Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

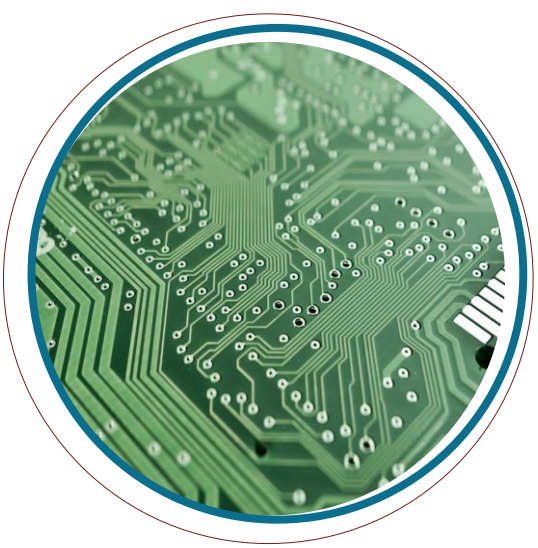
November 2024

Module 3

Endpoint Protection

Module 3 Contents:

- **Attack Surface Reduction**
  - Endpoint Security Policies
  - ASR Capabilities
- **Next-generation Protection**



Attack Surface Reduction

Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

Attack Surface Reduction

'Attack surfaces are all the places where your organization is vulnerable to cyberthreats and attacks …

… Defender for Endpoint includes several capabilities to help reduce your attack surfaces.'

ASR Capabilities

- Hardware Isolation
- ASR rules
- Application control
- Controlled folder access
- Device control
- Network protection
- Web protection
- Exploit protection

Enable ASR capabilities

Several methods available

- PowerShell
- Group Policy
- Microsoft Configuration Manager
- Microsoft Intune
  - for enrolled devices
  - for MDE-enrolled devices
- Endpoint Security Policies
  - for MDE-enrolled devices
  - Service-to-Service connection required

Source: https://learn.microsoft.com/en-us/mem/intune/protect/mde-security-integration#architecture

Service-to-Service connection

This connection offers some capabilities

- Risk Information of devices are usable in Intune and CA policies
- Each onboarded device gets device identity in Entra ID for communication with Intune
  - for already joined or hybrid joined devices the existing device ID is used
  - for new devices, a new syntactic device ID will be created
- Endpoint security policies could be used
  - Intune policies could be enforced by MDE for non-enrolled devices

Service-to-Service connection

Configuration

- must be done in both portals or both services (Intune and MDE)

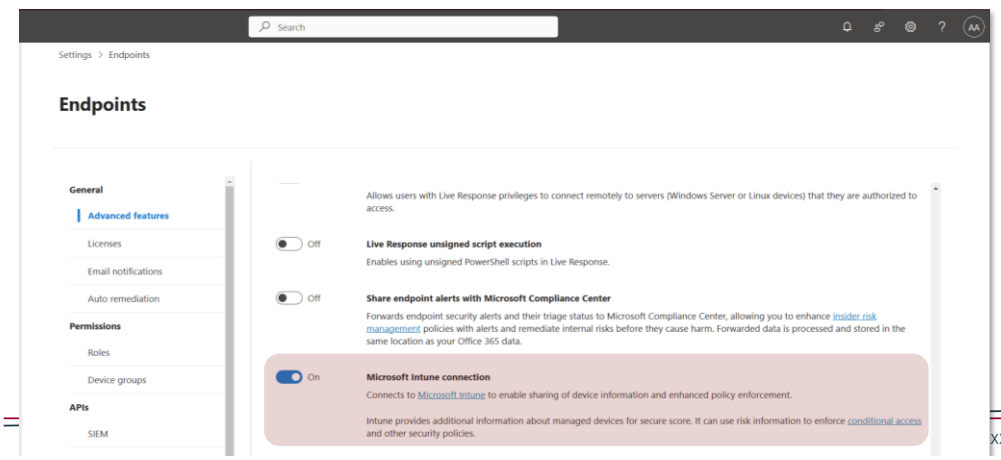
MDE portal

- Navigate to Settings | Endpoint | Adv Features
- Search for 'Microsoft Intune Connection' and set it to 'On'
- Click 'Save preferences'

