Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

November 2024

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

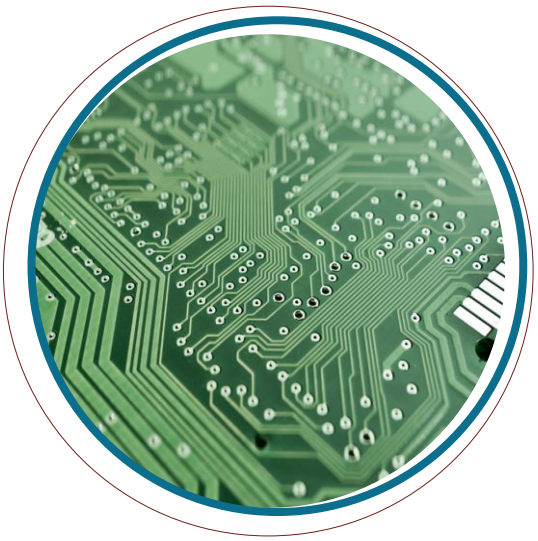
Trainings:
- Microsoft 365 & Azure Security
- Azure Administration & Solution Architecting
- PowerShell
- Windows Server & Client for Admins

Module 01

Overview

Module 1 Contents:

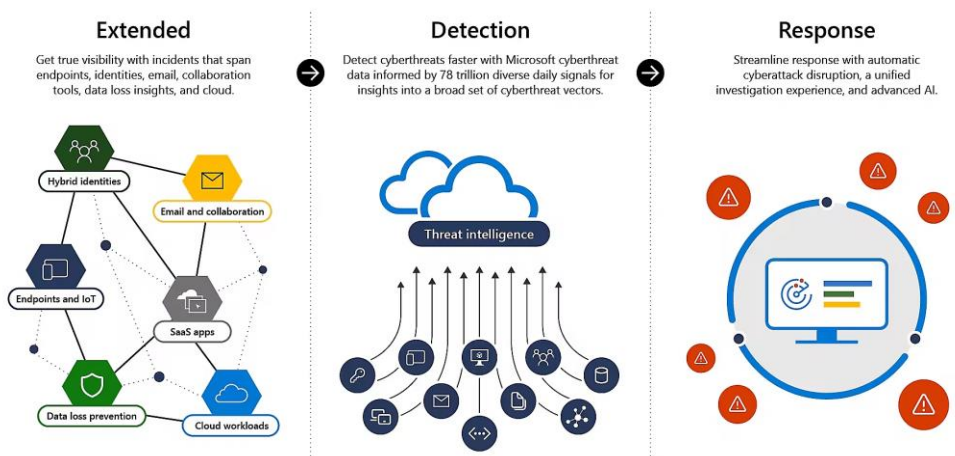
- **What is Microsoft Defender XDR?**
- **What is Microsoft Defender for Endpoint (MDE)?**
- **MDE vs. MS Intune**
- **Introduction to MDE**
  - Feature Overview
  - Licensing
  - Activating MDE
  - XDR/MDE portal
- **Role based access control**



