



Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

November 2024

Fast Lane Worldwide Experts in Technology Training and Consulting | Learn.Transform.Succeed.

1

Hello!

Thank you for joining me today

Instructor: DI Thomas Schleich

Microsoft Cybersecurity Architect
Microsoft Azure Solution Architect
Microsoft 365 Administrator Expert
Microsoft Certified Trainer

Self-employed

Trainings:

- Microsoft 365 & Azure Security
- Azure Administration & Solution Architecting
- PowerShell
- Windows Server & Client for Admins

© Copyright Microsoft Corporation. All rights reserved.



2



Module 01

Overview

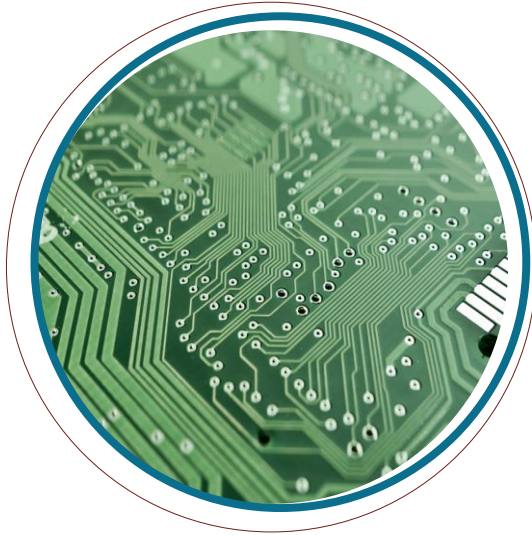
Fast Lane Worldwide Experts in Technology Training and Consulting | Learn.Transform.Succeed.

3

Module 1 Contents:

- **What is Microsoft Defender XDR?**
- **What is Microsoft Defender for Endpoint (MDE)?**
- **MDE vs. MS Intune**
- **Introduction to MDE**
 - Feature Overview
 - Licensing
 - Activating MDE
 - XDR/MDE portal
- **Role based access control**

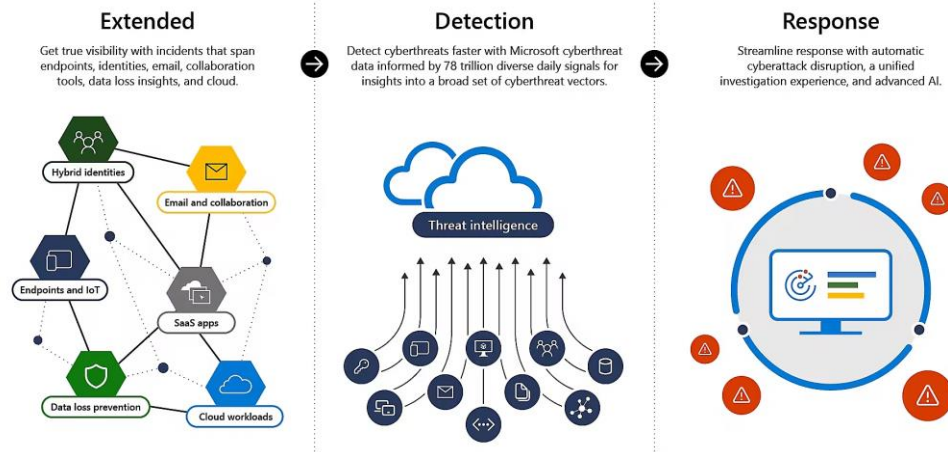
4



Microsoft XDR

5

Microsoft Defender XDR



6

Microsoft Defender XDR

- also: *Microsoft XDR*
- Platform for securing
 - Endpoints
 - Identities
 - Email and Collaboration
 - Cloud Apps
 - Compute resources
 - online
 - on-prem