Service-to-Service connection

Configuration

- MDE portal



MDE Settings

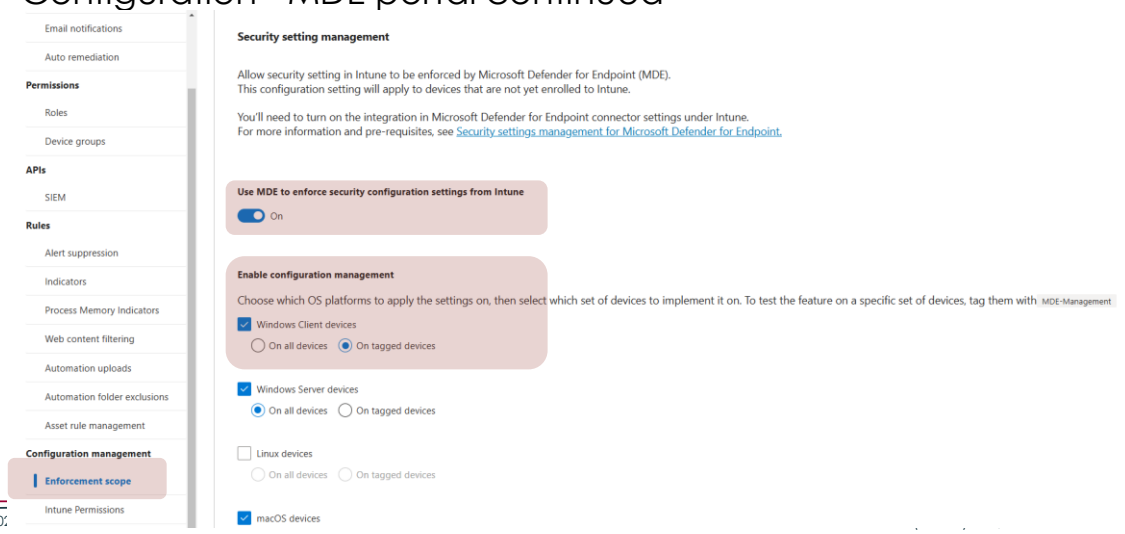
Service-to-Service connection

Configuration - MDE portal continued

- Navigate to Settings | Endpoint | Configuration management/Enforcement scope
- Set 'Use MDE to enforce security configuration settings from Intune' to 'On'
- Under 'Enable configuration management' select all OS platforms for which you want to use MDE as authority
- Scroll down till the end of page and click 'Save'

Service-to-Service connection

Configuration - MDE portal continued



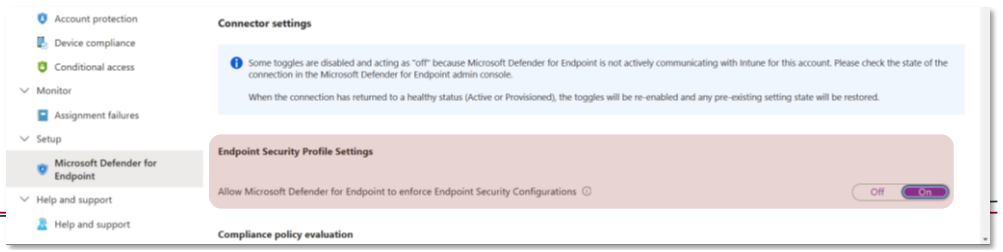
Service-to-Service connection

Configuration

Intune portal

- Navigate to Endpoint security | Setup/Microsoft Defender for Endpoint
- Set Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configuration' to 'On'
- Click 'Save'

