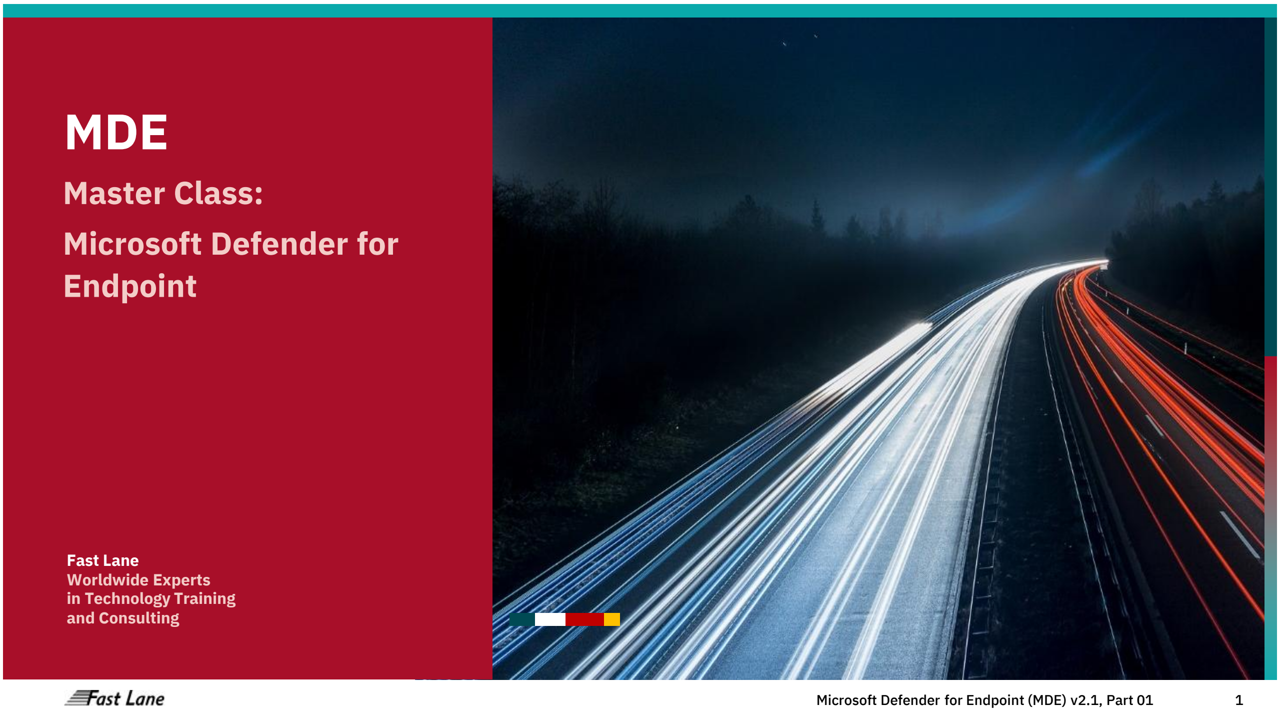


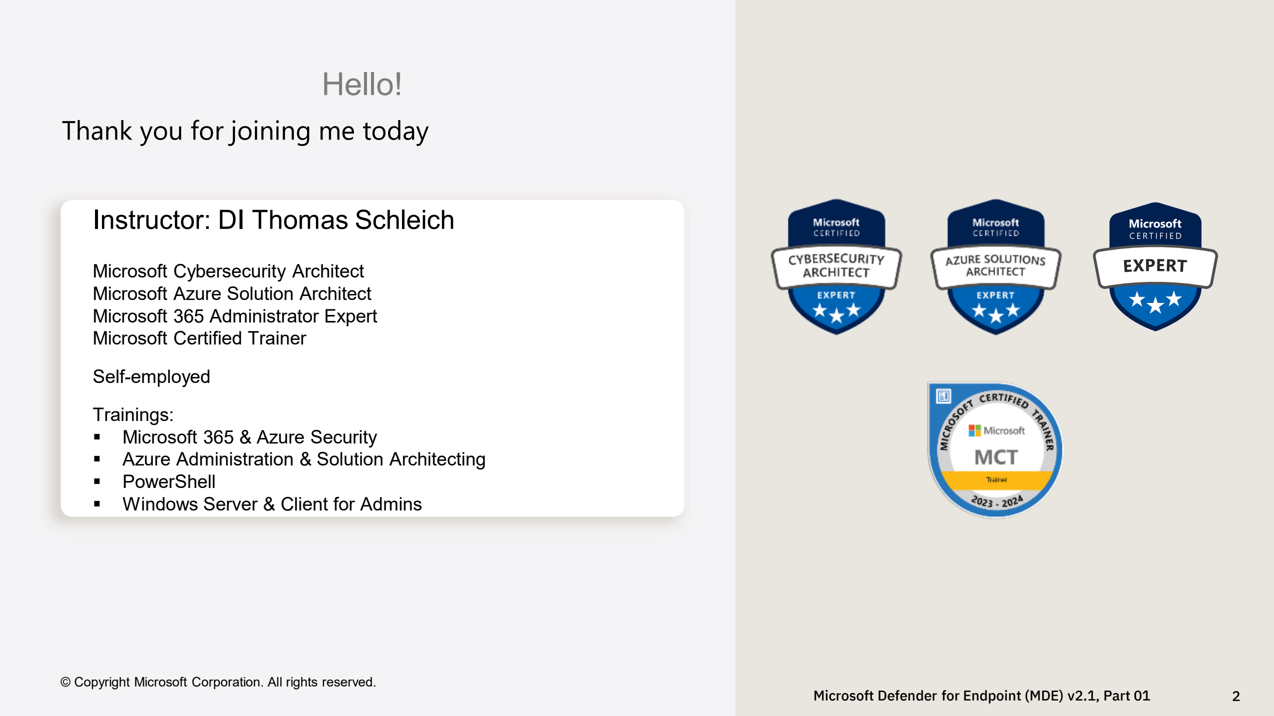
MDE

Master Class:

Microsoft Defender for Endpoint

Fast Lane
Worldwide Experts
in Technology Training
and Consulting

1



Hello!