© 2023 Fast Lane

Course name (FL-XXX) vx.x, Modulename

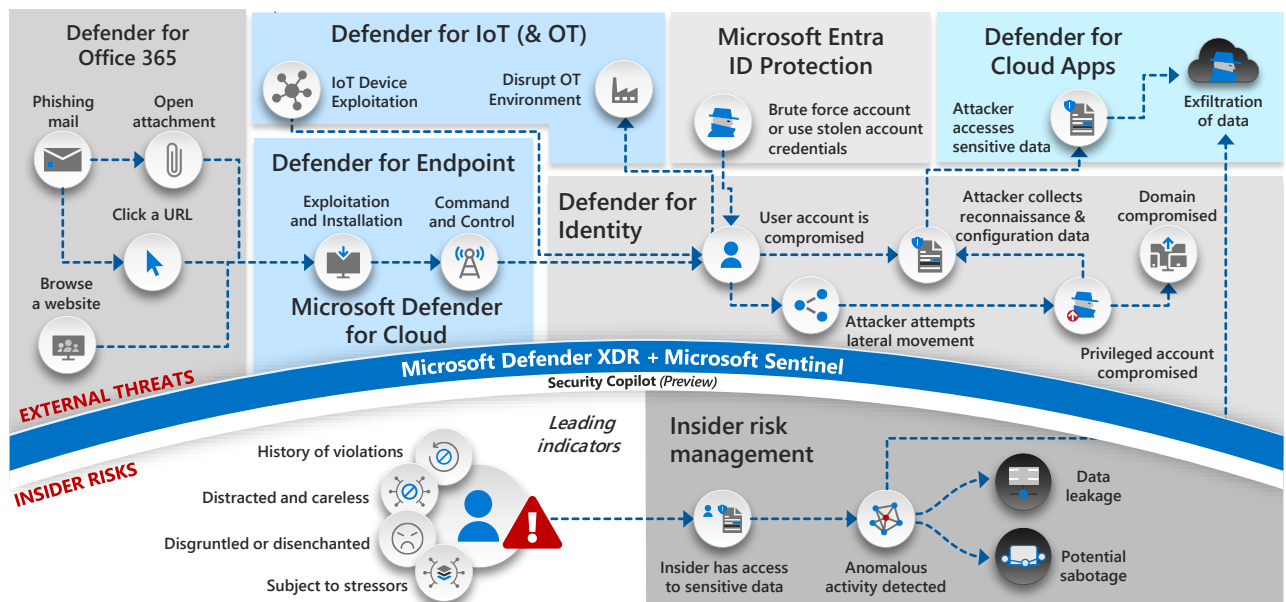
7

7

Defend across attack chains

Insider and external threats

Microsoft December 2023 – <https://aka.ms/MCRA>



8

Microsoft Defender for Endpoint

- *'... is an enterprise security platform designed to help enterprise networks prevent, detect, investigate and respond to advanced threats.'*^[1]
- Endpoint:
 - Laptops, phones, tablets, PCs
 - Access points, routers, firewalls

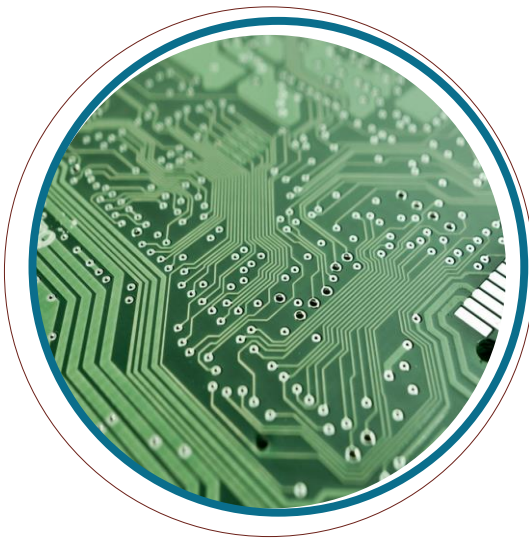
source: ^[1] <https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint>

