13.8.6 BitLocker Facts

BitLocker protects against unauthorized data access on lost or stolen laptops and on other compromised systems.

- 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 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 requires data to be decrypted before it can be used, which reduces disk I/O throughput.
- BitLocker is available only on Ultimate and Enterprise editions of Windows.
- In Windows 8 and later, you can choose to encrypt the entire volume or just the used space on the volume.

BitLocker uses the following components:

Component	Description
BitLocker partition	Implementing BitLocker requires two NTFS partitions: - The system partition is a 100 MB volume that contains the boot files. This partition is set to active, and is *not* encrypted by the BitLocker process. - The operating system partition must be large enough for the operating system files. This partition is encrypted by BitLocker. Be aware of the following: - A new Windows installation creates both partitions prior to the installation of the operating system files. - For operating systems already installed on a single partition, you may need to resize the existing partition and create the system partition required by BitLocker.
Trusted Platform Module (TPM)	A Trusted Platform Module (TPM) is a special hardware chip included on the computer motherboard that contains software in firmware that generates and stores cryptographic keys. The TPM chip must be enabled in the BIOS/UEFI. The TPM chip stores the BitLocker key that is used to unlock the disk partitions and stores information about the system to verify the integrity of the system hardware. The TPM ensures system integrity as follows: 1. The TPM examines the startup components present on the unencrypted partition. 2. Based on the hardware and system components, a system identifier is generated and saved in the TPM. 3. At startup, components are examined and a new system identifier is generated. 4. The new identifier is compared to the saved identifier. If the identifiers match, the system is allowed to boot.
Non-TPM Security	You have the following options for implementing Bitlocker on systems without a TPM chip: - You can save the BitLocker key on a USB device. The USB device is inserted before starting the computer and provides authentication before the operating system drive is decrypted. The BIOS must support reading USB devices during startup. - Windows 8 and later allows you to configure an unlock password for the operating system drive. To use this feature, enable Configure Use Of Passwords For Operating System Drives policy in the Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives node of Computer Configuration. - Windows supports authentication using a smart card certificate. The smart card certificate is stored on a USB device and is used similarly to the BitLocker key on a USB device.

BitLocker differs from the Encrypting File System (EFS) in the following ways:

- BitLocker encrypts the entire volume. EFS encrypts individual files.
- BitLocker encrypts the volume for use on the computer, 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 can access the file unless access has been granted to other users.
- BitLocker protects files against offline access only. 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.