
NESEC
ALWAYS SECURE, NEVER AT RISK

OneSec Defender for Endpoint – Migration offer

ONESEC

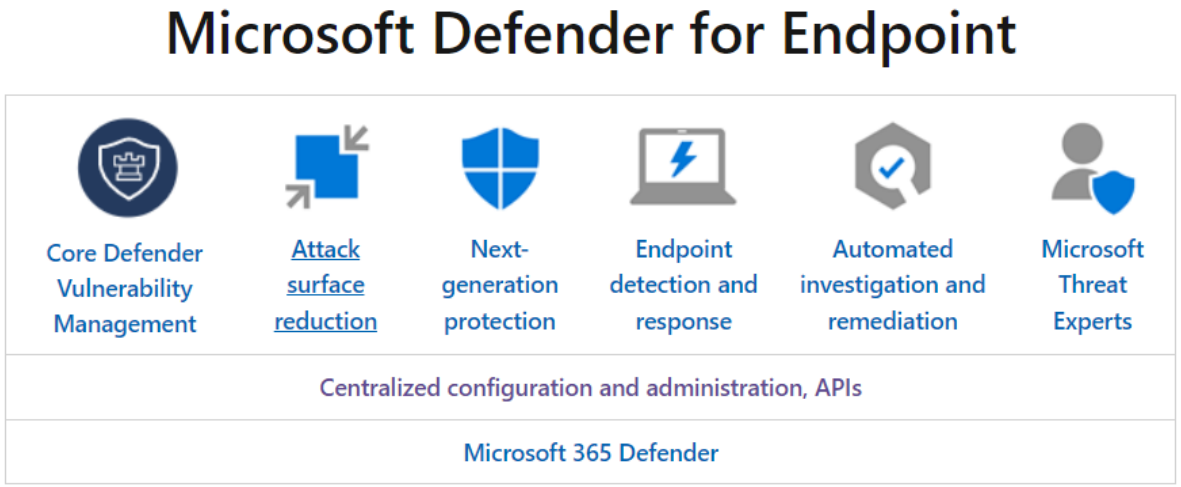
Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
Defender for Endpoint uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

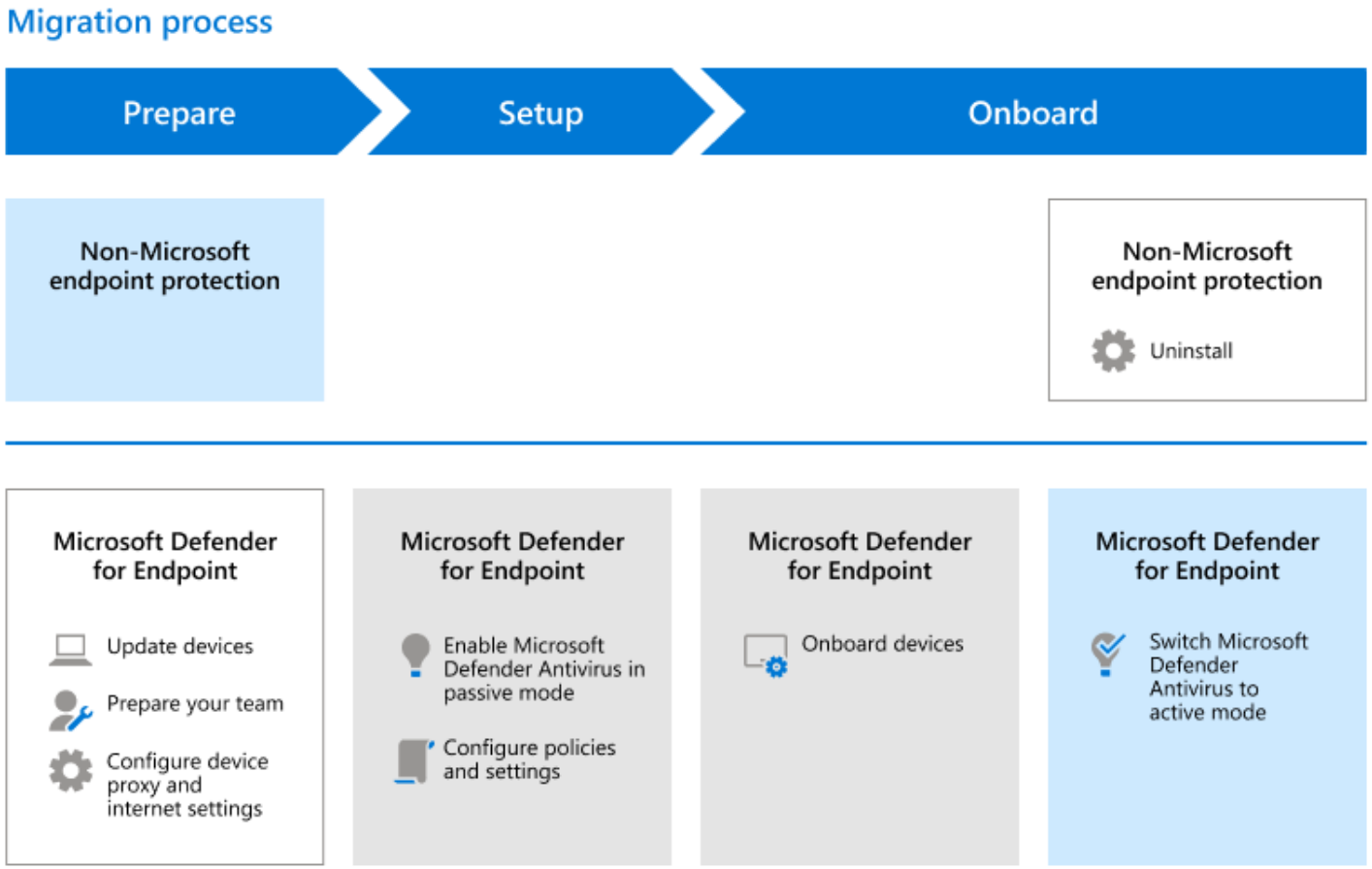
- Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and send this sensor data to your private, isolated, cloud instance of Microsoft Defender for Endpoint.