© 2023 Fast Lane

Coursename (FL-XXX) vx.x, Modulename

9

9



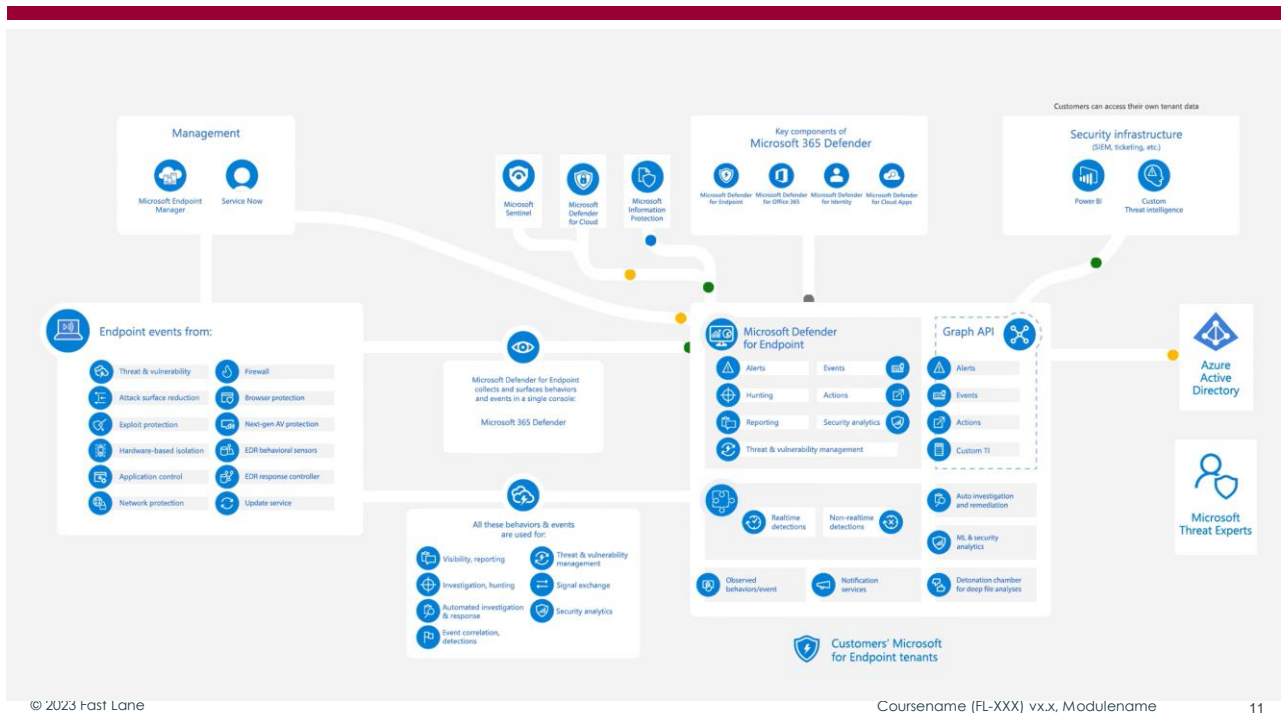
MDE Architecture

© 2023 Fast Lane

Coursename (FL-XXX) vx.x, Modulename

10

10



11

11

MDE - Architecture

- Cloud



12

12

MDE - Architecture

- Endpoint



13



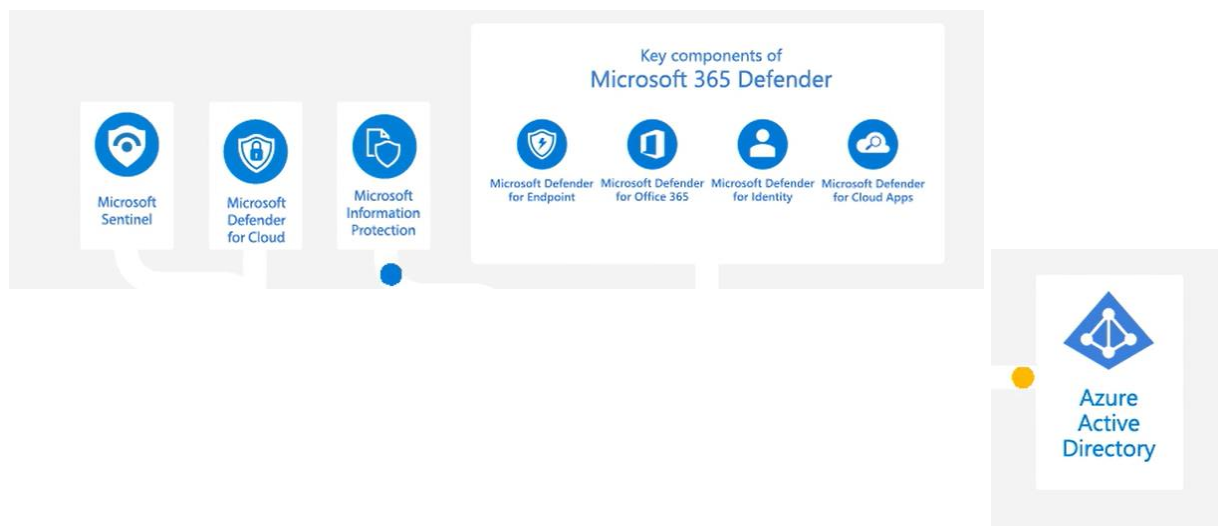
14

MDE - Architecture



15

MDE - Architecture



16



© 2023 Fast Lane

Course name (FL-XXX) vx.x, Modulename

17

17

MDE Portal

- Settings
- Device Inventory
- Threat & Vulnerability Management
- Incidents & Alerts
- Hunting
- Actions & submissions

The screenshot shows the Microsoft Defender MDE Portal interface. The left sidebar contains a navigation menu with the following items:

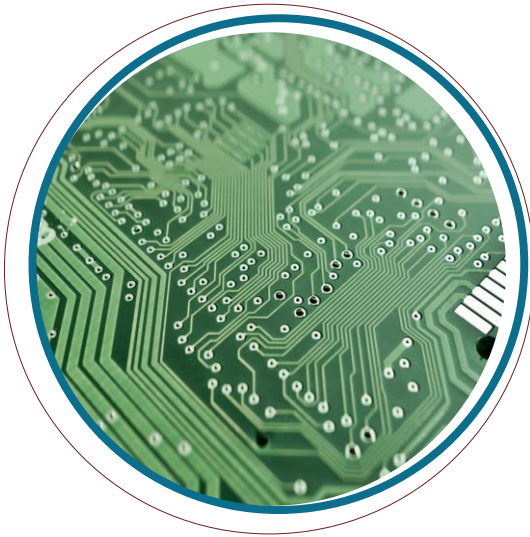
- Home
- Exposure management
- Investigation & response
- Incidents & alerts
- Hunting
- Actions & submissions
- Partner catalog
- Assets
- Devices
- Microsoft Sentinel
- Endpoints
- Vulnerability management
- Partners and APIs
- Configuration management
- Email & collaboration
- SOC optimization
- Reports
- System
- Audit
- Permissions
- Health
- Settings
- Customize navigation
- Show all

The main content area displays the "Home" dashboard with the following sections:

- Get your SIEM and XDR in one place:** A banner encouraging users to connect Microsoft Sentinel and Microsoft Defender XDR.
- Your optimizations data:** A section showing the status of optimizations (Active, In progress, Completed, Dismissed) with a "Connect a workspace" button.
- Recent optimizations value:** A section indicating "No recent optimizations value" and explaining that values will be shown once optimizations are completed.
- Top threat-based coverage optimizations:** A section indicating "No recent coverage optimizations" with a "Configure" button.

