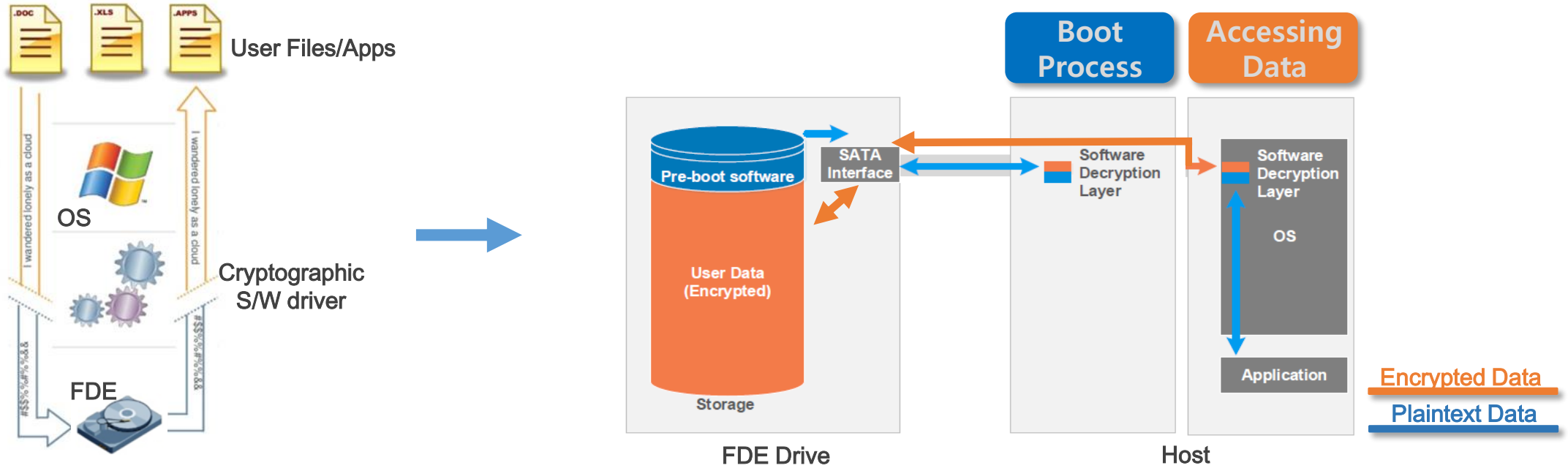
BitLocker Drive Encryption

What are SEDs ?

Classical FDE(Full Disk Encryption)

- Encryption performed by the OS
- FDE Software
  - Bitlocker(MS)
  - SecureDoc(Winmagic)
  - Embassy(WAVE)
  - SafeBoot(McAfee), etc

- PROS
  - User data is useless without the key
  - Hardware-based FDE : within a storage device is called a SED
  - Instant “Secure Erase” is possible : Simply delete the key
- CONS
  - Runtime performance degradation

