9.7.9 File Encryption Facts

Encryption of files, directories, and hard drives provides an additional level of data security. File encryption is part of a layered defense strategy and helps to protect confidential data in the event that physical, password, and ACL safeguards are breached. The following table lists some file encryption programs:

Implementation	Description
Encrypting File System	The Encrypting File System (EFS) encrypts files and folders stored on NTFS partitions. Use EFS to protect data on workstations whose physical security cannot be guaranteed, such as workstations in unsecured locations or laptops. Files are encrypted with EFS using a process called *key encapsulation*: 1. The user saves the file. 2. The system generates a symmetric key or a file encryption key (FEK). This key is used to encrypt the file contents. Later versions of Windows use a combination of AES, SHA, and ECC for encryption. 3. The encryption key is then encrypted using asymmetric encryption with the user's public key and stored in the file header in the Data Decryption Field (DDF). 4. The encryption key can also be encrypted using the public key of a data recovery agent (DRA). This allows a trusted agent to open (decrypt) the file if the user's private key is lost or corrupted. DRAs can be: - A local DRA for the individual workstation. - A domain-wide DRA for the entire domain. Only a domain administrator can set up a domain-wide DRA. The system must also have joined a domain. Additional authorized users can be given access. In this case, the symmetric key is decrypted using the added user's private key. Additional security considerations are: - EFS encryption is tied to a user account. EFS file encryption is compromised if the user's password is compromised. - A file cannot be encrypted by the user if the user's key becomes corrupted or the user's account is deleted. - The encryption process is transparent to the user and the applications using the file. - When the encryption attribute is set on a directory, all files and subdirectories within the directory are encrypted. A file is automatically unencrypted when it is moved or copied to a non-NTFS formatted device or media, such as a thumb drive. A file is also automatically unencrypted when you copy a file over the network using the SMB protocol.
GNU Privacy Guard and Pretty Good Privacy	*GNU Privacy Guard* (GPG) is an encryption tool that encrypts emails, digitally signs emails, and encrypts documents. GPG is an implementation of the Pretty Good Privacy (PGP) protocol. PGP make products available that can be used to protect laptops, desktops, USB drives, optical media, and smart phones. Both PGP and GPG: - Follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data. - Use both asymmetric and symmetric cryptography: 1. GPG/PGP generates a random symmetric key and uses it to encrypt the message. 2. The symmetric key is then encrypted using the receiver's public key and sent along with the message. 3. When the recipient receives a message, GPG/PGP first decrypts the symmetric key with the recipient's private key. 4. The decrypted symmetric key is then used to decrypt the rest of the message. GPG supports DSA, ElGamal, RSA, AES, 3DES, Blowfish, MD5, and SHA-1. DSA and ElGamal are used by default. GPG is unable to use IDEA because IDEA is patented. PGP can use either RSA or the Diffie-Hellman algorithm for asymmetric encryption and IDEA for symmetric encryption.
BitLocker	BitLocker Drive Encryption, or full volume encryption, protects offline data access on lost or stolen laptops or other compromised systems in the following way: - BitLocker encrypts the entire contents of the operating system partition, including operating system files, swap files, hibernation files, and all user files. A special BitLocker key is required to access the contents of the encrypted volume. - BitLocker uses TPM (Trusted Platform Module) to perform integrity checking early in the boot process to ensure that the drive contents have not been altered and that the drive is in the original computer. If any problems are found, the system will not boot, and the drive contents remain encrypted. The integrity check prevents hackers from moving the hard disk to another system in order to try to gain access to its contents. BitLocker differs from the Encrypting File System (EFS) in the following ways: - BitLocker encrypts the entire volume. EFS encrypts individual files. - BitLocker encrypts the disk partition containing the C:\ volume along with the master boot record.

	▪ BitLocker does not encrypt the system partition that contains the boot files. ▪ BitLocker encrypts the volume regardless of the user. Any user who has the PIN or startup key and who can successfully log on can access a BitLocker volume. With EFS, only the user who encrypted the file and any additionally designated users can access the file. ▪ BitLocker only protects files against offline access. If the computer boots successfully, any authorized user who can log on can access the volume and its data. EFS protects against offline access as well as online access for unauthorized users. EFS does not provide online protection if an authorized user's credentials are compromised. DriveLock is another solution that includes disk encryption.