© 2023 Fast Lane

18



MDE

Features

Licenses

Source: <https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint>

MDE Features

MDE Plan 1

Unified security tools and centralized management
 Next-generation antimalware
 Cyberattack surface reduction rules
 Device control (such as USB)
 Endpoint firewall
 Network protection
 Web control/category-based URL blocking
 Device-based conditional access
 Controlled folder access
 APIs, SIEM connector, custom threat intelligence
 Application control

MDE Plan 2

Endpoint detection and response
 Deception techniques
 Automated investigation and remediation
 Cyberthreat and vulnerability management
 Threat intelligence (cyberthreat analytics)
 Sandbox (deep analysis)
 Endpoint attack notifications⁶

Source: <https://learn.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#microsoft-defender-for-endpoint>

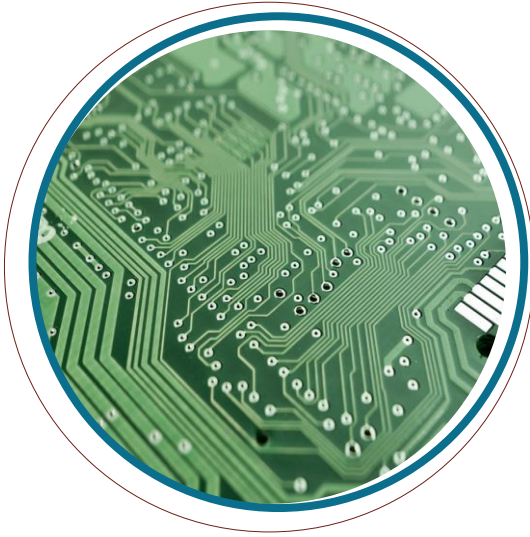
MDE Licenses

- **MDE Plan 1**
 - standalone user subscription license
 - part of Microsoft 365 E3/A3/G3
- **MDE Plan 2**
 - standalone user subscription license
 - part
 - Microsoft 365 E5/A5/G5 (Windows 11 Enterprise E5 incl.)
 - Microsoft E5/A5/G5/F5 Security
 - Microsoft 365 F5 Security & Compliance
 - Windows 11 Enterprise E5/A5

Source: <https://learn.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#microsoft-defender-for-business>

MDE Licenses

- Microsoft Defender for Business
 - standalone user license
 - part of Microsoft Business Premium
 - features of MDE plan 1 plus some of plan 2
 - server add-on available
- Microsoft Defender for Servers
 - part of Microsoft Defender for Cloud
 - Azure subscription required
 - also suitable for hybrid or multi-cloud hosted servers



MDE / Microsoft Intune

MDE vs. Microsoft Intune

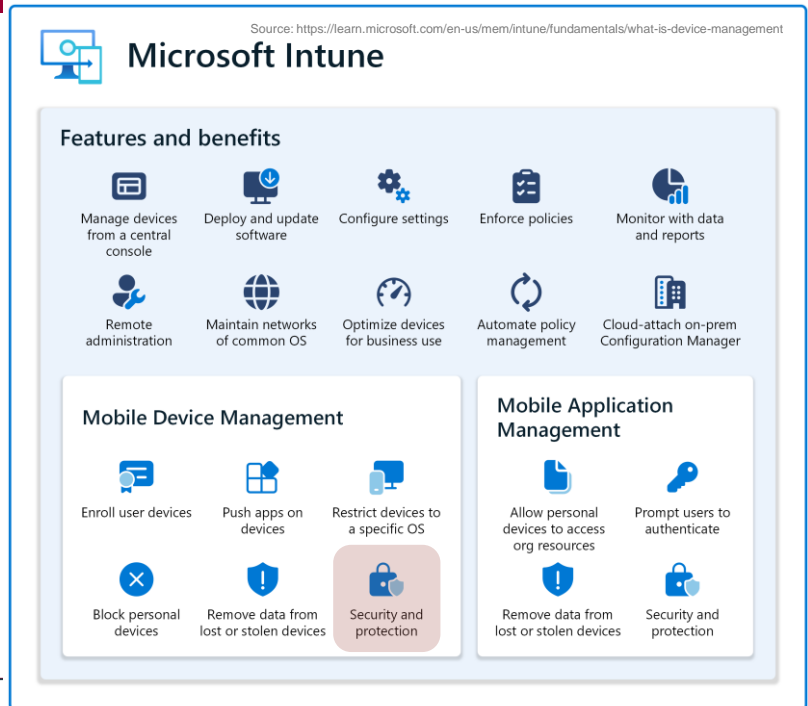
'Microsoft Intune is a **cloud-based endpoint management solution**. It manages user access to organizational resources and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.'

