

Table 3-1. Characteristics of Storage Encryption Technologies

SpyProof!

Characteristic	Full Disk Encryption	Volume Encryption	Virtual Disk Encryption	File/Folder Encryption
<b>Typical platforms supported</b>	Desktop and laptop computers	Desktop and laptop computers, volume-based removable media (e.g., USB flash drives)	All types of end user devices	All types of end user devices
<b>Data protected by encryption</b>	All data on the media (data files, system files, residual data, and metadata)	All data in the volume (data files, system files, residual data, and metadata)	All data in the container (data files, residual data and metadata, but not system files)	Individual files/folders (data files only)
<b>Mitigates threats involving loss or theft of devices?</b>	Yes	Yes	Yes	Yes
<b>Mitigates OS and application layer threats (such as malware and insider threats)?</b>	No	If the data volume is being protected, it sometimes mitigates such threats.* If the data volume is not being protected, then there is no mitigation of these threats.	It sometimes mitigates such threats*  See discussion on website	It sometimes mitigates such threats*
<b>Potential impact to devices in case of solution failure</b>	Loss of all data and device functionality	Loss of all data in volume; can cause loss of device functionality, depending on which volume is being protected	Loss of all data in container	Loss of all protected files/folders
<b>Portability of encrypted information</b>	Not portable	Not portable	Portable	Often portable

\* These storage encryption technologies can only protect the files against some OS and application layer threats if the user has not been authenticated in this session to access the files. If a single sign-on solution is used, then generally the user is authenticated to the storage encryption technology during OS login, so the files are not protected against these threats once OS login occurs. If a separate authentication solution is used, the files are protected until that separate authentication is performed.