Intune portal



15

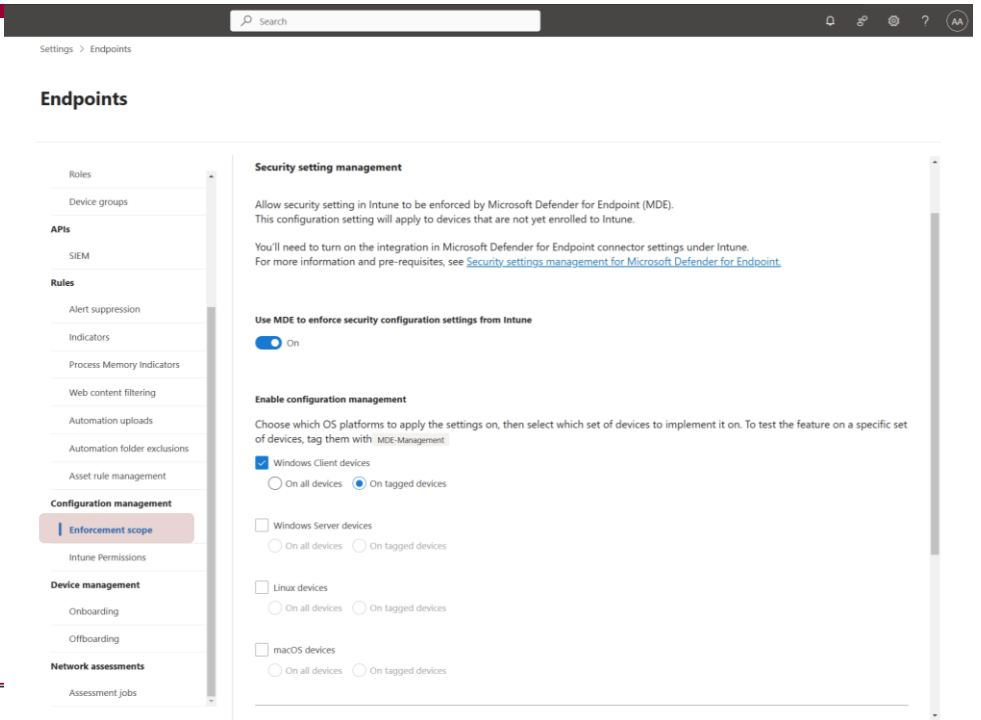
Service-to-Service connection

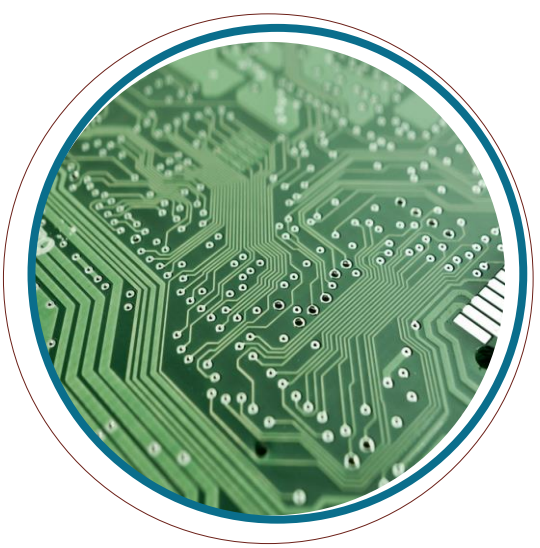
Configuration - Intune portal continued

- For using device risk level in Intune set Compliance policy evaluation to 'On'
- Maybe you change 'Number of days until partner is unresponsive'
- Click 'Save'

16

MDE settings





Attack Surface Reduction

ASR Capabilities

ASR Capabilities - MS Guide

- Hardware Isolation
- ASR rules
- Application control
- Controlled folder access
- Device control
- Network protection
- Web protection
- Exploit protection

ASR Capabilities - Course sequence

- Hardware Isolation
- ASR rules
- Controlled folder access
- Device control
- Network protection
- Web protection
- Application control
- Exploit protection

ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Source: https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/microsoft-defender-application-guard/reqs-md-app-guard

Hardware Isolation

- Available for Microsoft Edge and Windows applications
- untrusted sites are browsed in an isolated container

Prerequisites:

- Software and Hardware
  - refer to the source link
- Windows Feature 'Microsoft Defender Application Guard'
  - could be installed via Intune e.g.
- Administrator declares trusted sites
  - Intune portal: ASR | Policy profile: App and Browser Isolation

Source: https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/microsoft-defender-application-guard/reqs-md-app-guard

Hardware Isolation

- Available for Microsoft Edge, Windows applications
- untrusted sites are browsed in a container

DEPRICATED
Under Windows 11 24H2 no longer available

Prerequisites:

- Software and hardware
  - refer to the source
- Windows Features 'Microsoft Defender Application Guard'
  - could be installed e.g.
- Administrator defines trusted sites
  - Intune portal: ASR | Policy profile: App and Browser Isolation

ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Source: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-deployment
https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference

ASR Rules

'ASR rules target certain unsecure software behaviors.'

Examples

- Block Office apps from creating executable content
- Block rebooting machine in Safe Mode
- Bloc execution of potentially obfuscated scripts
- …

Source: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#per-asr-rule-alert-and-notification-details

ASR Rules

Modes

Audit

- see how a rule would affect the user's process without blocking

Block

- user's process blocked

Warn

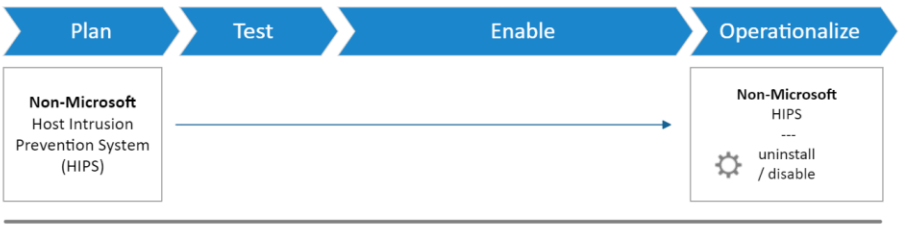
- user's process blocked, but can be overwritten by user

Notification & alerts

If a rule is triggered:

- User gets a display notification
  - this could be customized
- Alert is generated
  - Shown in XDR portal
  - refer to source for reference

ASR Rules deployment guide



Plan	Test *ring (n)*	Enable *ring (n) to implement*	Enable - *part 2* *ring (n) + 1*	Operationalize *all rings*
1. Identify business units 2. Identify ASR Rules champions 3. Inventory line-of-business apps, understand business unit processes 4. Prepare reporting and response team roles and responsibilities 5. Define rings	1. Start with the first ring 2. Enable ASR rules in **Audit** mode 3. Understand reporting in the Microsoft 365 Defender portal 4. Assess impact 5. Define exclusions	1. Continuing with ring (n), set ASR rules to **Block** or **Warn** mode 2. Use **Warn** mode for problematic rules - Focus on easy rules first 3. For {rules = **Block**}, assess impact, refine exclusions	1. Move the next ring into the Test phase, then into Enable 2. Continue until all rings are enabled (set to Block or Warn) 3. When all rings are enabled and exclusions configured, proceed to the Operationalize phase	- Review processes regularly - Review reports daily, watch for outliers - Review exclusions - Use ASR Rules events for hunting and forensics