Microsoft XDR

5

Microsoft Defender XDR



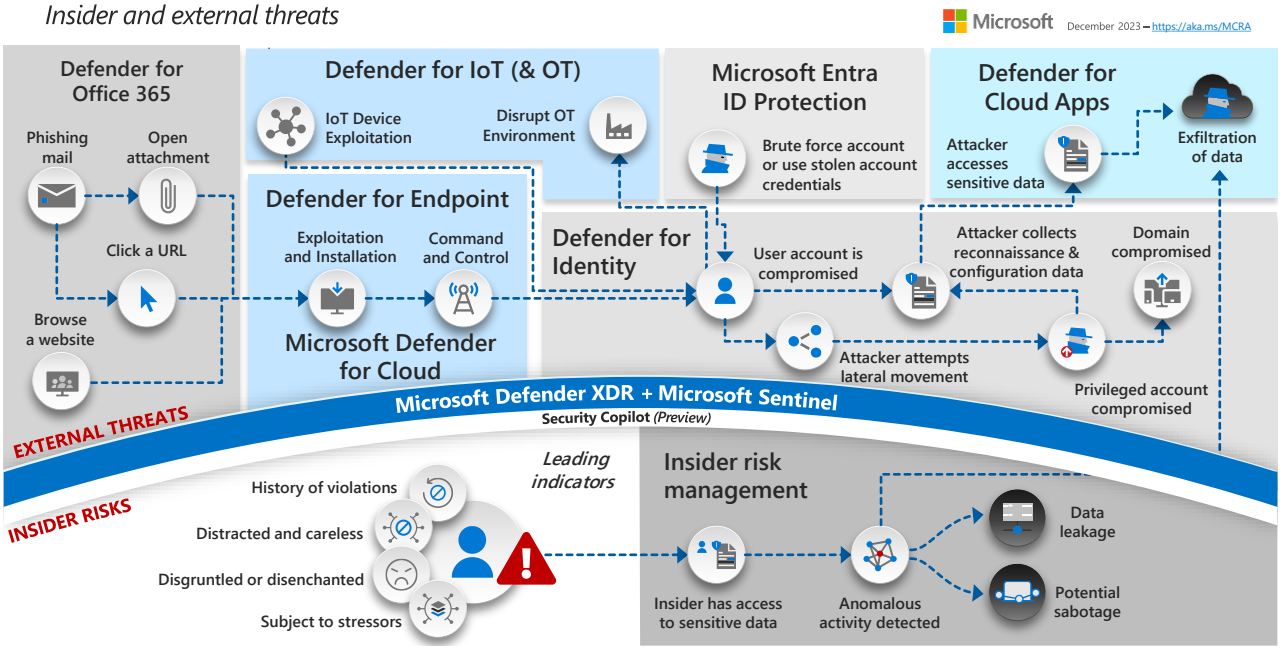
6

Microsoft Defender XDR

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

Defend across attack chains

Insider and external threats

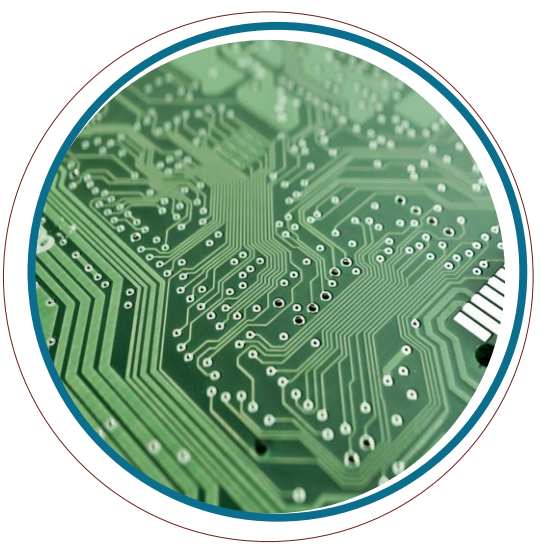


8

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



MDE

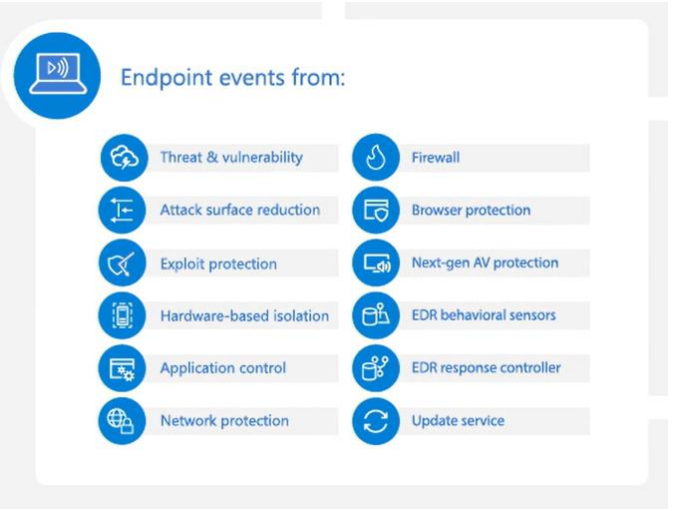
Architecture

