Full-Disk Encryption (FDE)

Return to Glossary

Full-Disk Encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion. Without the proper authentication key, even if the hard drive is removed and placed in another machine, the data remains inaccessible. FDE can be installed on a computing device at the time of manufacturing or it can be added later on by installing a special software driver.

The advantage of FDE is that it requires no special attention on the part of the end user after he initially unlocks the computer. As data is written, it is automatically encrypted. When it is read, it is automatically decrypted. Because everything on the hard drive is encrypted, including the operating system, a disadvantage of FDE is that the encrypting/decrypting process can slow down data access times, particularly when virtual memory is being heavily accessed.

FDE is especially useful for laptops and other small computing devices that can be physically lost or stolen. Because one key is used to encrypt the entire hard drive, FDE on the corporate level requires the network administrator to enforce a strong password policy and provide an encryption key backup process in case an employee forgets his password or leaves the company unexpectedly. Source: https://whatis.techtarget.com/definition/full-disk-encryption-FDE