MDE vs. Intune

'Microsoft Intune is a **cloud-based endpoint management solution**. It manages user access to organizational resources and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.'

© 2023 Fast Lane

25



MDE vs. Microsoft Intune

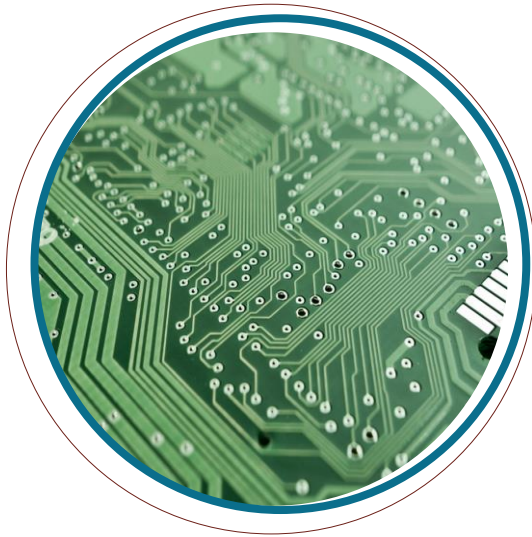
- Intune is not required for MDE
- MDE is not required for Intune
- MDE extends security capabilities on and for devices
 - EDR
 - Security configuration
- Intune portal could be used for some settings in MDE

© 2023 Fast Lane

Coursename (FL-XXX) vx.x, Modulename

26

26



Zero Trust

Zero Trust

'... is a security strategy for designing and implementing the following set of security principles:'

Verify explicitly	Use least privilege access	Assume breach
Always authenticate and authorize based on all available data points.	Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Defender for Endpoint is a primary component of the Assume breach principle and an important element of your extended detection and response (XDR) deployment with MS Defender XDR.

Zero Trust

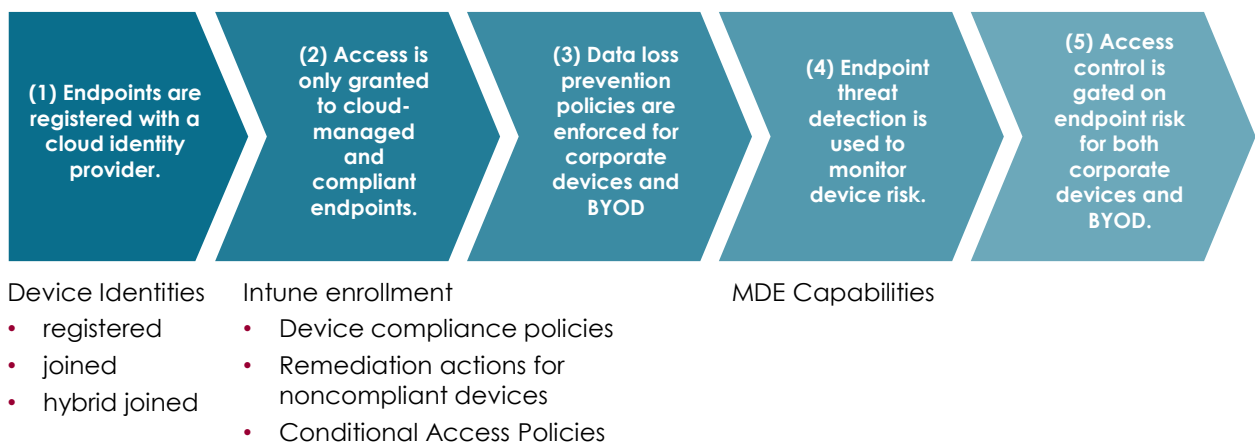
used technologies

- Endpoint behavioral sensors
- Cloud security analytics
- Threat intelligence

Threat protection for Zero Trust

- Core Defender Vulnerability Management
- Attack surface reduction
- Next-generation protection
- EDR
- Automated investigation and remediation
- Secure Score for Devices
- MS Threat Experts