Thank you for joining me today

Instructor: DI Thomas Schleich

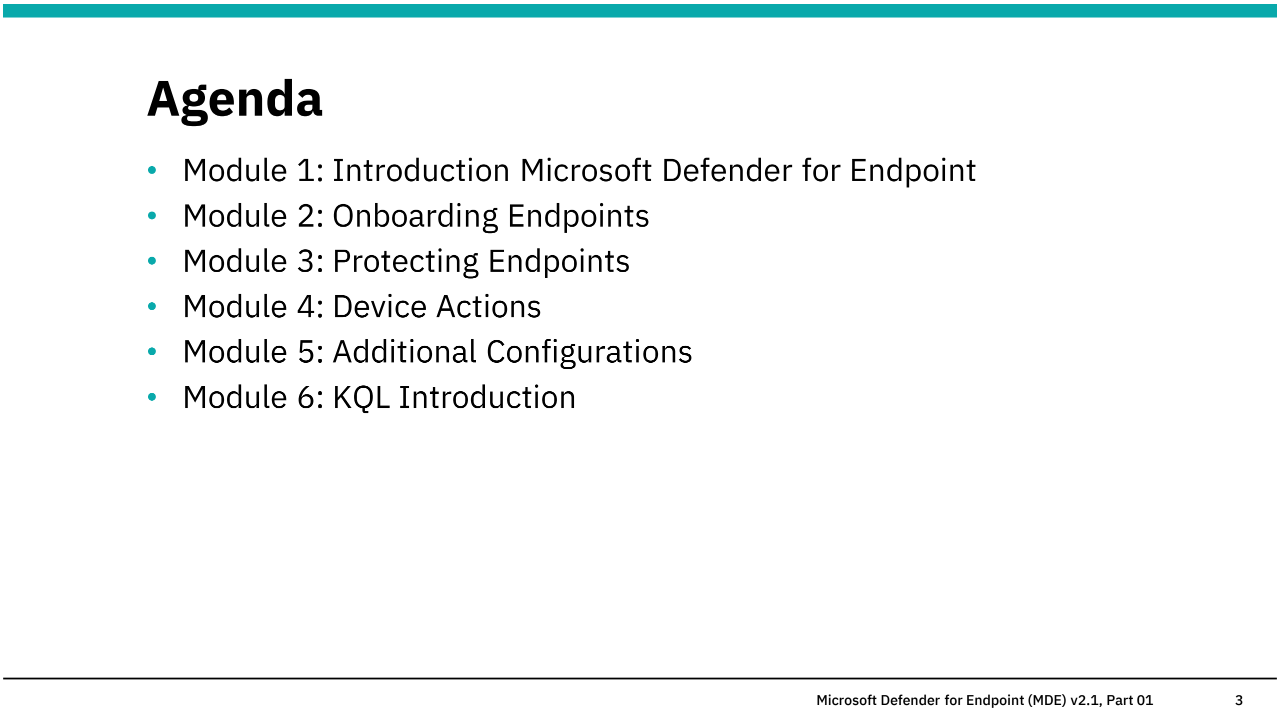
Microsoft Cybersecurity Architect
Microsoft Azure Solution Architect
Microsoft 365 Administrator Expert
Microsoft Certified Trainer

Self-employed

Trainings:

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

2



Agenda

- Module 1: Introduction Microsoft Defender for Endpoint
- Module 2: Onboarding Endpoints
- Module 3: Protecting Endpoints
- Module 4: Device Actions
- Module 5: Additional Configurations
- Module 6: KQL Introduction

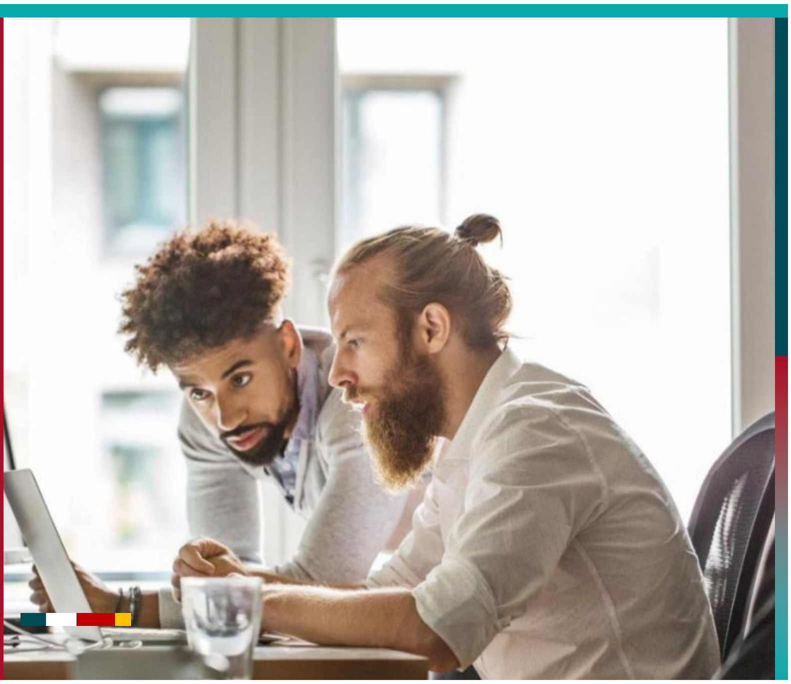
Module 1

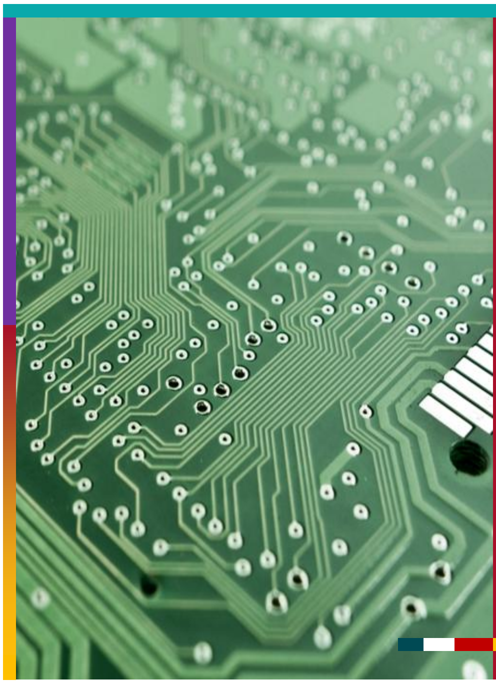
Overview

Fast Lane
Worldwide Experts
in Technology Training
and Consulting

Content Module 1

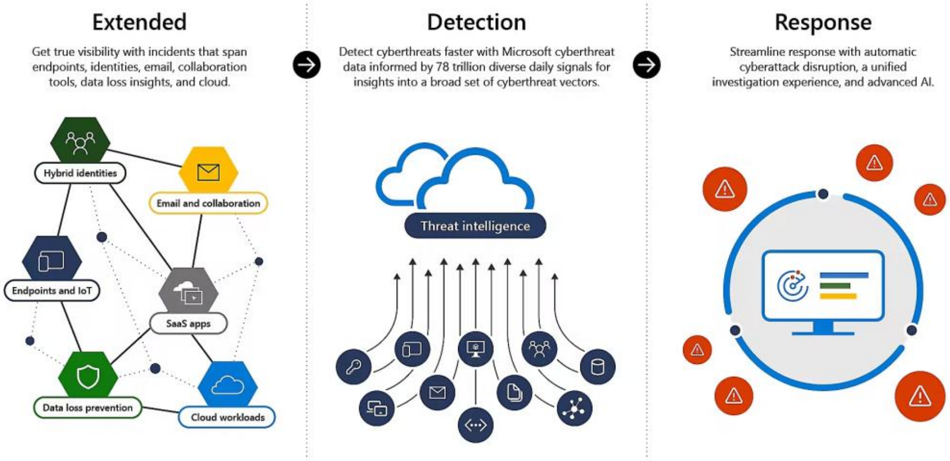
- **What is Microsoft Defender XDR?**
- **What is Microsoft Defender for Endpoint (MDE)?**
- **MDE vs. MS Intune**
- **Introduction to MDE**
  - Feature Overview
  - Licensing
  - Activating MDE
  - XDR/MDE portal
- **Role based access control**





Microsoft XDR

Microsoft Defender XDR



Extended

Get true visibility with incidents that span endpoints, identities, email, collaboration tools, data loss insights, and cloud.

Detection

Detect cyberthreats faster with Microsoft cyberthreat data informed by 78 trillion diverse daily signals for insights into a broad set of cyberthreat vectors.

Response

Streamline response with automatic cyberattack disruption, a unified investigation experience, and advanced AI.

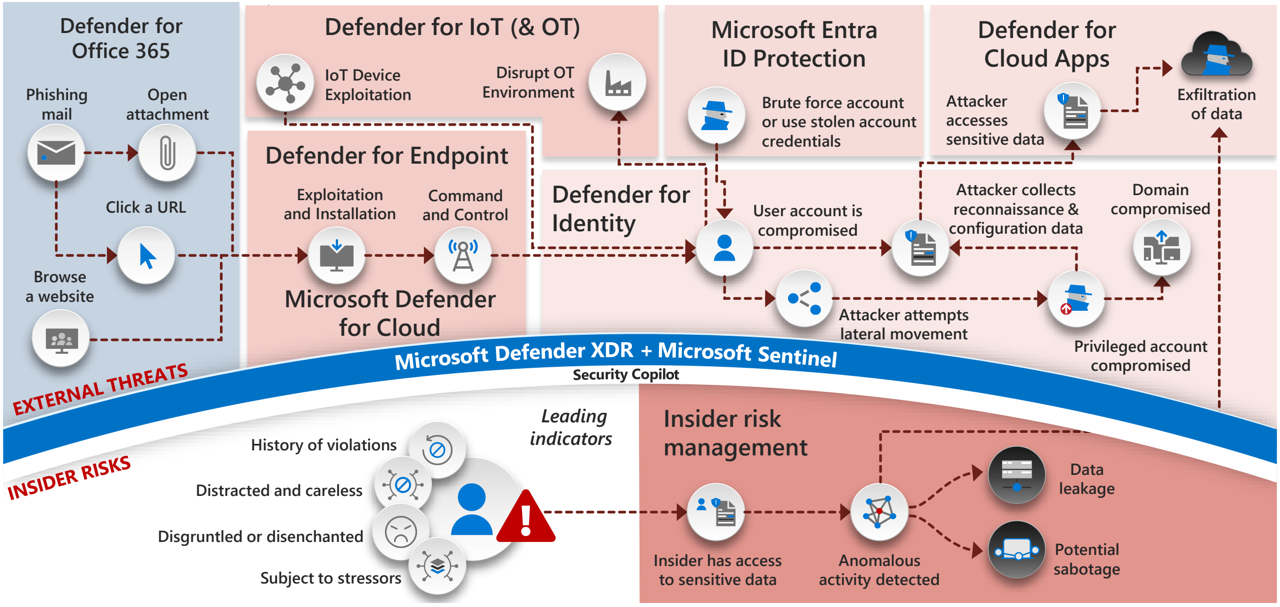
Microsoft Defender XDR

- 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

Microsoft April 2025 – https://aka.ms/MCRA



Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Defender for IoT (& OT)

IoT Device Exploitation

Disrupt OT Environment

Defender for Endpoint

Exploitation and Installation

Command and Control

Microsoft Defender for Cloud

Microsoft Entra ID Protection

Brute force account or use stolen account credentials

Defender for Cloud Apps

Attacker accesses sensitive data

Exfiltration of data

Defender for Identity

User account is compromised

Attacker collects reconnaissance & configuration data

Domain compromised

Attacker attempts lateral movement

Privileged account compromised

EXTERNAL THREATS

Microsoft Defender XDR + Microsoft Sentinel

Security Copilot

INSIDER RISKS

History of violations

Distracted and careless

Disgruntled or disenchanted

Subject to stressors

Leading indicators

Insider risk management

Insider has access to sensitive data

Anomalous activity detected

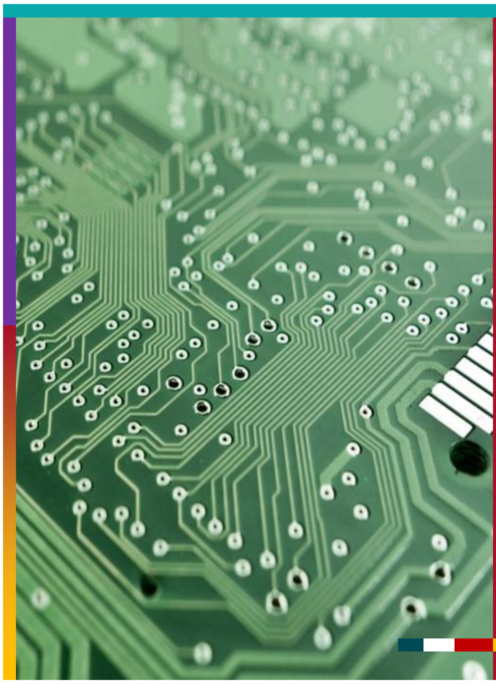
Data leakage

Potential sabotage

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

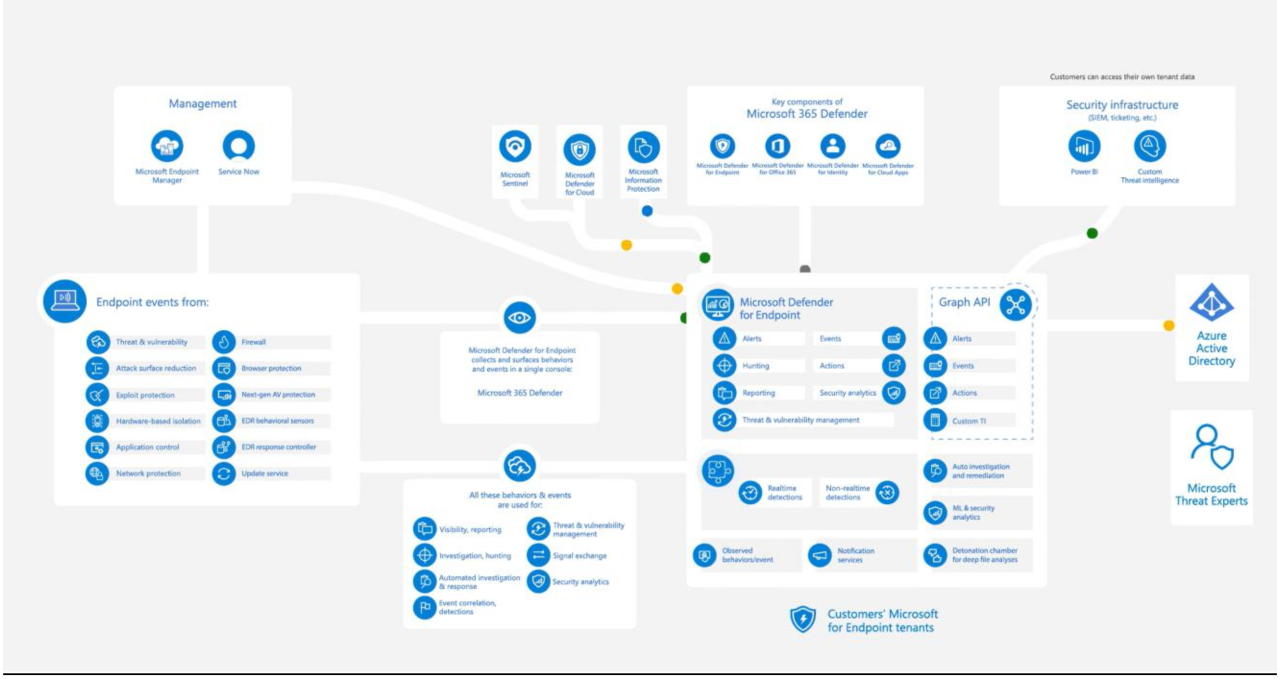
Microsoft Defender for Endpoint

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



MDE

Architecture



Management

Microsoft Endpoint Manager

Service Now

Microsoft Sentinel

Microsoft Defender for Cloud

Microsoft Information Protection

Key components of Microsoft 365 Defender

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Customers can access their own tenant data

Security infrastructure (SIEM, ticketing, etc.)

Power BI

Custom Threat intelligence

Endpoint events from:

- Threat & vulnerability