MDE - Architecture

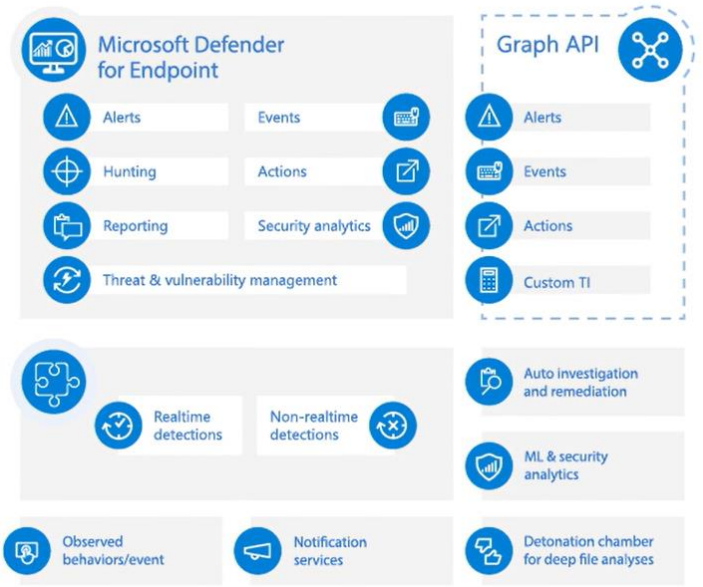
- Cloud

MDE - Architecture

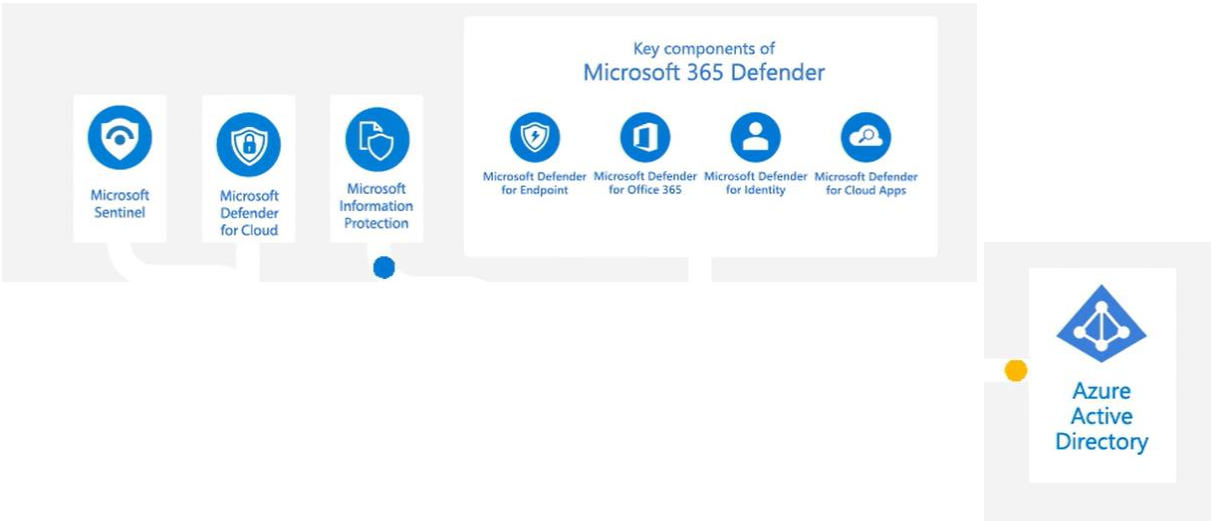
- Endpoint



MDE - Ar

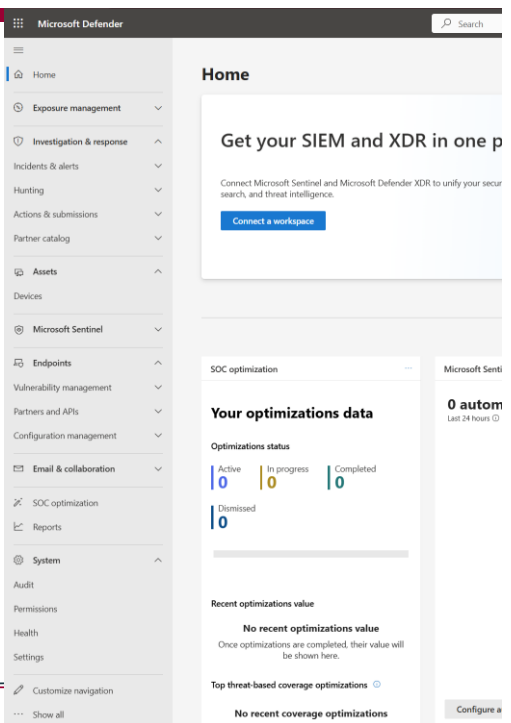


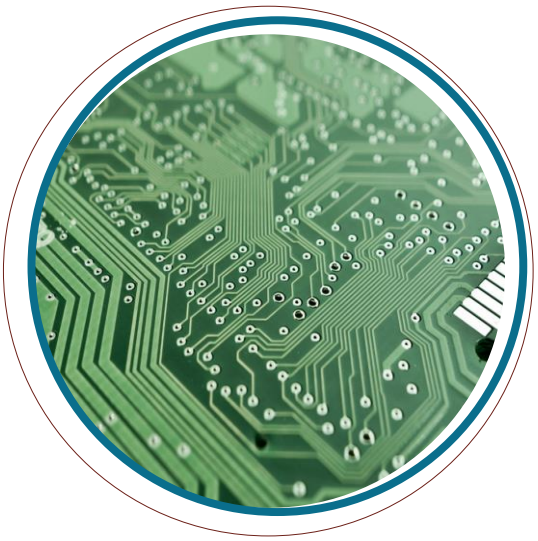
MDE - Architecture



MDE Portal

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





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