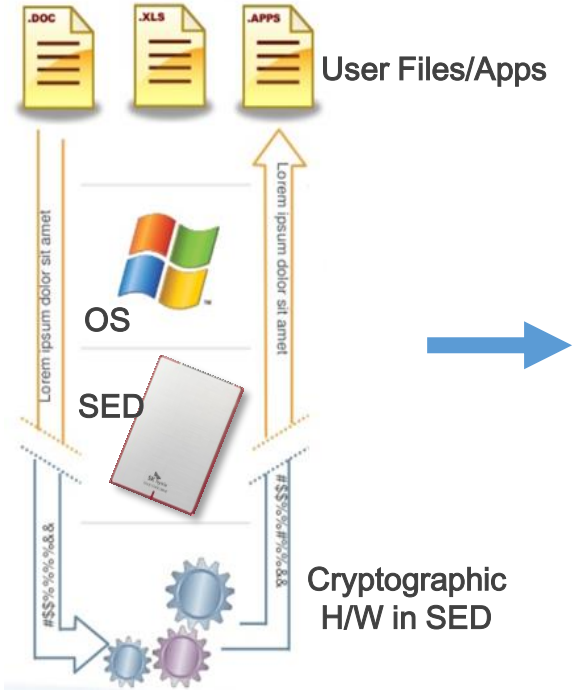


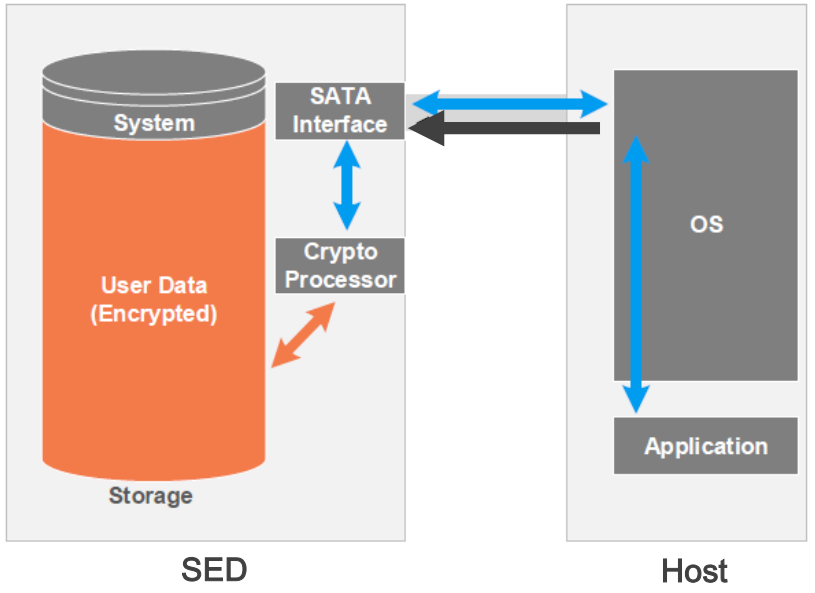
What are SEDs ?

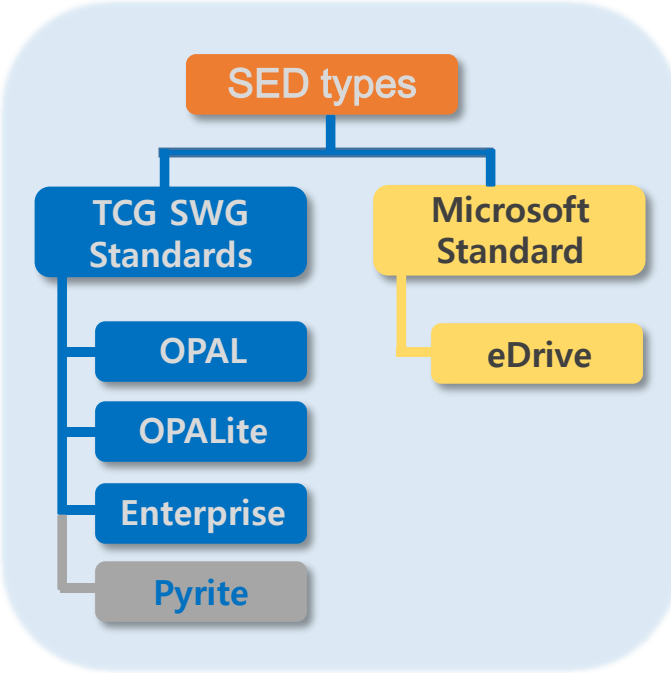
SED(Self Encrypting Drive)

- Hardware AES engine
- Encryption performed by the driver controller
- SED security = SED + ISV application
- Provide more Secure Solution than FDE
- Protect against to Malware

- PROS
  - No performance Overhead
  - Instant in-place Encryption
  - Secure Boot flow is available
- CONS
  - ?







Encrypted Data

Plaintext Data

Security Commands

What are SEDs ?

▪ FDE(S/W Encryption based) vs SED(H/W based)

	Software based FDE	Hardware based SED
▪ Transparency	X	O
▪ Ease of management	X	O
▪ Disposal cost	O	X
▪ Re-encryption	O	X
▪ Performance degradation	O	X
▪ Consumes valuable computer resource - CPU, Memory, etc.	O	X
▪ Open to attack - Key generation exposed - Key storage accessible to OS	O	X
▪ Secure crypto erase	sometimes	O
▪ Standardization	X	O