28

ASR Rules Configuration

- Endpoint Security Policy
  - Template: Attack Surface Reduction Rules
- Intune
  - Attack surface reduction | Policy Profile ASR

29

Source: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#asr-rule-to-guid-matrix

ASR Rules Configuration

- PowerShell
  - Add-MpPreference
  - AttackSurfaceReductionRules_Ids refer to source
  - ASRRuleActionTypes:
    - Disabled, Enabled, AuditMode, NotConfigured, Warn
- GPO
  - Computer Configuration > Administrative templates > Windows Components > Microsoft Defender Exploit Guard > Attack Surface Reduction
  - Value Name = GUID of Rule
  - Value = Mode as Integer

ASR Rules Troubleshooting

- Querying active rules
  - PowerShell: Get-MpPreference
  - Properties AttackSurfaceReductionRules_Ids and AttackSurfaceReductionRules_Actions
- Querying events
  - Event Viewer: Microsoft-Windows-Windows Defender/Operational
- Get Antimalware logs
  - MpCmdRun.exe -getfiles (for MS Support)

ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Source: https://learn.microsoft.com/en-us/defender-endpoint/controlled-folders#what-is-controlled-folder-access

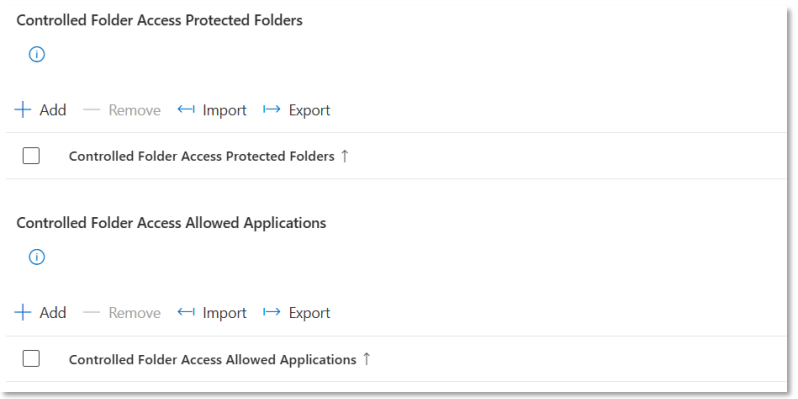
Controlled Folder Access

- *'Controlled folder access helps protect your valuable data from malicious apps and threats, such as ransomware. Controlled folder access protects your data by checking apps against a list of known, trusted apps.'*

- turned on by
  - Endpoint Security policy
  - Intune
  - Endpoint Config Manager
  - Windows Security App

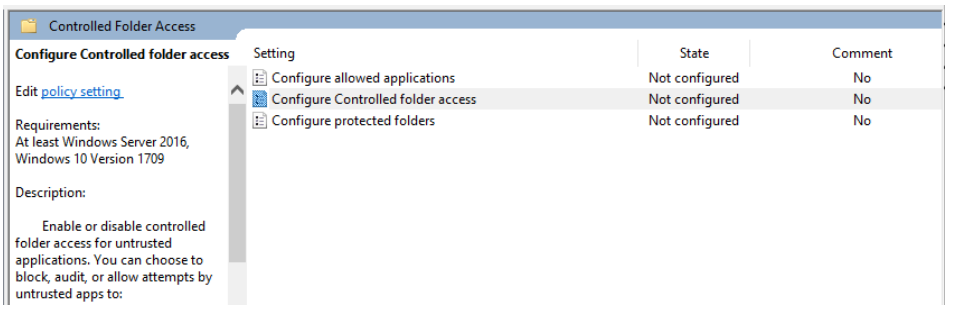
Controlled Folder Access configuration

- Endpoint Security policy (Template ASR)
- Intune (Attack surface reduction | Policy Profile ASR)



Controlled Folder Access configuration

- GPO
  - Computer Configuration > Administrative Templates
  - Windows Components > Microsoft Defender Antivirus > Microsoft Defender Exploit Guard > Controlled folder access



Controlled Folder Access configuration

- PowerShell

```
Add-MpPreference -ControlledFolderAccessProtectedFolders @('c:\localData')
Add-MpPreference -ControlledFolderAccessAllowedApplications @('C:\windows\notepad.exe')
Set-MpPreference -EnableControlledFolderAccess Audit # Enalbed, Disabled
```


ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Source: https://learn.microsoft.com/en-us/defender-endpoint/device-control-overview

Device Control

'Device control helps protect your organization from potential data loss, malware, or other cyberthreats by allowing or preventing certain devices to be connected to users' computers.
'

Capabilities in Windows OS

- Bitlocker
- Device installation

Capabilities in MDE

- Granular access control
- Reporting and advanced hunting

Also available in Endpoint data loss prevention (Endpoint DLP)

Device Control

Already in Windows OS

- Bitlocker
- Device installation restriction

Managed via GPOs

MDE

- Granular access control
- Reporting and advanced hunting

Managed via

- Endpoint Security Policy
- Intune ASR policies
- GPO

Device Control Policies

Device installation restriction (examples)