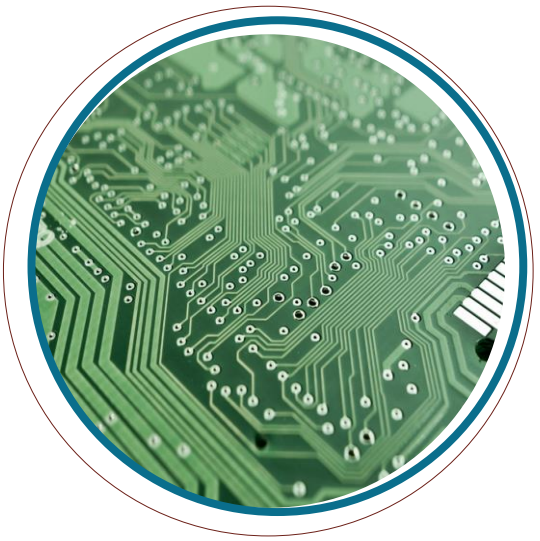
- MDE **Plan 1**
  - standalone user subscription license
  - part of Microsoft 365 E3/A3/G3
- MDE **Plan 2**
  - standalone user subscription license
  - part
    - Microsoft 365 E5/A5/G5 (Windows 11 Enterprise E5 incl.)
    - Microsoft E5/A5/G5/F5 Security
    - Microsoft 365 F5 Security & Compliance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