Performance Comparison

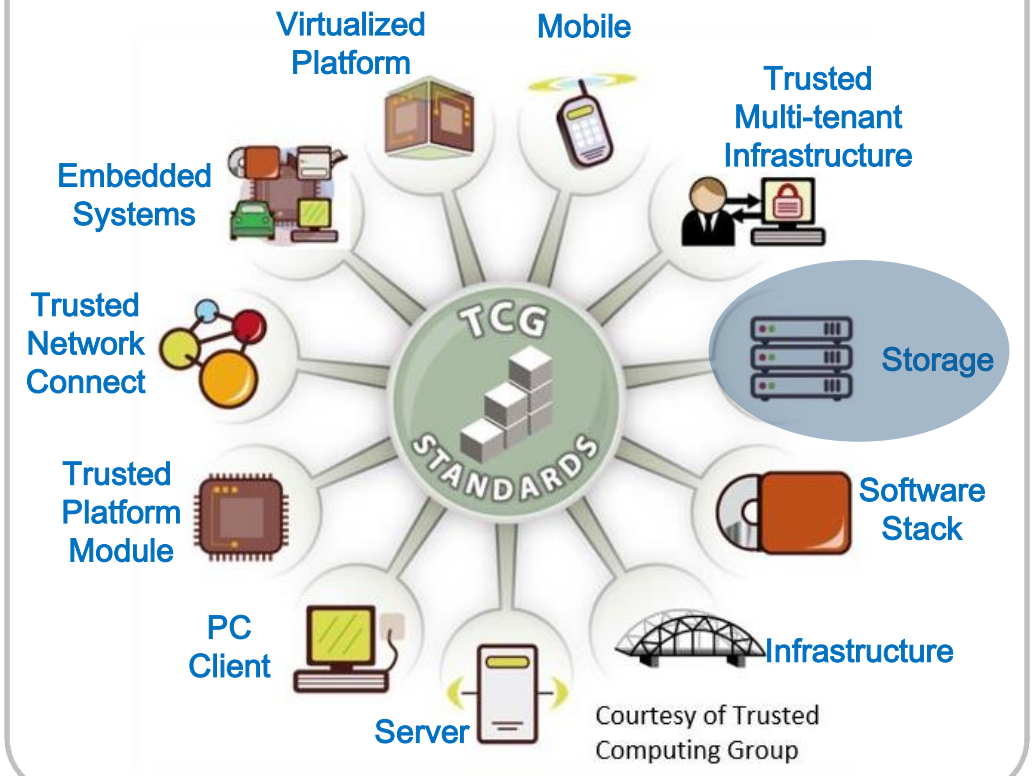
MB/Sec	HDD: no encryption	HDD: S/W encryption	HDD: SED	SSD: no encryption	SSD: S/W encryption	SSD: SED
Startup	7.90	6.97	7.99	82.50	47.90	95.33
App Loading	7.03	5.77	5.71	48.33	30.77	60.37
Modest size file test	6.13	5.00	5.28	41.13	26.77	50.40
Large Scale Data Read	84.67	52.88	82.75	178.00	70.23	169.33
Large Scale Data Write	79.60	49.50	50.31	170.80	63.60	164.50

자료출처 : https://www.trustedstrategies.com/

What is a TCG OPAL SED ?