- Prevent installation of removable devices
- Allow installation of devices using drivers that match these device setup classes
- Allow installation of devices that match any of these device instance IDs
- Allow installation of devices that match any of these device IDs

Take this for reference:

- Policy CSP - DeviceInstallation
- USB device class drivers in Windows

Device Control Policies

Removable Storage Access

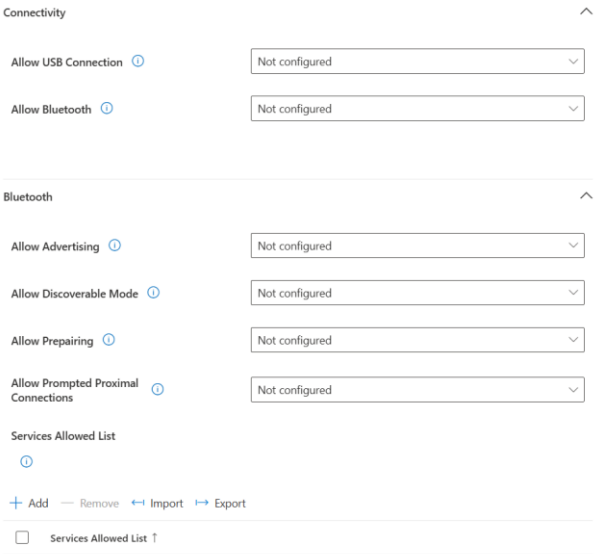
- WPD Devices: Deny read access
- WPD Devices: Deny write access

Take this for reference:

- WPDDevices_DenyRead_Access
- WPDDevices_DenyWrite_Access

Device Control Policies

Bluetooth



Source: https://learn.microsoft.com/en-us/defender-endpoint/device-control-deploy-manage-gpo

Device Control deployment

- Endpoint Security policy
  - Template Device Control
- Intune
  - Attack surface reduction | Policy Profile Device Control
- GPO
  - refer to source

ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Network Protection

'Network protection is an attack surface reduction capability that helps prevent people in your organization from accessing domains that are considered dangerous through applications.'

Foundation for

- Web Threat in 3rd party Browsers
- Web Content Filtering
- Custom Indicators

Network Protection

Prerequisites

- MDAV is in active mode
- Behavior Monitoring is enabled
- Cloud Protection is enabled
  - and network connectivity is functional

Network Protection

Enabling

- Endpoint Security Policy
  - Template: Microsoft Defender Antivirus
  - Policy: Enable Network Protection
  - Setting: Enabled - Audit - Disabled

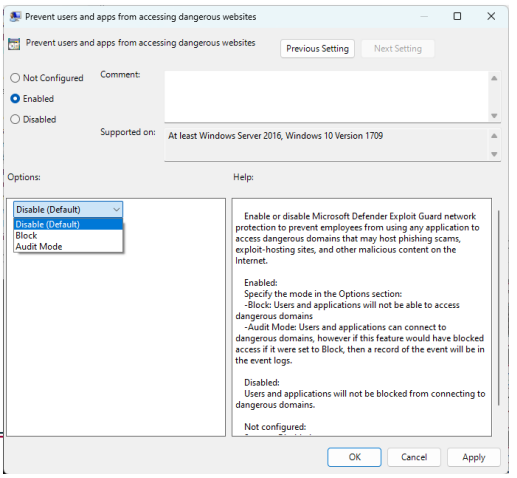
- PowerShell

```
Set-MpPreference -EnableNetworkProtection AuditMode
# parameter values: Enabled or AuditMode or Disabled
```

Network Protection

Enabling

- GPO
  - Computer configuration
    > Administrativ templates
  - Windows components
    > Microsoft Defender Antivirus
    > Microsoft Defender Exploit Guard
    > Network protection



Network Protection

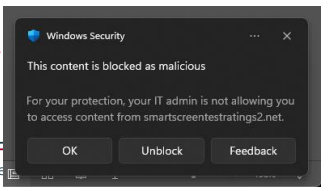
Evaluation

- PowerShell

```
Get-MpPreference | Format-List -Property EnableNetworkProtection
# 0: Disabled
# 1: Enabled
# 2: AuditMode
```

```
Invoke-WebRequest -Uri 'https://smartscreentestratings2.net'
```

- Browser
  - Navigate to https://smartscreentestratings2.net



ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Source: https://learn.microsoft.com/en-us/defender-endpoint/web-protection-overview

Web Protection

- 'Web protection lets you secure your devices against web threats and helps you regulate unwanted content.'