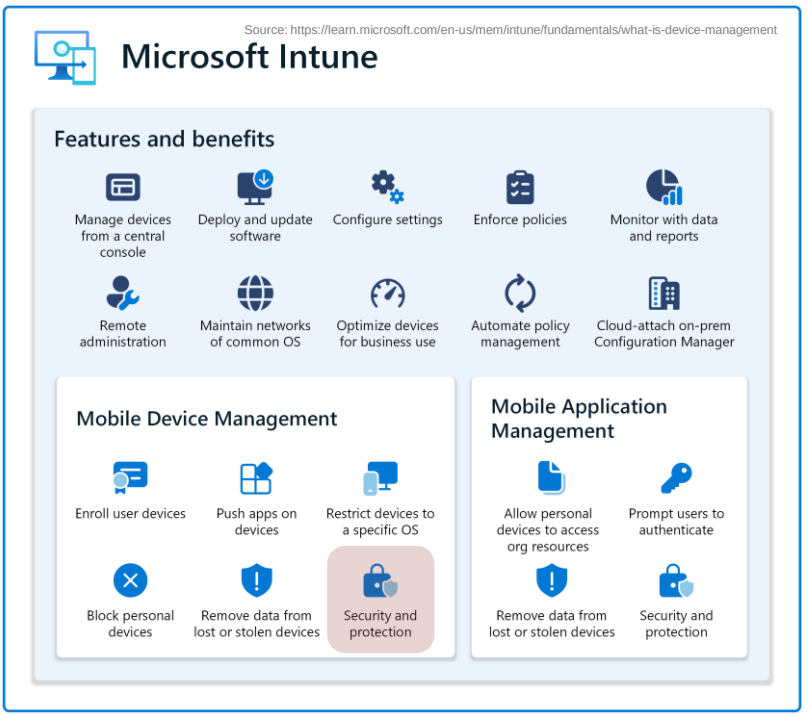
MDE / Microsoft Intune

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.'*

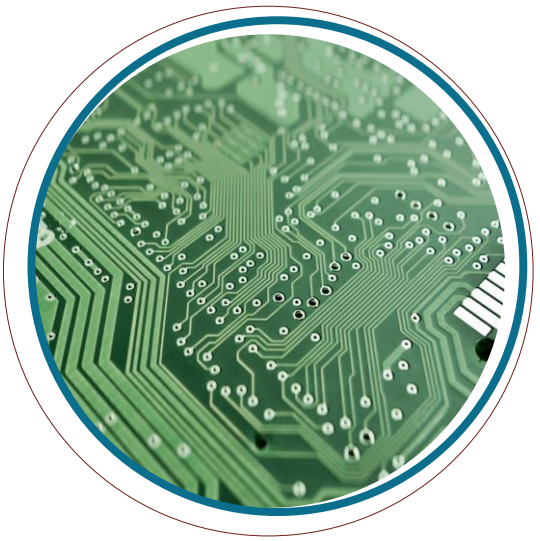


MDE vs. Microsoft Intune

- 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



Zero Trust

Source: https://learn.microsoft.com/en-us/defender-endpoint/zero-trust-with-microsoft-defender-endpoint

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

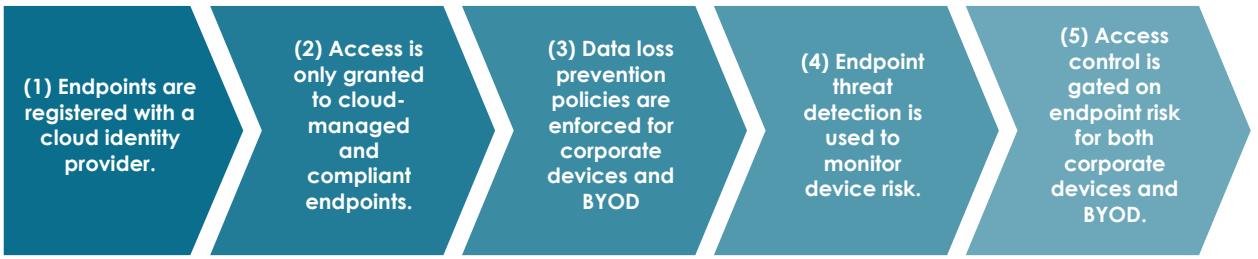
- Endpoint behavioral sensors
- Cloud security analytics
- Threat intelligence

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

Source: https://learn.microsoft.com/en-us/security/zero-trust/deploy/endpoints

Endpoint Zero Trust deployment guide



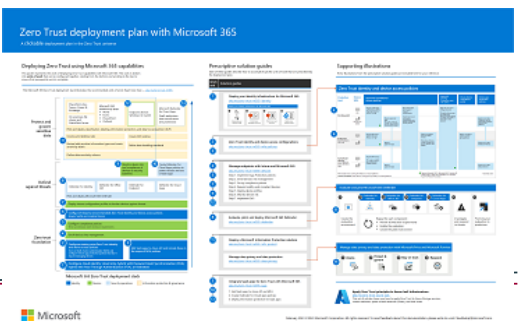
Device Identities
- registered
- joined
- hybrid joined

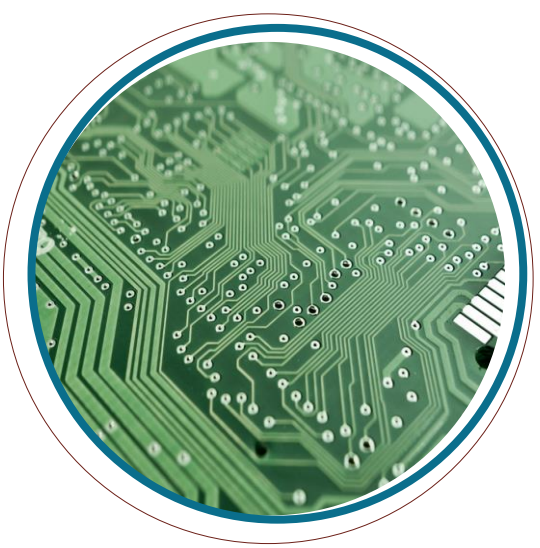
Intune enrollment
- Device compliance policies
- Remediation actions for noncompliant devices
- Conditional Access Policies

MDE Capabilities

MDE Zero Trust Deployment guide is part of

Zero Trust Deployment Guide





MDE Deployment

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

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)

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)

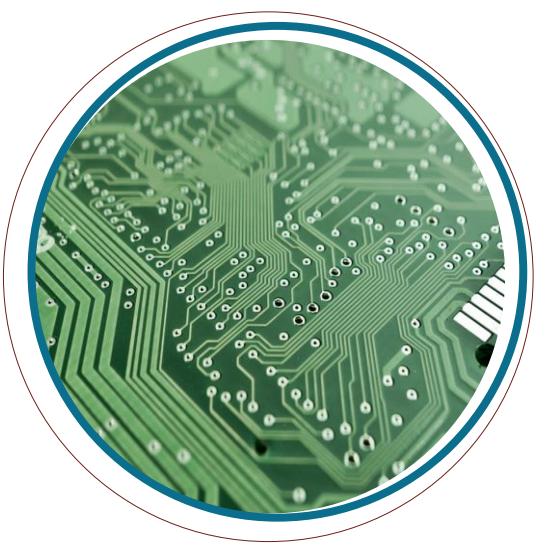
Onboard Devices

- discussed later …

MDE Deployment (Step 5)

Configure MDE capabilites

- 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**

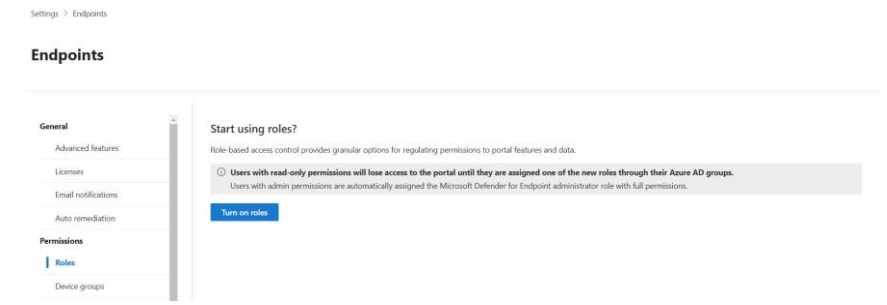
MDE Permissions

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

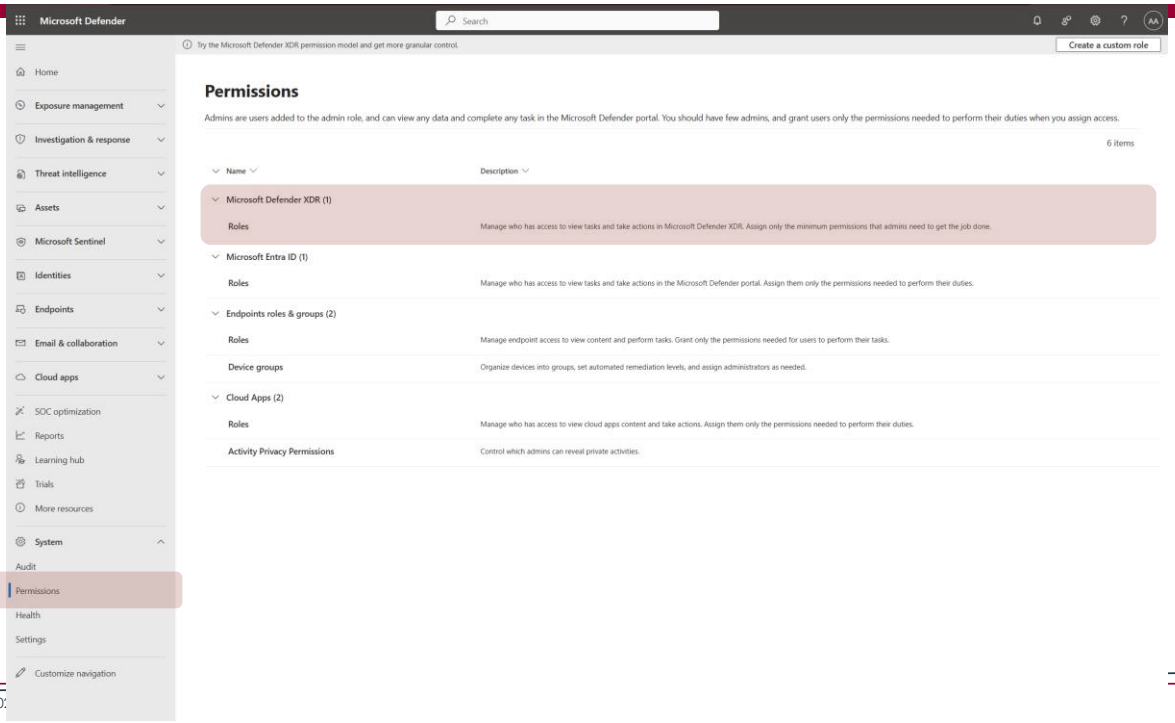
'The Microsoft Defender XDR Unified role-based access control (RBAC) model provides a single permissions management experience that provides one central location for administrators to control user permissions across different security solutions.'