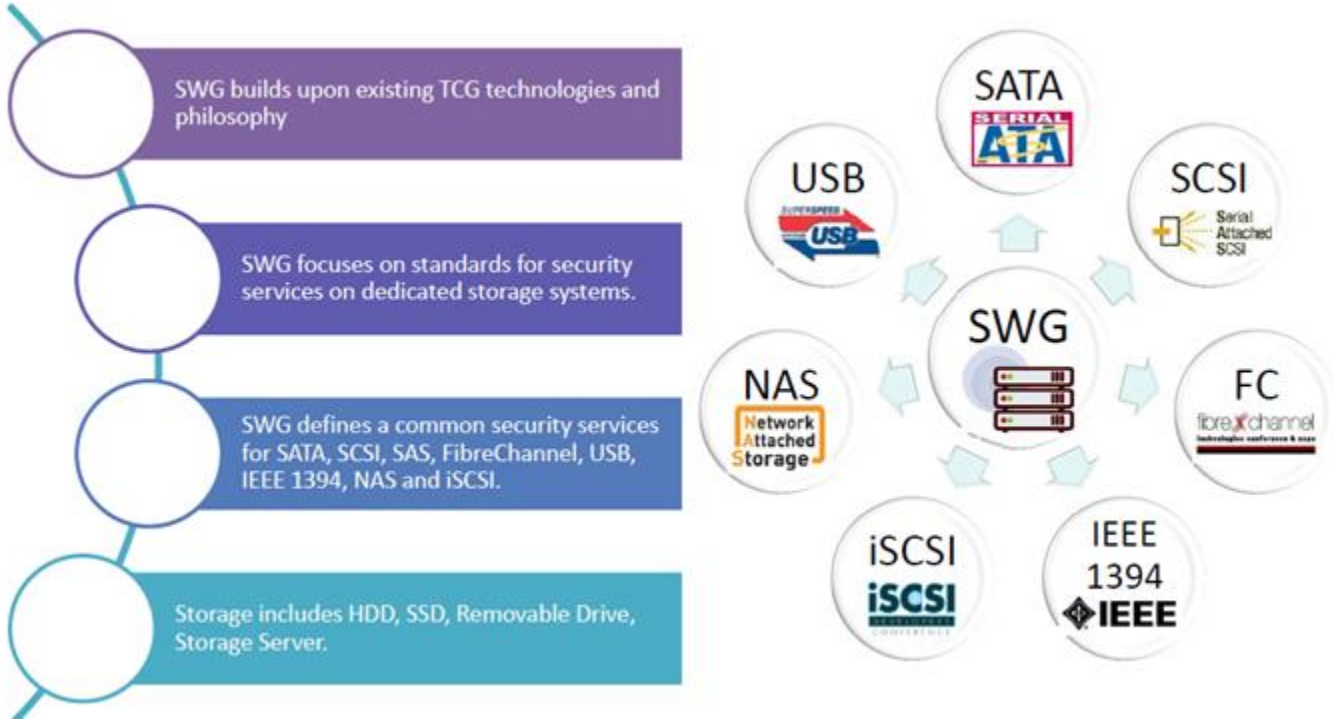
- **TCG(Trusted Computing Group) > SWG(Storage Work Group)**

TCG Members



TCG SWG

(Storage Work Group)

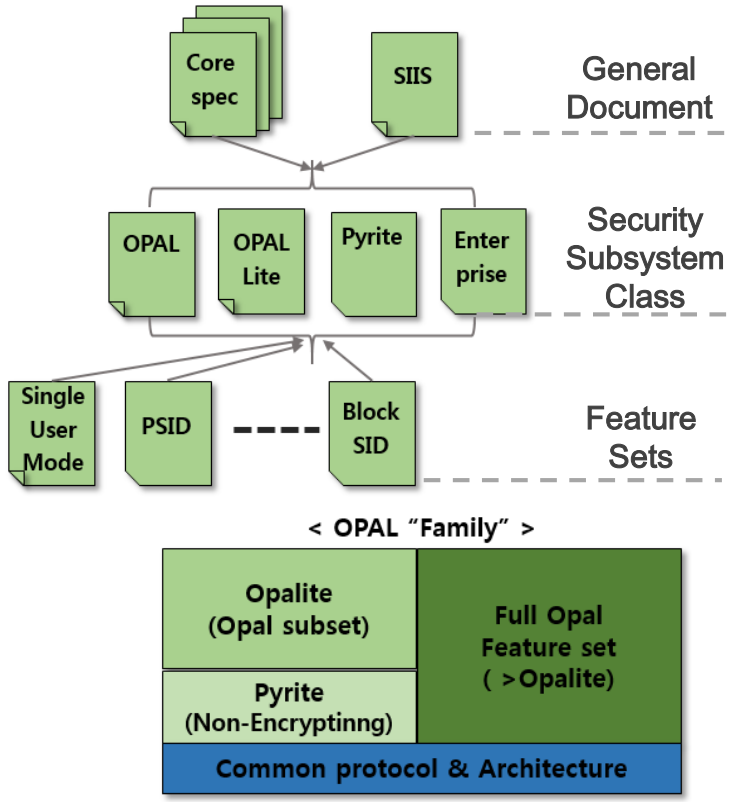


자료출처 : www.trustedcomputinggroup.org

What is a TCG OPAL SED ?

