wanstor

Microsoft 365 Defender for Endpoint

Service Description

Confidentiality and copyright

EXECUTIVE SUMMARY

Microsoft Defender for Endpoint is a complete enterprise endpoint security platform that is used to prevent, detect, investigate, and respond to many different threats to endpoint devices in the enterprise through technologies that are built into windows 10/11 and technologies offered through Microsoft's cloud services.

Defender for Endpoint leverages the following combination of robust technologies:

- **Endpoint behavioural sensors** - Embedded in Windows 10/11, these sensors collect and process behavioural 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, behavioural 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.
- **Centralized configuration and integration with Microsoft solutions** – Defender integrations into existing workflows and integrates with solutions such as Defender for cloud, Microsoft Sentinel, Intune, Defender for Cloud Apps, Identity, and Office 365.

Defender for Endpoint Plans

Defender for Endpoint is available in three plans, The following summarizes what's included with each plan.

Feature / Capability	**Defender for Endpoint Plan 1**	**Defender for Endpoint Plan 2**	**Defender for Business ***
	Standalone	**Enterprise Customers**	**Enterprise Customers**
Centralized Management	✓	✓	✓
Attack surface reduction capabilities	✓	✓	✓
Next-generation protection	✓	✓	✓
Cross-platform support (Windows, macOS, iOS, and Android OS)	✓	✓	✓
Partner APIs	✓	✓	✓
Endpoint detection and response	✗	✓	✓ [2]
Automated investigation and response	✗	✓	✓ [3]
Threat analytics	✗	✓	✓ [5]
Threat & vulnerability management	✗	✓	✓
Simplified client configuration	✗	✗	✓
Threat hunting and six months of data retention	✗	✓	✗ [4]
Microsoft Threat Experts	✗	✓	✗

*** Defender for Business notes:**
Up to **300 employees**
EDR capabilities include behaviour-based detection and four **manual response actions**: Run AV scan, Isolate device, stop and quarantine the file, and add an indicator to block or allow.
Automated investigation and response turned **on by default.**
No timeline view for Defender for Business.
Threat Analytics is **optimized for small and medium-sized** businesses.

Defender for Server Plans

Defender for Server is available in two plans, The following summarizes what's included with each plan.

Feature / Capability	Defender for Server Plan 1	Defender for Server Plan 2
Microsoft Defender for Endpoint	✓	✓
Microsoft threat and vulnerability management	✓	✓
Automatic agent onboarding, alert, and data integration	✓	✓
Just-in-time VM access for management ports	✖	✓
Network layer threat detection	✖	✓
Adaptive application controls	✖	✓
File integrity monitoring	✖	✓
Adaptive network hardening	✖	✓
Integrated vulnerability assessment powered by Qualys	✖	✓
Log Analytics 500MB free data ingestion	✖	✓

Defender for Server notes:

1. For non-Azure servers, Azure Arc is required, and Defender for Cloud for Servers needs to be enabled.
2. For Azure VMs Defender for Cloud for Servers needs to be enabled.

Defender for Endpoint deployment

For all Windows end-user devices in scope, Wanstor will complete the following deployment steps:

- **Prerequisites**: Wanstor will confirm that device prerequisites have been met and are in line with objectives.
- **Review current antivirus product**: Wanstor will review the current status of your existing antivirus, and document all policies, including exclusion lists, and current license count. Wanstor will then review and plan Defender policies based on findings.
- **Purchase required licensing**: If not already purchased, Wanstor will ensure adequate licensing has been purchased and applied to the users.
- **Implement Defender policies and configuration**: Based on Wanstor best practice for Defender for Endpoint configuration, Wanstor will enable and implement the Defender for Endpoint policies and configuration (new configuration includes: attack surface reduction, Endpoint detection, and response).
- **Prepare for migration**: Wanstor will ensure all devices have had windows updates recently installed, and remove any policies that might be disabling Defender for your endpoint devices.
- **Setup Defender for Endpoint**: Wanstor will enable or reinstall Defender Antivirus and set it to passive mode. If required, add Defender to the existing antivirus exclusion list.
- **Onboard to Defender for Endpoint**: Wanstor will onboard all devices to Defender for Endpoint, run detection tests and confirm Defender is running in passive mode, and update Defender with the latest definitions.
- **Review attack surface reduction rules**: Wanstor will review the attack surface reduction rules in audit mode, add exclusions based on findings and implement blocking mode based on best practice.
- **Remove existing Antivirus product**: Once all devices have been onboarded to Defender for Endpoint, Wanstor will remove the existing antivirus product and ensure Defender for Endpoint moves from passive mode to active mode, and that ensure Defender for Endpoint works as expected.