- made up of
  - Web threat protection
  - Web content filtering
  - Custom indicators

- discussed later

ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Application Control

- *'[…] allows organizations to control which drivers and applications are allowed to run on their Windows clients.'*

- Policies used for configuration
- based on
  - Path from which app of file is launched
  - Attributes of app (Filename, version, hash)
  - Reputation of apps (MS Intelligent Security Graph)
  - Attributes of code signing certificate
  - …
- Policies are applied to all users of a managed machine

Source: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/appcontrol-design-guide
https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/appcontrol-wizard

Application Control

- Design Guide
  - refer to source

- Deployment - Higher steps
  - Prepare an endpoint as reference
  - Donwload App Control for Business Wizard
  - Create a policy file (*.xml)
  - Convert the policy to a binary file
  - Deploy binary file

Source: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/deployment/appcontrol-deployment-guide

Application Control

Deployment Methods

- Intune
- Config Manager
- GPO
  - save binary file on network share first
- Script

```
CiTool.exe --update-policy path-to-binary-file.cip
```

ASR Capabilities - Course sequence

Hardware Isolation

ASR rules

Controlled folder access

Device control

Network protection

Web protection

Application control

Exploit protection

Exploit Protection

'Exploit protection automatically applies many exploit mitigation techniques to operating system processes and apps.'

- Features of EMET (Enhanced Mitigation Experience Toolkit) included

Configuration

- Enabled by default
- System and app settings could be set by
  - PowerShell, GPO, Intune (for enrolled devices), Config Manager
  - *not by Endpoint Security Policies*

Source: https://learn.microsoft.com/en-us/defender-endpoint/exploit-protection-reference

Exploits Protection - System and Apps

Mitigation	Description
Control flow guard (CFG)	… mitigates the risk of attackers using memory corruption vulnerabilities by protecting indirect function calls. For example, an attacker may use a buffer overflow vulnerability to overwrite memory containing a function pointer, and replace that function pointer with a pointer to executable code of their choice.
Data Execution Prevention (DEP)	… helps protect against an attacker injecting malicious code into the process, such as through a buffer overflow, and then executing that code.
Force randomization of images (Mandatory ASLR)	Address Space Layout Randomization (ASLR) mitigates the risk of an attacker using their knowledge of the memory layout of the system in order to execute code that is already present in process memory and already marked as executable.
Randomize memory allocations (Bottom-up ASLR)	… adds entropy to relocations, so their location is randomized and therefore less predictable.
Validate exception chains (SEHOP)	… is a mitigation against the *Structured Exception Handler (SEH) overwrite* exploitation technique.
Validate heap integrity	… mitigation increases the protection level of heap mitigations in Windows, by causing the application to terminate if a heap corruption is detected. (Heap = dynamic memory for processes)

Source: https://learn.microsoft.com/en-us/defender-endpoint/exploit-protection-reference

Exploits Protection - Apps only

Mitigation	Description
Arbitrary code guard (ACG)	Prevents the introduction of non-image-backed executable code and prevents code pages from being modified. Can optionally allow thread opt-out and allow remote downgrade (configurable only with PowerShell).
Block remote images	Prevents loading of images from remote devices.
Block untrusted fonts	Prevents loading any GDI-based fonts not installed in the system fonts directory, notably fonts from the web.
Code integrity guard	Restricts loading of images signed by Microsoft, WHQL, or higher. Can optionally allow Microsoft Store signed images.
Disable extension points	Disables various extensibility mechanisms that allow DLL injection into all processes, such as AppInit DLLs, window hooks, and Winsock service providers.
Disable Win32k system calls	Prevents an app from using the Win32k system call table.
Don't allow child processes	Prevents an app from creating child processes.
and some more …	refer to source

Exploit Protection

Configuration with PowerShell

- System level

```
# Enalbes DEP for the system level
Set-ProcessMitigation -System -Enable DEP
# Disables DEP for the system level
Set-ProcessMitigation -System -Disable DEP
# Reset DEP for the system level
Set-ProcessMitigation -System -Remove -Disable DEP
# Reset the system level
Set-ProcessMitigation -System -Reset
```

- possible values for Enable/Disable parameter:
  - use Ctrl + Space

Exploit Protection

Configuration with PowerShell

- App level

```
# Enalbes CFG only for a single app
Set-ProcessMitigation -Name C:\Windows\notepad.exe -Enable CFG
```

- multiple mitigations must be separated by commas
- possible values for Enable/Disable parameter:
  - use Ctrl + Space
- Export all settings

```
Get-ProcessMitigation -RegistryConfigFilePath c:\Temp\myExploitPolicy.xml
```

Exploit Protection

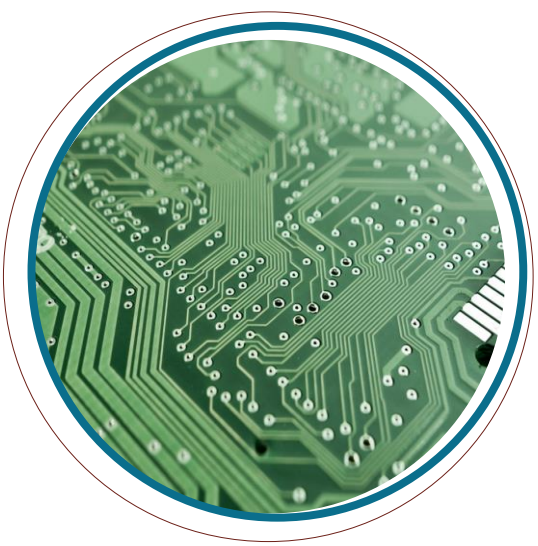
Configuration with PowerShell

- configfile

```
# Export all settings
Get-ProcessMitigation -RegistryConfigFilePath c:\Temp\myPolicy.xml

# Import all settings
Set-ProcessMitigation -PolicyFilePath C:\Temp\myPolicy.xml
```

- This file could be used for a GPO or an Intune Device configuration policy

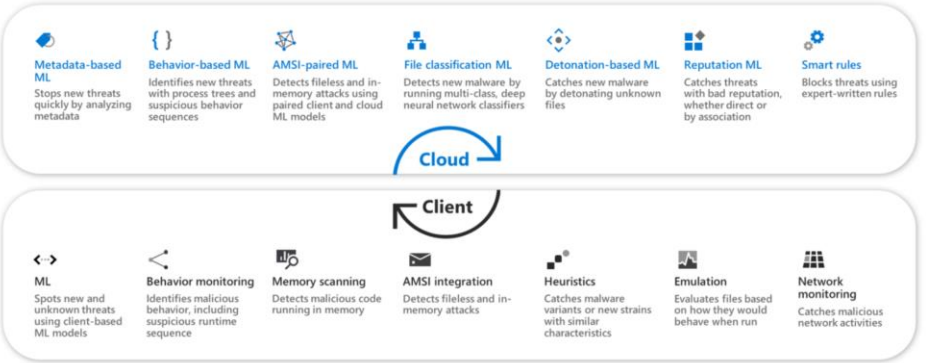


Next-generation Protection

Source: https://learn.microsoft.com/en-us/defender-endpoint/next-generation-protection
https://learn.microsoft.com/en-us/defender-endpoint/adv-tech-of-mdav

Next-generation Protection

'Next-generation protections, such as Microsoft Defender Antivirus blocks malware using local and cloud-based machine learning models, behavior analysis, and heuristics. Microsoft Defender Antivirus uses predictive technologies, machine learning, applied science, and artificial intelligence to detect and block malware at the first sign of abnormal behavior.'



Next-generation Protection

Capabilities

- Cloud protection
- Tamper protection
- Behavioral, heuristic and real-time protection

Next-generation Protection

Microsoft Defender for Antivirus
Capabilities

- Anomaly detection
  - detects not only know malware
  - through ML and cloud protection
- works on- and offline
- stops threats based on behaviours and process trees

- compatible with other antivirus/antimalware solutions

Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-windows#microsoft-defender-antivirus-processes-and-services

Next-generation Protection

Microsoft Defender for Antivirus - Services

Process or service	Where to view its status
Microsoft Defender Antivirus Core service (MdCoreSvc)	- **Processes** tab: Antimalware Core Service - **Details** tab: MpDefenderCoreService.exe - **Services** tab: Microsoft Defender Core Service
Microsoft Defender Antivirus service (WinDefend)	- **Processes** tab: Antimalware Service Executable - **Details** tab: MsMpEng.exe - **Services** tab: Microsoft Defender Antivirus
Microsoft Defender Antivirus Network Realtime Inspection service (WdNisSvc)	- **Processes** tab: Microsoft Network Realtime Inspection Service - **Details** tab: NisSrv.exe - **Services** tab: Microsoft Defender Antivirus Network Inspection Service
Microsoft Defender Antivirus command-line utility	- **Processes** tab: N/A - **Details** tab: MpCmdRun.exe - **Services** tab: N/A
Microsoft Security Client Policy Configuration Tool	- **Processes** tab: N/A - **Details** tab: ConfigSecurityPolicy.exe - **Services** tab: N/A

Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-windows#comparing-active-mode-passive-mode-and-disabled-mode

Next-generation Protection

Microsoft Defender for Antivirus - Modes

Mode	What happens
Active mode	In active mode, Microsoft Defender Antivirus is used as the primary antivirus app on the device. Files are scanned, threats are remediated, and detected threats are listed in yoaur organization's security reports and in your Windows Security app.
Passive mode	In passive mode, Microsoft Defender Antivirus isn't used as the primary antivirus app on the device. Files are scanned, and detected threats are reported, but threats aren't remediated by Microsoft Defender Antivirus. **IMPORTANT**: Microsoft Defender Antivirus can run in passive mode only on endpoints that are onboarded to Microsoft Defender for Endpoint. See Requirements for Microsoft Defender Antivirus to run in passive mode.
Disabled or uninstalled	When disabled or uninstalled, Microsoft Defender Antivirus isn't used. Files aren't scanned, and threats aren't remediated. In general, we don't recommend disabling or uninstalling Microsoft Defender Antivirus.

```
Get-MpComputerStatus | Format-List -Property AMRunningMode
```


Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-windows#comparing-active-mode-passive-mode-and-disabled-mode

Next-generation Protection

Microsoft Defender for Antivirus - Configuration

- MDE Endpoint Security Policy Management
- Microsoft Intune
- Microsoft Configuration Manager
- Group Policy
- PowerShell cmdlets
- WMI

Next-generation Protection

Cloud protection

- *'To identify new threats dynamically, next-generation technologies work with large sets of interconnected data in the Microsoft Intelligent Security Graph and powerful artificial intelligence (AI) systems driven by advanced machine learning models. Cloud protection works together with Microsoft Defender Antivirus to deliver accurate, real-time, and intelligent protection.'*

Foundation for

- Checking against metadata
- Sample submission
- Tamper protection
- …

Source: https://learn.microsoft.com/en-us/defender-endpoint/specify-cloud-protection-level-microsoft-defender-antivirus

Next-generation Protection

Cloud protection level

- Not configured: Default state.
- High: Applies a strong level of detection.
- High plus: Uses the High level and applies extra protection measures (might affect client performance)
- Zero tolerance: Blocks all unknown executables.