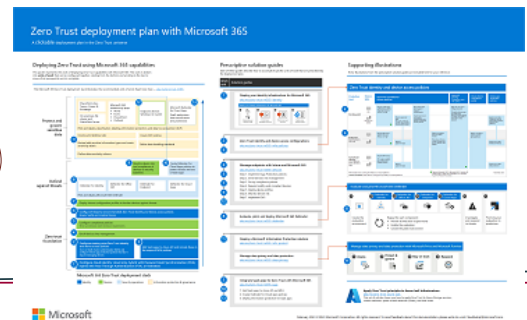
Endpoint Zero Trust deployment guide





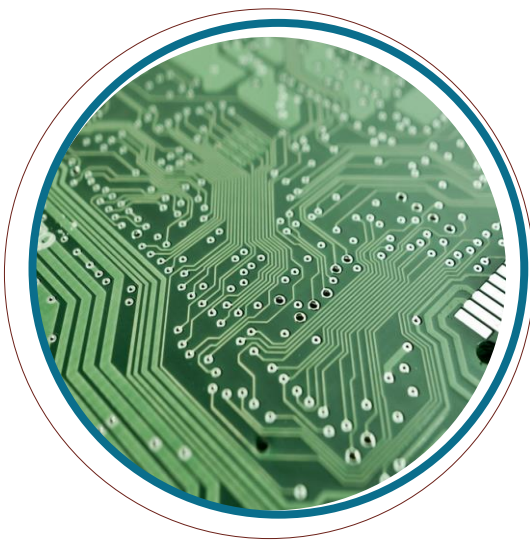
MDE Zero Trust Deployment guide is part of

Zero Trust Deployment Guide



© 2023 Fast Lane

31



MDE Deployment

© 2023 Fast Lane

Coursename (FL-XXX) vx.x, Modulename

32

32

Source: <https://learn.microsoft.com/en-us/defender-endpoint/production-deployment>

MDE Deployment (Step 1)

Set up

- Check licenses
- use Microsoft Defender portal
 - <https://security.microsoft.com>
 - click on Assets/Devices (e.g.)
 - for the first time we have to go for a coffee
 - wait for Org ID in Settings | Microsoft Defender XDR
 - and the item Settings | Endpoints
- Data center location
 - same as for Defender XDR
 - cannot be changed



Hang on! We're preparing new spaces for your data and connecting them.



This takes a few minutes. When we're done, your data will gradually consolidate and light up the console in the next few hours. [Learn about Microsoft Defender XDR](#)

© 2023 Fast Lane

Course name (FL-XXX) vx.x, Module name

33

33

Source: <https://learn.microsoft.com/en-us/defender-endpoint/production-deployment>

MDE Deployment (Step 2)

Assign roles and permissions

- Concept of least Privileges
- Choices
 - Basic permissions management
 - RBAC
 - Unified RBAC (P2 required)
- more later
- for the start be a Global or Security Administrator (Entra ID role)

© 2023 Fast Lane

Course name (FL-XXX) vx.x, Module name

34

34

MDE Deployment (Step 3)

Identify architecture and deployment/onboarding method

- Know the OS(s) of devices
- Know the current configuration management system
 - Config Manager
 - Intune
 - GPO
 - ...
- Derive the onboarding method

MDE Deployment (Step 3)

Identify architecture and deployment/onboarding method

Architecture	Description
Cloud-native	We recommend using Microsoft Intune to onboard, configure, and remediate endpoints from the cloud for enterprises who don't have an on-premises configuration management solution or are looking to reduce their on-premises infrastructure.
Co-management	For organizations who host both on-premises and cloud-based workloads we recommend using Microsoft's ConfigMgr and Intune for their management needs. These tools provide a comprehensive suite of cloud-powered management features, and unique co-management options to provision, deploy, manage, and secure endpoints and applications across an organization.
On-premises	For enterprises who want to take advantage of the cloud-based capabilities of Microsoft Defender for Endpoint while also maximizing their investments in Configuration Manager or Active Directory Domain Services , we recommend this architecture.
Evaluation and local onboarding	We recommend this architecture for SOCs (Security Operations Centers) who are looking to evaluate or run a Microsoft Defender for Endpoint pilot, but don't have existing management or deployment tools. This architecture can also be used to onboard devices in small environments without management infrastructure, such as a DMZ (Demilitarized Zone).

MDE Deployment (Step 3)

Identify architecture and deployment/onboarding method

- Deployment tool
 - local script
 - GPO
 - MS Intune
 - MS Config Manager
 - VDI scripts
 - ...

MDE Deployment (Step 3)

Identify architecture and deployment/onboarding method

Endpoint	Deployment tool	
Windows	Local script (up to 10 devices) Group Policy Microsoft Intune/ Mobile Device Manager	Microsoft Configuration Manager VDI scripts
Win/Lx servers	Integration with Microsoft Defender for Cloud	
macOS	Local script Microsoft Intune JAMF Pro	Mobile Device Management
Linux servers	Local script Puppet Ansible	Chef Saltstack
Android	Microsoft Intune	
iOS	Microsoft Intune Mobile Application Manager	

MDE Deployment (Step 4)

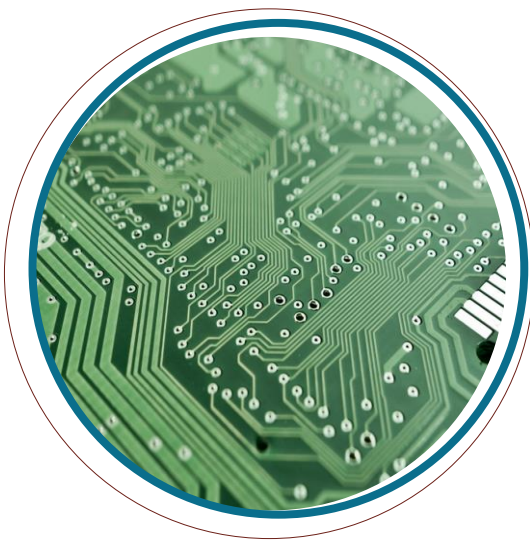
Onboard Devices

- discussed later ...