- **Configure Alerting rules:**
  - **For customers that wish to manage their own alerting**: Wanstor will configure Windows Defender for Endpoint alerting rules and specify the high, medium, and low alerts to email the teams that the customer has defined.
- **For customers that purchase E5, Business Premium, and Defender for Server Plan2**: Wanstor will review the threat and vulnerability reporting and recommend a remediation plan, a separate quote to remediate the threats and vulnerabilities can be requested.
- **Defender for office 365, Defender for Cloud Apps**: Depending on the licenses, Wanstor will configure both Defender for Office 365, and Defender for Cloud Apps as part of the deployment of Defender for Endpoint.

Defender for Server deployment

If it has been identified that servers need to be migrated over as part of the migration, the following steps will be performed by Wanstor.

- **Prerequisites**: Confirm that the device prerequisites have been met and are in line with objectives.
- **Deploy and add on-premise servers to Azure Arc**: Any server not running in Azure will be added to the Azure Arc service, and depending on the plan chosen, configured to match the endpoint plan. Additional resource requirements include log analytic workspaces, resource groups, and existing resources if required/exist.
- **Enable Defender for Cloud – Defender for Servers**: For both Azure Arc and Azure Virtual machines, Defender for Server needs to be enabled. Wanstor will enable auto-provisioning and integrations to ensure new devices are onboarded in the future.
- **Implement Defender policies and configuration**: Based on Wanstor best practice for Defender for Endpoint configuration, Wanstor will enable and implement the Defender for Endpoint policies and configuration (new configuration includes: attack surface reduction, Endpoint detection, and response).
- **Prepare for migration**: Ensure all devices have had windows updates recently installed (for Server 2012 R2 and 2016 ensure the latest monthly rollup packages are installed), add a group policy, or manually edit the server registry to force passive mode for servers.
- **Onboard Servers to Defender for Server**: Onboard all supported servers to Defender for Servers by either installing the agent and running the onboarding package, or from 2019 onward, running onboarding package.

  Ensure passive mode is set for servers and run detection tests and confirm Defender is running in passive mode,

  Update Defender with latest definitions. **Note**: For passive mode to work on endpoints running Windows Server 2016 and Windows Server 2012 R2, those endpoints must be onboarded before Passive mode can be enabled.
- **Remove existing Antivirus product**: Once all servers have been onboarded to Defender for Cloud, Wanstor will remove the existing antivirus product, and ensure any group policies preventing Defender from changing to Active mode are removed and needed manually change the registry keys to allow **Active mode**, Wanstor will ensure Defender for Servers works as expected.

Project Deliverables

Defender for Endpoint

Assumptions

Customer's endpoint devices: Meet the pre-requisites defined by Microsoft:

https://docs.microsoft.com/en-us/microsoft-365/security/Defender-endpoint/minimum-requirements?view=o365-worldwide

Administrative accounts: Sufficient permissions to complete the project are met before the start of the project. This includes M365 global admin, on-premise accounts, cloud accounts, and any third-party service that falls in scope of the completing the project. One account coving all permissions is also accepted.

Licenses: Purchased before the start of the project, or approval given to the engineer to purchase the licenses when required.

VPN access where needed: Where on-premises systems exist, access to the private networks via means of a VPN or other connectivity method.

Device management

- Existing devices are enrolled in Intune: if this is not already in place, further time will need to be added to the project.
- Existing Antivirus console for uninstallation tasks to remove old antivirus or uninstallation scripts that can be run through the MDM solution.
- For Servers, an Azure subscription configured with Wanstor's implementation of Azure Lighthouse for Engineer access. Can be implemented as part of the project.
- For M365 Services implementation of Wanstor's GDAP to allow engineer access as required. Can be implemented as part of the project.