- **TCG(Trusted Computing Group) > SWG(Storage Work Group)**

TCG Storage Specifications



TCG SWG Motivation

TCG OPAL/Enterprise SSCs address the DAR problem

- Data leak through stolen or lost laptop or storage device
- End of life and disposal
- Provides Encrypting/Locking
- Simple password based authentication

With TCG OPAL SED

- Compared to S/W-based encryption solutions, SEDs offer many benefits to user

Zero impact on hardware performance

Seamless integration

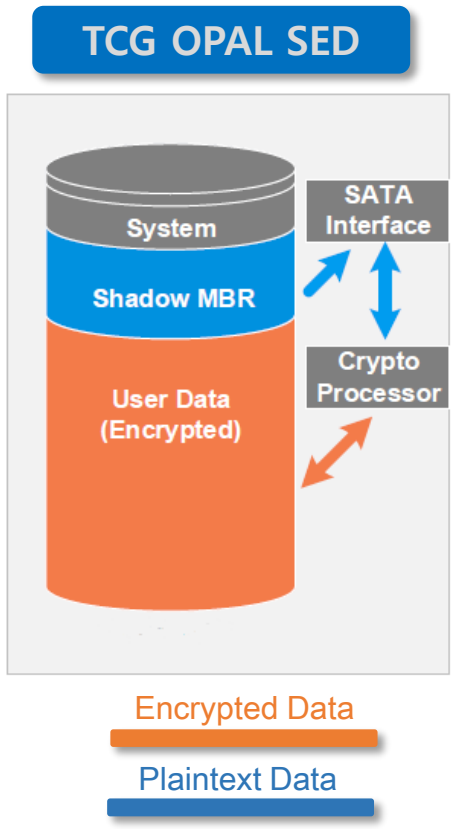
Remote SED management

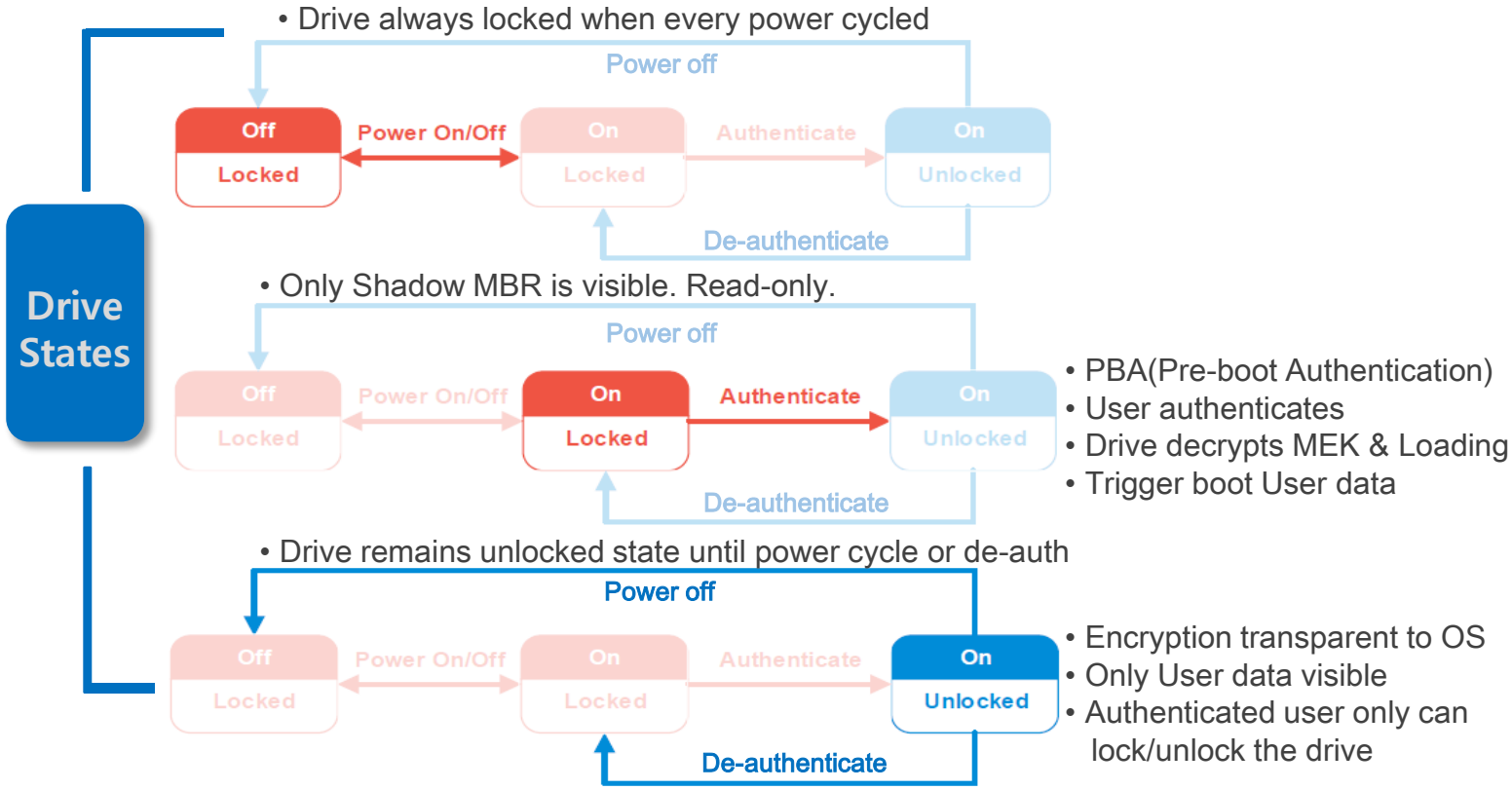
Constant encryption

What is a TCG OPAL SED ?

TCG OPAL SED Contents

- **System Area**
  - TCG Tables and Templates
  - MEK(Media Encryption Key)
  - FW variables and settings, etc.
- **Shadow MBR**
  - Pre-Boot Environment
- **User Data Area**
  - Always Encrypted with MEK
  - Potential for Multiple Ranges(or bands) with different MEK

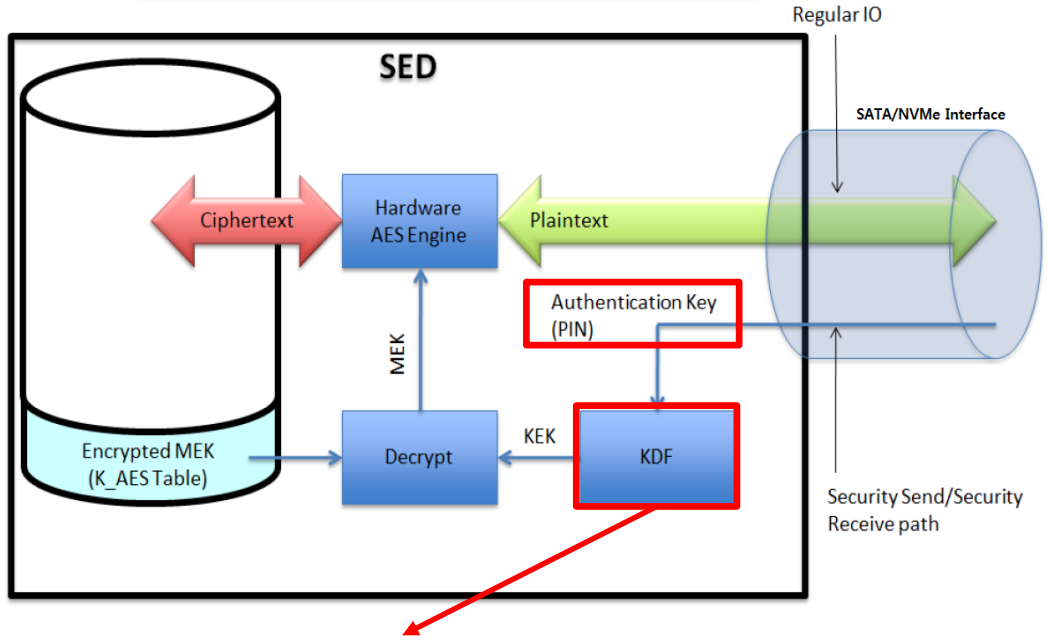




What is a TCG OPAL SED ?

