Introducing Microsoft Defender for Endpoint

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

1. Describe the Microsoft Defender for Endpoint product

Learner Objective: *Describe Microsoft Defender for Endpoint*

Description: In this episode, you will learn the basics about Microsoft Defender for Endpoint.

- Microsoft Defender for Endpoint is designed to protect laptops, phones, tablets, PCs, and more from various security threats including malware attacks.
- The product is available in two plans - Plan 1 and Plan 2
- There is also a new Microsoft Vulnerability Management add-on that is available with Plan 2
- Defender for Endpoint uses the following technologies built in to Windows 10 or Windows 11:
    - Endpoint behavioral sensors
    - Cloud security analytics
    - Threat intelligence
- The core components of Microsoft Defender for Endpoint are:
    - Core Defender Vulnerability Management
    - Attack surface reduction
    - Next-generation protection
    - Endpoint detection and response
    - Automated investigation and remediation
    - Microsoft Threat Experts
    - Centralized administration
    - Data sent to Microsoft 365 Defender
    - Integration with Defender for Cloud, Sentinel, Intune, Defender for Cloud Apps, Defender for Identity, Defender for Office, Skype for Business
- Requirements:
    - Microsoft Edge
    - Google Chrome
    - Windows 11 Enterprise, Pro, or Education
    - Windows 10 Enterprise, Pro, IoT
    - Windows 8.1 Enterprise or Pro
    - Windows 7 SP1 Enterprise or Pro
    - Windows Server 2008 R2 SP1 or greater
    - Azure Virtual Desktop
    - MacOS
    - Linux
    - Android
    - iOS
    - Cores: 2 minimum; 1 GB memory
    - Microsoft Defender Antivirus in active or passive mode (passive mode is used when you rely on an alternative antivirus solution)

Additional Resources:

Microsoft Defender for Endpoint
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide