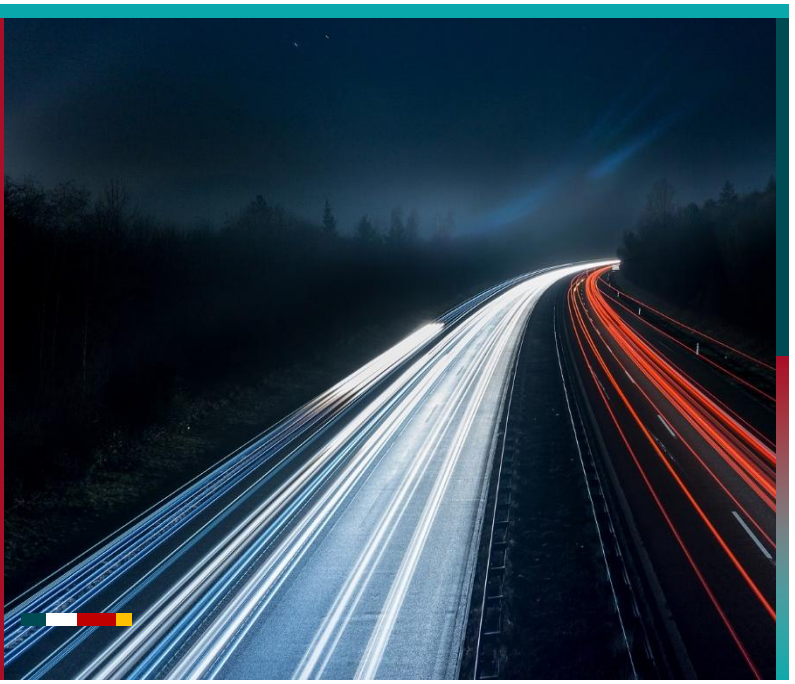
# MDE

## Master Class:

## Microsoft Defender for Endpoint



**Fast Lane**
Worldwide Experts
in Technology Training
and Consulting



1

# Module 5

## Additional Configurations

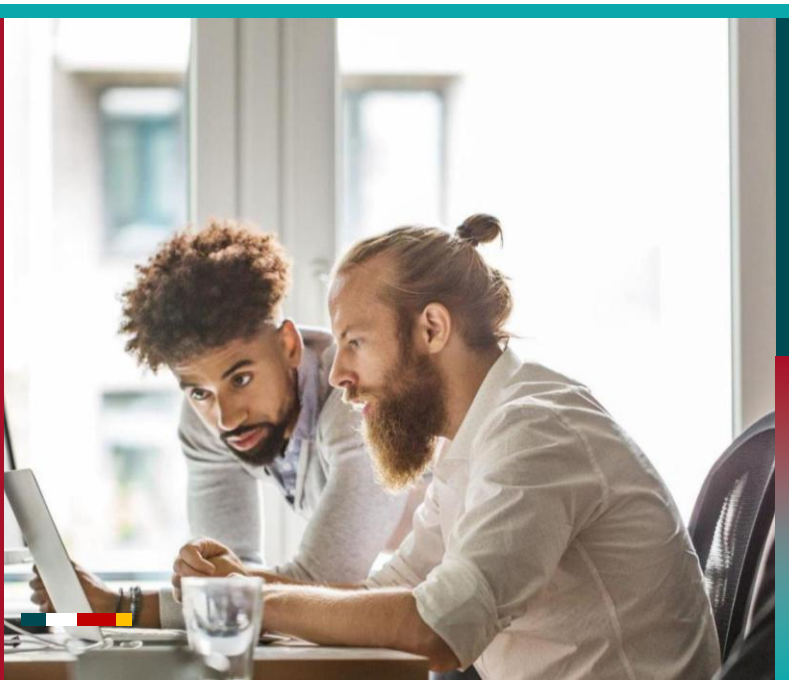
**Fast Lane**
Worldwide Experts
in Technology Training
and Consulting



2

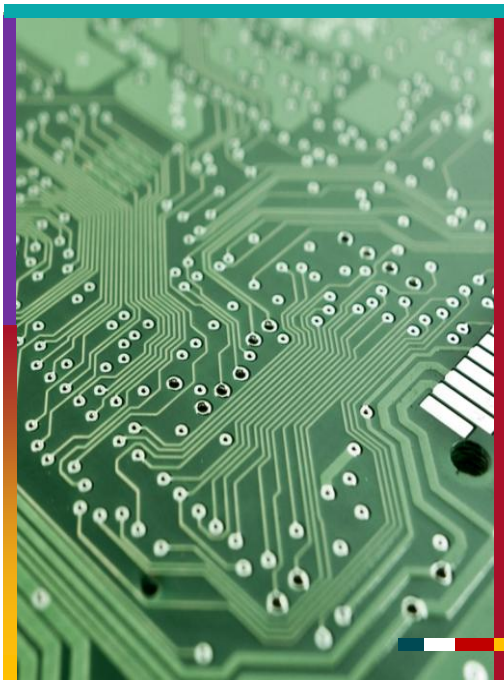
# Content Module 5

- Advanced Features - Overview
- Indicators
- Web Content Filtering
- Vulnerability Management
- Endpoint DLP





3



Source: https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-client

# Advanced Features



4

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

# Advanced Features

Overview

- Restrict correlation to within scoped device groups
- Enable EDR in block mode
- Automatically resolve alerts
- Allow or block file
- Hide potential duplicate device records
- Custom network indicators
- Tamper protection
- Show user details
- Skype for business integration



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

# Advanced Features

Overview

- Microsoft Defender for Cloud Apps
- Web content filtering
- Unified audit log
- Device discovery
- Download quarantined files
- Default to streamlined connectivity
- Apply streamlined connectivity settings ...
- Live Response (3 times)
- Share endpoint alerts with Microsoft Compliance Center

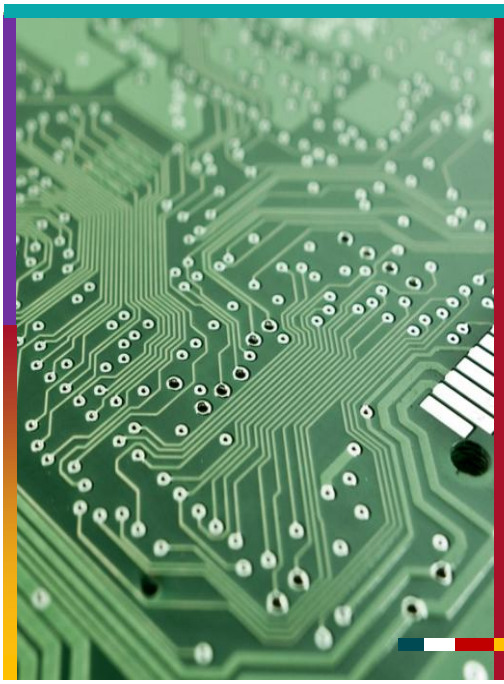
Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

# Advanced Features

Overview

- Microsoft Intune connection
- Authenticated telemetry
- Preview Features





# Indicators

Source: https://learn.microsoft.com/en-us/defender-endpoint/manage-indicators

# Indicators

*'An Indicator of compromise (IoC) is a forensic artifact, observed on the network or host. [...]* This capability gives SecOps the ability to set a list of indicators for detection and for blocking (prevention and response).'

Useful for

- customer known bad files e.g.
- allow false positives

Types




Source: https://learn.microsoft.com/en-us/defender-endpoint/manage-indicators

# Indicators

IoC engines

- Endpoint prevention engine (MDAV)
- Automated Investigation and Remediation (AIR)
- Cloud detection

Enforcement types

- Allow
- Audit
- Warn
- Block execution
- Block and remediate

Source: https://learn.microsoft.com/en-us/defender-endpoint/manage-indicators
Source: https://learn.microsoft.com/en-us/defender-endpoint/manage-indicator

# Indicators

Configuration

Prerequisites for all kind of IoCs

- Behavior Monitoring is enabled
- Cloud-based protection is turned on
- Cloud Protection network connectivity is functional
- Antimalware client version > 4.18.1901.x
- OS: Win 10/11; Win 2012 R2 or later (usual requirements)



Source: https://learn.microsoft.com/en-us/defender-endpoint/manage-indicators

# Indicators

Configuration - **Files**

Prerequisites

- MDAV in active mode
- File hash computation enabled
  - GPO: Computer Configuration|Administrative Templates |Windows Components|Microsoft Defender AV|MpEngine
  - Policy: Enable file hash computation feature
  - PowerShell:

```
Set-MpPreference -EnableFileHashComputation $true
Get-MpPreference | Format-List -Property EnableFileHashComputation
```

Source: https://learn.microsoft.com/en-us/defender-endpoint/manage-indicators

# Indicators

Configuration - **Files**

- Generate File hash of executable (*.exe or *.dll)

```
Get-FileHash -Path 'C:\Temp\notepad++.exe' -Algorithm SHA256
```

- Settings|Endpoints|Rules/Indicators
- Tab 'File hashes'|+ Add item

From file investigation page also possible



Source: https://learn.microsoft.com/en-us/defender-endpoint/indicator-file#policy-conflict-handling

# Indicators

Policy Conflict handling - **Files/Certs**

- Open documentation

Source: https://learn.microsoft.com/en-us/defender-endpoint/indicator-ip-domain#non-microsoft-edge-and-internet-explorer-processes

# Indicators

Configuration - **IPs and URLs**

Prerequisites

- Network protection enabled
- Settings|Endpoints|Adv Features: Custom network indicators: ON

- For Non Microsoft Edge and IE processes
  - TCP, HTTP, HTTPS supported
  - only single IP addresses (no CIDR)
  - not supported in Application Guard sessions



Source: https://learn.microsoft.com/en-us/defender-endpoint/indicator-ip-domain#ioc-ip-url-and-domain-policy-conflict-handling-order

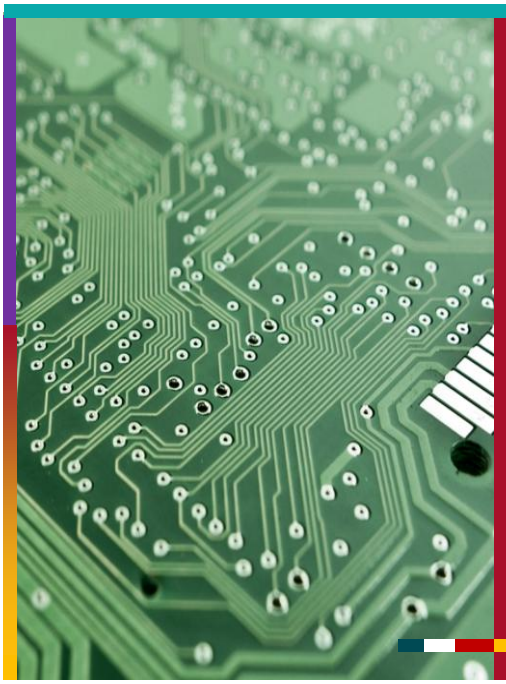
# Indicators

Configuration - **IPs and URLs**

IoC conflict handling order

- *Allow* wins over *Warn* wins over *Block*

- Settings|Endpoints|Rules/Indications
- Tab 'Ip addresses'|+ Add item
- Tab 'URLs/domain'|+ Add item



# Web Protection



17

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



18

# Web protection

**Web threat protection**

- Enabled, if Network protection is enabled

**Custom Indicator**

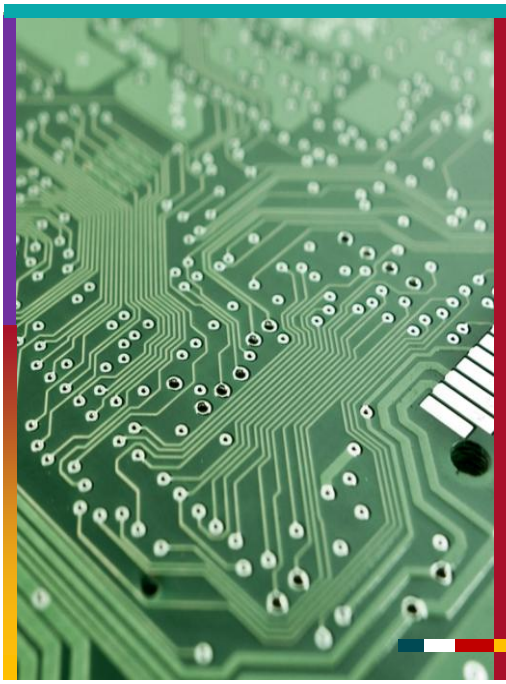
- Settings|Adv Features: Custom network indicators: On
- Configured Settings|Endpoint|Rules/Indicators
- Types:
  - IPs
  - URLs/domains



# Web protection

**Web content filtering**

- Settings|Endpoint|Adv Features: Web content filtering: On
- Configured by policies
  - Settings|Endpoint| Rules/Web content filtering
  - Categories to block
  - Scope: Device Group this filter should be applied



# Vulnerability Managment



Source: https://learn.microsoft.com/en-us/defender-vulnerability-management/defender-vulnerability-management

## Vulnerability Management

*'Vulnerability management serves as an infrastructure for reducing organizational exposure, hardening endpoint surface area, and increasing organizational resilience.'*

# Vulnerability Management

Standalone license provides all features

*MDE P2 Features*

- Device discovery
- Device inventory
- Vulnerability assessment
- Configuration assessment
- Risk based prioritization
- Remediation tracking
- Continuous monitoring
- Software inventory
- Software usages insights

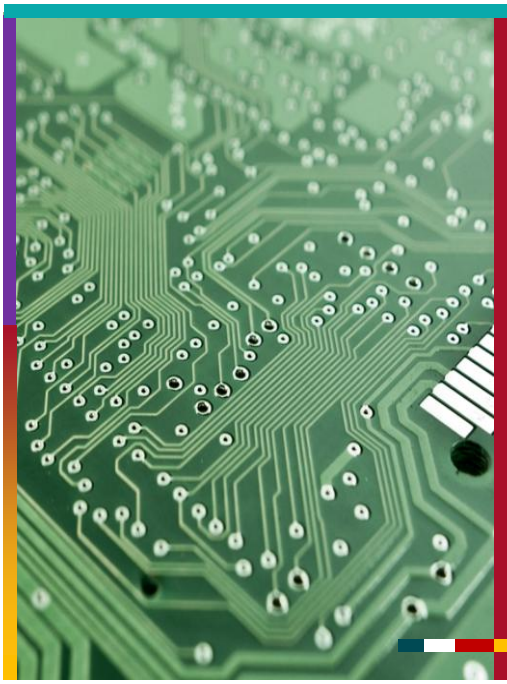
*Add-On Features*

- Security baselines assessment
- Block vulnerable applications
- Browser extensions assessment
- Digital certificate assessment
- Network share analysis
- Hardware and firmware assessment
- Authenticated scan for Windows



# Vulnerability Management

- Portal
- Dashboard
- Recommendations
- Remediation
- Inventories
- Weaknesses
  - Common Vulnerabilites and Exposures (CVEs)
- Event timeline



# Endpoint DLP



25

Source: https://learn.microsoft.com/en-gb/purview/dlp-learn-about-dlp
https://learn.microsoft.com/en-gb/purview/endpoint-dlp-learn-about

## Endpoint Data Loss Prevention

*' To help protect this sensitive data, and to reduce the risk from oversharing, they need a way to help prevent their users from inappropriately sharing sensitive data with people who shouldn't have it. This practice is called* ***data loss prevention (DLP)****.'*

*'* ***Endpoint data loss prevention (Endpoint DLP)*** *extends the activity monitoring and protection capabilities of DLP to Windows 10/11 [and] macOS ... '*



26

# Endpoint DLP

Prerequisites

- Licenses
  - included in M365 E5, E5 Compliance, F5 Compliance
- OS: Windows Client & MacOS
- Activation
  - Turned on in Purview settings
  - reversible
- Onboarding of devices
  - already onboarded MDE devices usable
- Portal
  - https://purview.microsoft.com



# Endpoint DLP - Configuration Settings

- Settings|Date Loss Prevention|**Endpoint DLP settings**
  - Advanced classification scanning and protection
  - File path exclusion
  - Restricted apps and app groups
  - Unallowed Bluetooth apps
  - Browser and domain restrictions to sensitive data
  - Removeable USB device groups
  - ... some more
- Settings|Data Loss Prevention|**Just-in-time protection**

# Endpoint DLP - Configuration Policies

- Configured in Purview portal and solution Data Loss Prevention
- Settings:
  - Name
  - Location (Devices)
  - Mode
- Rule(s):
  - Conditions
    - what is the sensitive information
  - Actions
    - what is allowed to do with sensitive information



## Questions?

**Fast Lane Group**

Worldwide Education & Professional Services

# End of Module 5

**Fast Lane Group**

Worldwide Education & Professional Services