TCG OPAL SED Operation flow

TCG OPAL SED Operation flow



PBKDF2(Password-Based Key Derivation Function 2)
with SHA256

TCG OPAL SED Layout

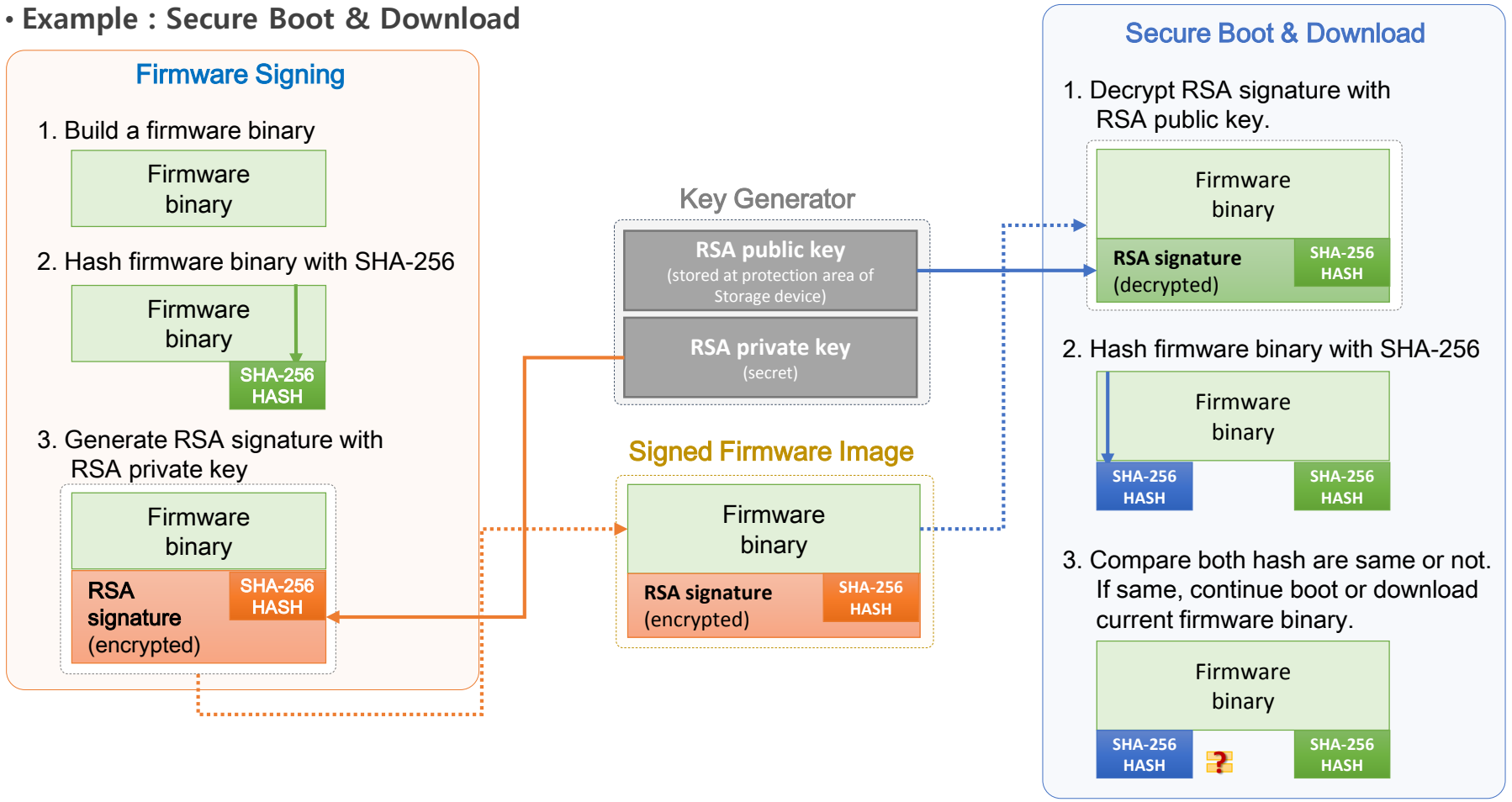
	Size:	Area:	
Device	varies	System (firmware, TCG tables, etc.)	Access with IF-SEND and IF-RECEIVE
	128mb+	Shadow MBR Region	Typically contains pre-boot authentication app
	1k+	DataStore	Typically contains pre-boot variables
User (LBA 0 to LBA [Max])	varies	Global Range	Default range, contains user data
	Varies, set by admin	Range 1	Admin-configured range, contains user data
	Varies, set by admin	Range 2	Admin-configured range, contains user data
	varies	Global Range, Continued	(rest of the default range that is not used by any admin-configured LBA ranges)

자료출처 : www.trustedcomputinggroup.org

Appendix – Additional Security Features

- Digitally Signed Firmware Binaries
- All vendor unique commands or other abilities, including for debug, must be protected
- Security versioning, logging, etc.

• **Example : Secure Boot & Download**



Thank You

SK hynix