- 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

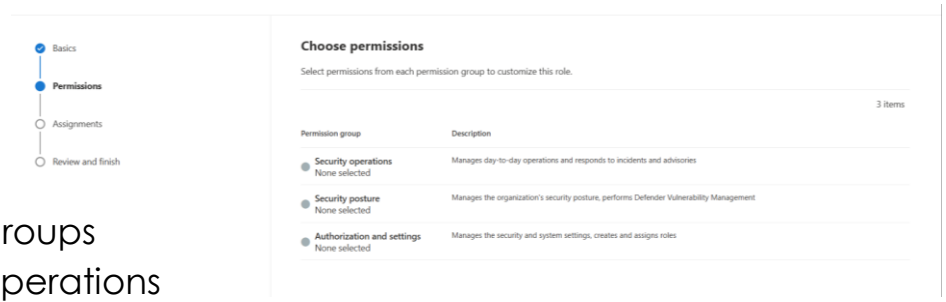
Process

- 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



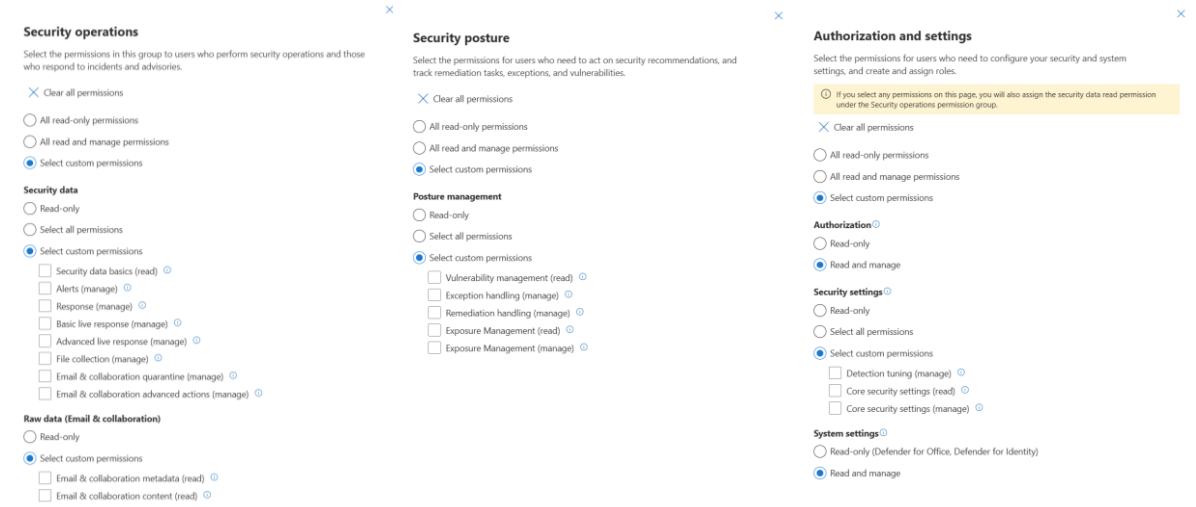
MDE Permissions - Unified RBAC

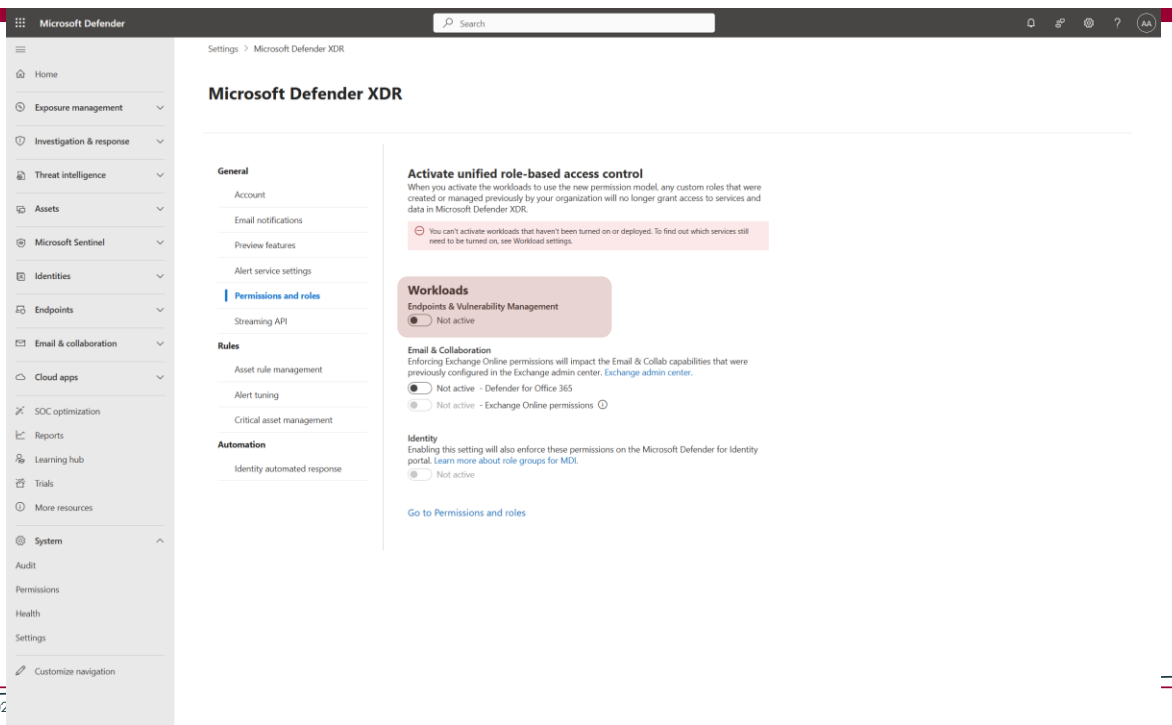
Role settings
- Name
- Description



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

Permission Groups





MDE Permission

References

- Unified RBAC permissions
- Map Unified RBAC permissions to existing RBAC permissions