MDE Deployment (Step 5)

Configure MDE capabilities

- discussed later ...



Permissions

MDE Permissions

Basic Permissions

- Default Entra ID Roles

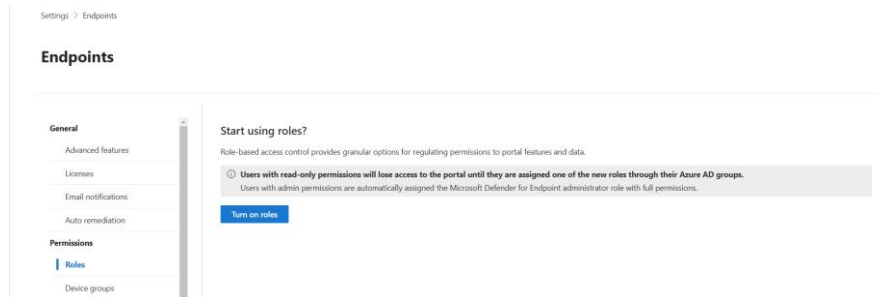
Global Administrator Security Administrator	Full Access
Security Reader	Read-only access No Access to device inventory

MDE Permissions

Role-based access control (RBAC)

- Configured in MDE settings
- Roles & Device groups
- suitable if tiering is necessary
- Turn on
Settings | Endpoints | Permissions/Roles
Settings | Endpoints | Permissions/Device groups

MDE Permissions



- Turn on
 - XDR Portal | Settings | Endpoints | Permissions/Roles
 - irreversible
 - former admins became MDE administrators with full permissions
 - former readers will have no permissions

MDE Permissions - RBAC

- Roles are
 - a set of permissions
 - assigned to an Entra ID group
 - stored under a custom name
- Device groups are
 - a set of onboarded devices
 - devices are filtered by name, domain, tag, OS (and/or)
 - assigned to an Entra ID group with assigned role

MDE Permission - Unified RBAC

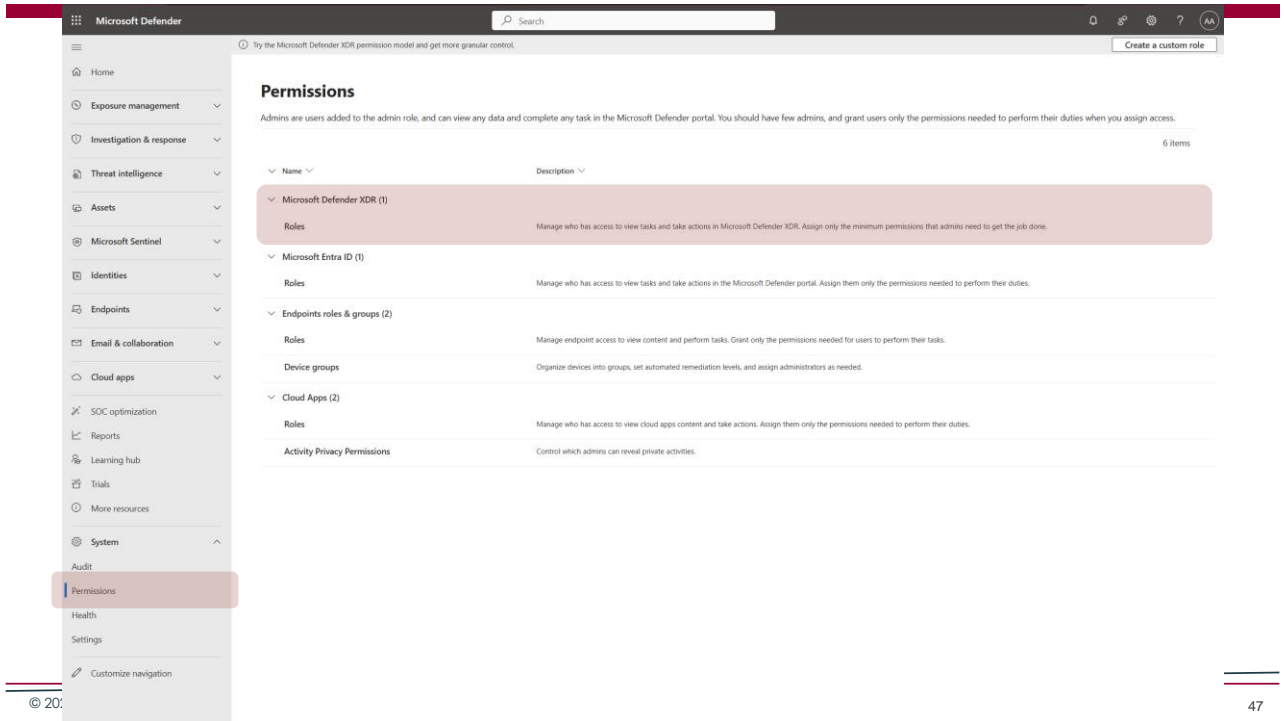
'The Microsoft Defender XDR Unified role-based access control (RBAC) model provides a single permissions management experience that provides one central location for administrators to control user permissions across different security solutions.'