Next-generation Protection

Cloud protection timeout

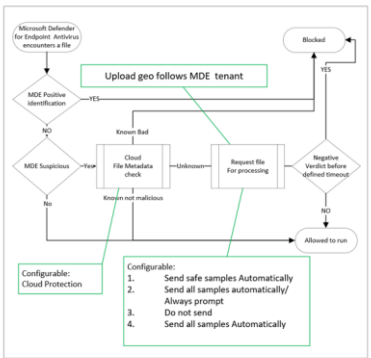
- While investigating a file it is block
- default 10 seconds
- timeout could be extended

Source: https://learn.microsoft.com/en-us/defender-endpoint/cloud-protection-microsoft-antivirus-sample-submission

Next-generation Protection

Cloud protection
Sample submission

Microsoft Defender For Endpoint Cloud-delivered Protection



Setting	Description
Send safe samples automatically	- Safe samples are samples considered to not commonly contain PII data. Examples include .bat, .scr, .dll, and .exe. - If file is likely to contain PII, the user gets a request to allow file sample submission. - This option is the default configuration on Windows, macOS, and Linux.
Always Prompt	- If configured, the user is always prompted for consent before file submission - This setting isn't available in macOS and Linux cloud protection
Send all samples automatically	- If configured, all samples are sent automatically - If you would like sample submission to include macros embedded in Word docs, you must choose **Send all samples automatically** - This setting isn't available on macOS cloud protection
Do not send	- Prevents "block at first sight" based on file sample analysis - "Don't send" is the equivalent to the "Disabled" setting in macOS policy and "None" setting in Linux policy. - Metadata is sent for detections even when sample submission is disabled

Next-generation Protection

Cloud protection - Configuration

- Endpoint security policy | Template Defender AV
- Policies:
  - Allow Cloud Protection
  - Cloud Block level
  - Cloud extended timeout
  - Submit Samples Consent

Next-generation Protection

Cloud protection - Configuration

- PowerShell

```
Set-MpPreference -MAPSReporting Advanced
Set-MpPreference -SubmitSamplesConsent SendAllSamples
```

  - only Cloud protection (MAPSReporting) and SubmitSampleConsent is available

- GPO
  - for all settings possible
  - refer to the documentation

Source: https://learn.microsoft.com/en-us/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection

Next-generation Protection

Tamper protection

- *'Tamper protection is a capability in Microsoft Defender for Endpoint that helps protect certain security settings, such as virus and threat protection, from being disabled or changed.'*

- Configurable in MDE Settings | Endpoint | Advanced Features
- Turned on by default

- to exclude single devices, use Intune or troubleshooting mode

Source: https://learn.microsoft.com/en-us/defender-endpoint/behavior-monitor

Next-generation Protection

Behavior monitoring

'Monitors process behavior to detect and analyze potential threats based on the behavior of applications, services, and files. Rather than relying solely on signature-based detection (which identifies known malware patterns), behavior monitoring focuses on observing how software behaves in real-time.'

- Benefits
  - defending against fileless malware
  - Real-Time threat detection
  - Dynamic Approach

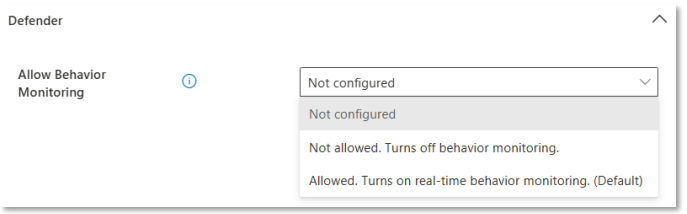
Source: https://learn.microsoft.com/en-us/defender-endpoint/behavior-monitor

Next-generation Protection

Behavior monitoring

Configuration

- Endpoint Security Settings



- PowerShell

```
Set-MpPreference -DisableBehaviorMonitoring $false
Get-MpPreference | Format-List -Property DisableBehaviorMonitoring
```

- GPO
- …

Source: https://learn.microsoft.com/en-us/defender-endpoint/edr-in-block-mode?view=o365-worldwide

Next-generation Protection

EDR in block mode

'*[…] allows Microsoft Defender Antivirus to take actions on post-breach, behavioral EDR detections.*'

- Benefits
  - MDAV in active or passive mode
  - artifacts are classified as malicious in cloud and
  - remediated on endpoint

Configuration

- Settings | Endpoints | Adv Features: EDR in block mode: On

End of Module 3