

Episode Title: Manage Windows BitLocker Drive Encryption

Objectives:

At the end of this episode, I will be able to:

1. Describe how BitLocker encrypts drive contents
2. Explain BitLocker recovery methods
3. Configure BitLocker on a Windows Server

Key Points:

Key Point 1

BitLocker uses a Trusted Platform Module on-premises to encrypt operating system and data drives. In Azure, it also provides Trusted Launch and Platform Attestation features.

Key Point 2

There are a few different recovery options including Entra ID, Active Directory, USB drives, or even printed keys.

Key Point 3

BitLocker can be configured locally on a system through the graphical interface, PowerShell, or by using Group Policy.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- BitLocker overview
: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>