- Cross workload permissions within a single role
- Ability to assign roles to individual users as well as security group
- Multi assignment within a single role

MDE Permission - Unified RBAC

Process

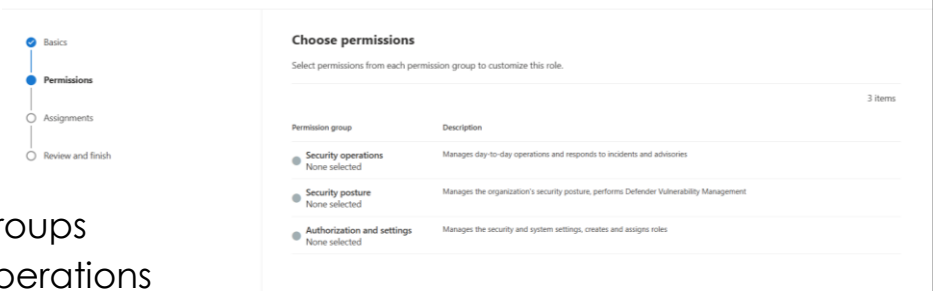
- Assure to be a Global or Security Administrator
- Using
 - Create custom roles
 - Import existing roles
 - View, edit and delete
- Activate MS XDR Unified RBAC model



MDE Permissions - Unified RBAC

Role settings

- Name
- Description
- Permission groups
 - Security operations
 - Security posture
 - Authorization and settings



Permission Groups

Security operations

Select the permissions in this group to users who perform security operations and those who respond to incidents and advisories.

Clear all permissions

All read-only permissions

All read and manage permissions

Select custom permissions

Security data

Read-only

Select all permissions

Select custom permissions

Security data basics (read)

Alerts (manage)

Response (manage)

Basic live response (manage)

Advanced live response (manage)

File collection (manage)

Email & collaboration quarantine (manage)

Email & collaboration advanced actions (manage)

Raw data (Email & collaboration)

Read-only

Select custom permissions

Email & collaboration metadata (read)

Email & collaboration content (read)

Security posture

Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.

Clear all permissions

All read-only permissions

All read and manage permissions

Select custom permissions

Posture management

Read-only

Select all permissions

Select custom permissions

Vulnerability management (read)

Exception handling (manage)

Remediation handling (manage)

Exposure Management (read)

Exposure Management (manage)

Authorization and settings

Select the permissions for users who need to configure your security and system settings, and create and assign roles.

If you select any permissions on this page, you will also assign the security data read permission under the Security operations permission group.

Clear all permissions

All read-only permissions

All read and manage permissions

Select custom permissions

Authorization

Read-only

Read and manage

Security settings

Read-only

Select all permissions

Select custom permissions

Detection tuning (manage)

Core security settings (read)

Core security settings (manage)

System settings

Read-only (Defender for Office, Defender for Identity)

Read and manage

© 2023 Fast Lane

Coursename (FL-XXX) vx.x, Modulename

49

49

Microsoft Defender

Settings

Microsoft Defender XDR

Home

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Identities

Endpoints

Email & collaboration

Cloud apps

SOC optimization

Reports

Learning hub

Trials

More resources

System

Audit

Permissions

Health

Settings

Customize navigation

Microsoft Defender XDR

General

Account

Email notifications

Preview features

Alert service settings

Permissions and roles

Streaming API

Rules

Asset rule management

Alert tuning

Critical asset management

Automation

Identity automated response

Activate unified role-based access control

When you activate the workloads to use the new permission model, any custom roles that were created or managed previously by your organization will no longer grant access to services and data in Microsoft Defender XDR.

You can't activate workloads that haven't been turned on or deployed. To find out which services still need to be turned on, see Workload settings.

Workloads

Endpoints & Vulnerability Management

Not active

Email & Collaboration

Enforcing Exchange Online permissions will impact the Email & Collab capabilities that were previously configured in the Exchange admin center. Exchange admin center.

Not active - Defender for Office 365

Not active - Exchange Online permissions

Identity

Enabling this setting will also enforce these permissions on the Microsoft Defender for Identity portal. Learn more about role groups for MDI.

Not active

Go to Permissions and roles

© 2023

50

50

25

MDE Permission

References

- [Unified RBAC permissions](#)
- [Map Unified RBAC permissions to existing RBAC permissions](#)