Filename: microsoft-ms101-7-1-1-plan-windows-defender-atp-solution
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Windows Defender Advanced Threat Protection (ATP)
EpisodeName: Plan Windows Defender ATP Solution
Description: Adam and Wes discuss how to plan for the Windows Defender ATP solution.

Plan Windows Defender ATP Solution

Implement Microsoft 365 Security and Threat Management (30-35%)

Implement Windows Defender Advanced Threat Protection (ATP)
• Plan Windows Defender ATP Solution
• Configure Preferences
• Implement Windows Defender ATP Policies
• Enable & Configure Security Features of Windows 10 Enterprise

==========

Plan Windows Defender ATP Solution

Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's cloud service:

```
Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and
```

process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.

```
Cloud security analytics: Leveraging big-data & machine-learning, behavioral
```

signals are translated into insights, detections, and recommended responses to advanced threats.

```
Threat intelligence: Generated by Microsoft hunters, security teams, and
```

augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

Licensing requirements

Microsoft Defender Advanced Threat Protection requires one of the following Microsoft Volume Licensing offers:

```
• Windows 10 Enterprise E5
• Windows 10 Education E5
• Microsoft 365 E5 (M365 E5) which includes Windows 10 Enterprise E5
```

Browser requirements

Access to Microsoft Defender ATP is done through a browser, supporting the following browsers:

```
• Microsoft Edge
• Internet Explorer version 11
• Google Chrome
```

Hardware and software requirements

Supported Windows versions:

```
• Windows 7 SP1 Enterprise
• Windows 7 SP1 Pro
• Windows 8.1 Enterprise
• Windows 8.1 Pro
• Windows 10, version 1607 or later
• Windows 10 Enterprise
• Windows 10 Education
• Windows 10 Pro
• Windows 10 Pro Education
• Windows Server 2008 R2 SP1
• Windows Server 2012 R2
• Windows Server 2016
• Windows Server 2016, version 1803
• Windows Server 2019
```

Other supported operating systems

```
• macOSX
• Linux
• Android
```

NOTE: You will need to know the exact Linux distros, Android, and macOS versions that are compatible with Microsoft Defender ATP for the integration to work.

Microsoft Defender Security Center portal:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/portal-overview

Network and data storage and configuration requirements

When you run the onboarding wizard for the first time, you must choose where your Microsoft Defender Advanced Threat Protection-related information is stored: in the European Union, the United Kingdom, or the United States datacenter.

NOTE: You cannot change your data storage location after the first-time setup.

Diagnostic data settings

You must ensure that the diagnostic data service is enabled on all the machines in your organization. By default, this service is enabled, but it's good practice to check to ensure that you will get sensor data from them.

Use the command line to check the Windows 10 diagnostic data service startup type:

Open an elevated command-line prompt on the machine:

```
a. Go to Start and type cmd
b. Right-click Command prompt and select Run as administrator
```

Enter the following command, and press Enter:

```
sc qc diagtrack
```

NOTE: If the START_TYPE is not set to AUTO_START, then you will need to set the service to automatically start.

```
sc config diagtrack start=auto
```

Windows Defender Antivirus configuration requirement

The Microsoft Defender ATP agent depends on the ability of Windows Defender Antivirus to scan files and provide information about them.

NOTE: You must configure Security intelligence updates on the Microsoft Defender ATP machines whether Windows Defender Antivirus is the active antimalware or not.

When Windows Defender Antivirus is not the active antimalware in your organization and you use the Microsoft Defender ATP service, Windows Defender Antivirus goes on passive mode.

If your organization has disabled Windows Defender Antivirus through group policy or other methods, machines that are onboarded to Microsoft Defender ATP must be excluded from this group policy.

If you are onboarding servers and Windows Defender Antivirus is not the active antimalware on your servers, you should not uninstall Windows Defender Antivirus. You will need to configure it to run on passive mode.

Windows Defender Antivirus Early Launch Antimalware (ELAM) driver is enabled

If you are running a third-party antimalware client and use Mobile Device Management solutions or System Center Configuration Manager (current branch) version 1606, you will need to ensure that the Windows Defender Antivirus ELAM driver is enabled.

IN ADDITION TO ALL THAT, NOTE THESE THINGS FOR THE EXAM:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

```
1. Ports 80 & 443 are in use to communicate between the client and the portal

2. Traffic is anonymous, and not tied to any client user

3. If using SSL, you must exempt or whitelist the service URLs so the traffic
```

is not inspected

```
4. netsh can be used to set a static proxy if necessary

5. You can use Group Policy to configure a registry based static proxy

6. You can test connectivity using the Windows Defender ATP Connectivity
```

Analyzer tool

INTEGRATIONS ARE IMPORTANT !!!

```
Microsoft Cloud App Security
Azure ATP
o365 Threat Intelligence
Windows Server with the Microsoft Monitoring Agent
Down-Level Windows clients
SIEM
```

NOTE: Microsoft ATA IS NOT on the list !!!