- Cloud security analytics: Leveraging big-data, device learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, 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 Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they are observed in collected sensor data.



Migrate to Microsoft Defender for Endpoint from non-Microsoft endpoint protection



When you migrate to Defender for Endpoint, you begin with your non-Microsoft antivirus/antimalware protection in active mode. Then, you configure Microsoft Defender Antivirus in passive mode, and configure Defender for Endpoint features. Then, you onboard your organization's devices, and verify that everything is working correctly. Finally, you remove the non-Microsoft solution from your devices.

The process of migrating to Defender for Endpoint can be divided into three phases:

1. Prepare for your migration
2. Set up Defender for Endpoint
3. Onboard to Defender for Endpoint

OneSec Defender for Endpoint – Migration offer

The OneSec Defender for Endpoint – Migration offer helps your organization in the process of migrating to Microsoft Defender for Endpoint on Windows 10/11 devices. Our offering provides the guidelines based on Microsoft best practices, assistance, and support to Migrate to Microsoft Defender for Endpoint from non-Microsoft endpoint protection.
The migration process requires an approximate time of 5 weeks and consists of 3 main phases:

Phase 1- “Prepare for your migration”
1 Week

OneSec Defender for Endpoint – Migration offer **Required Information & Deliverables**

Required Information

- ✓ Current AD Connect version
- ✓ OS version (Enterprise, Pro, etc) Windows 10/11 of the endpoints?
- ✓ Release of the Operating System (20H2, 22H2, etc.) Windows 10/11 that the endpoints have?
- ✓ Current protection tool (Antimalware) on endpoints?
- ✓ Do the endpoints have the System Center Configuration Manager agent installed?
- ✓ Are the endpoints enrolled in the Microsoft Endpoint Manager platform (Microsoft Intune)?

Deliverables

- ❖ Design document and migration architecture to Microsoft Defender for Endpoint based on current technologies available to the client
- ❖ Functional specification document detailing the configurations made in the Microsoft Defender for Endpoint console

Technical Requirements

- Microsoft Security Console Access (https://security.microsoft.com) with administrator privileges
- Compatible Windows versions
    - Windows 11 Enterprise
    - Windows 11 Education
    - Windows 11 Pro
    - Windows 11 Pro Education
    - Windows 10 Enterprise
    - Windows 10 Enterprise LTSC 2016 (or later)
    - Windows 10 Enterprise loT
    - Windows 10 Education
    - Windows 10 Pro
    - Windows 10 Pro Education
- The Defender hardware requirements for device endpoints are the same for supported editions.
    - Cores: 2 minimum and 4 preferred
    - Memory: 1 GB minimum, 4 preferred
- Administrator User:
    - Microsoft Defender for Endpoint license assignment
    - Security Administrator or Global administrator
- End user:
    - Microsoft Defender for Endpoint license assignment
- Define and validate security policies.
- Uninstalling the current Antivirus solution.
- Enabling/Updating the Microsoft Defender (Antivirus) solution.
- Not having a restriction policy in the Active Directory that disables the execution of the following services:
    - Windows Advanced Threat Protection
    - Windows Defender
    - Telemetry
- Note: In case of having this policy, the teams that were part of the Project must be excluded.
- Computer Firewall exceptions: Configure and validate Microsoft Defender Antivirus network connections | Microsoft Learn