**Data in Transit**

Data in transit or Data in motion means moving/sending a data from one location to another location. Here, data can be moved across the public/private network, internet and/or from device to device. This includes our daily activities like browsing online, accessing and sending email, and accessing application in cloud.

**Data at Rest**

Data at rest refers a stored data on any physical storage device, includes company sensitive data, backup of any other sensitive data and data files on employees laptop.

Data at rest denotes data stored in computer systems, including files on an employee's laptop, company files on a server, or copies of these files on an off-site tape backup. Securing data at rest in a cloud is not drastically different than securing it outside a cloud environment. A customer deploying in a PaaS environment needs to find the risk level acceptable and make sure that the cloud provider is the primary custodian of the data.

Full Disk Encryption method encrypts all the files which are stored on hard disk or drive that includes file system/operating system. This encryption will be done as sector wise on hard disk. The filter driver encrypts every file at boot, those are stored in hard disk and decrypts all the files when required. An encryption and decryption process is transparent to user and application.

A full disk encryption can be implemented using hardware or software to safe guard the sensitive data at rest. Self-Encryption Drive(SED) is a hardware based disk encryption methods, it was developed by Trusted Computing Group(TCG). A SED ensures the security by encrypting data and locking an entire disk/drive. To unlock the drive, an authentication key is required when disk is start running then Data Encryption Key (DEK) used to decrypt the data. These key won’t be stored in Trusted Platform Module(TPM). A TPM is a crypto processor module stores cryptographic keys and it is typically attached with motherboard.

Most of the full disk encryption methods provides encryption key at pre-boot in different stages: by inserting USB which contains key, using One-Time Password(OTP), using passphrase or password and using biometric devices. A multi-factors authentication can be implemented using two or more above methods to strengthen the authentication.

1. [Link-Full Disk Encryption](https://wentzwu.com/2021/03/15/cissp-practice-questions-20210316/)

Most full disk encryption products allow users to provide the system’s encryption key at the pre-boot stage in several ways: in the form of a password or passphrase; by inserting a USB drive containing the encryption key; using a one-time password-generating device such as an RSA token; or using a biometric device such as a fingerprint reader (usually connected to a [Trusted Platform Module](https://en.wikipedia.org/wiki/Trusted_Platform_Module) which holds the actual encryption key).

A combination of two or more of these methods can be used to create multifactor authentication, for greater encryption strength and added security. As information is read from the disk that is protected by full disk encryption, it is decrypted on the fly and stored in memory – and any information written to the disk is also encrypted on the fly. Without the encryption key, the data stored on the disk remains inaccessible to thieves and hackers.

1. [Link 2](https://www.esecurityplanet.com/mobile/full-disk-buyers-guide/)