- Attack surface reduction
- Exploit protection
- Hardware-based isolation
- Application control
- Network protection
- Firewall
- Browser protection
- Next-gen AV protection
- EDR behavioral sensors
- EDR response controller
- Update service

Microsoft Defender for Endpoint collects and surfaces behaviors and events in a single console:

Microsoft 365 Defender

All these behaviors & events are used for:

- Visibility, reporting
- Investigation, hunting
- Automated investigation & response
- Event correlation, detections
- Threat & vulnerability management
- Signal exchange
- Security analytics

Microsoft Defender for Endpoint

- Alerts
- Hunting
- Reporting
- Events
- Actions
- Security analytics
- Threat & vulnerability management

Graph API

- Alerts
- Events
- Actions
- Custom TI

Realtime detections

Non-realtime detections

Auto investigation and remediation

ML & security analytics

Observed behaviors/event

Notification services

Detonation chamber for deep file analyses

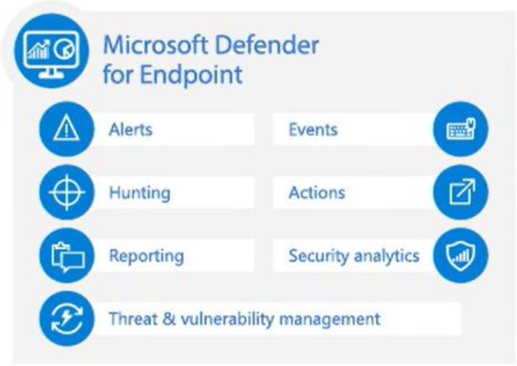
Azure Active Directory

Microsoft Threat Experts

Customers' Microsoft for Endpoint tenants

MDE - Architecture

- Cloud



Microsoft Defender for Endpoint

Alerts

Events

Hunting

Actions

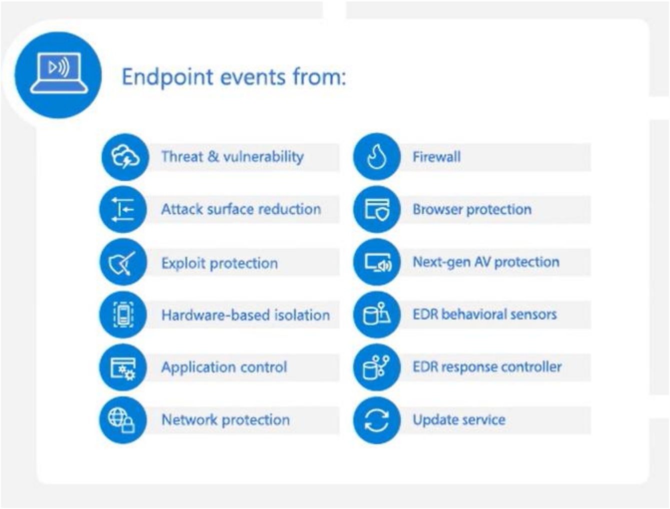
Reporting

Security analytics

Threat & vulnerability management

MDE - Architecture

- Endpoint



Endpoint events from:

Threat & vulnerability

Firewall

Attack surface reduction

Browser protection

Exploit protection

Next-gen AV protection

Hardware-based isolation

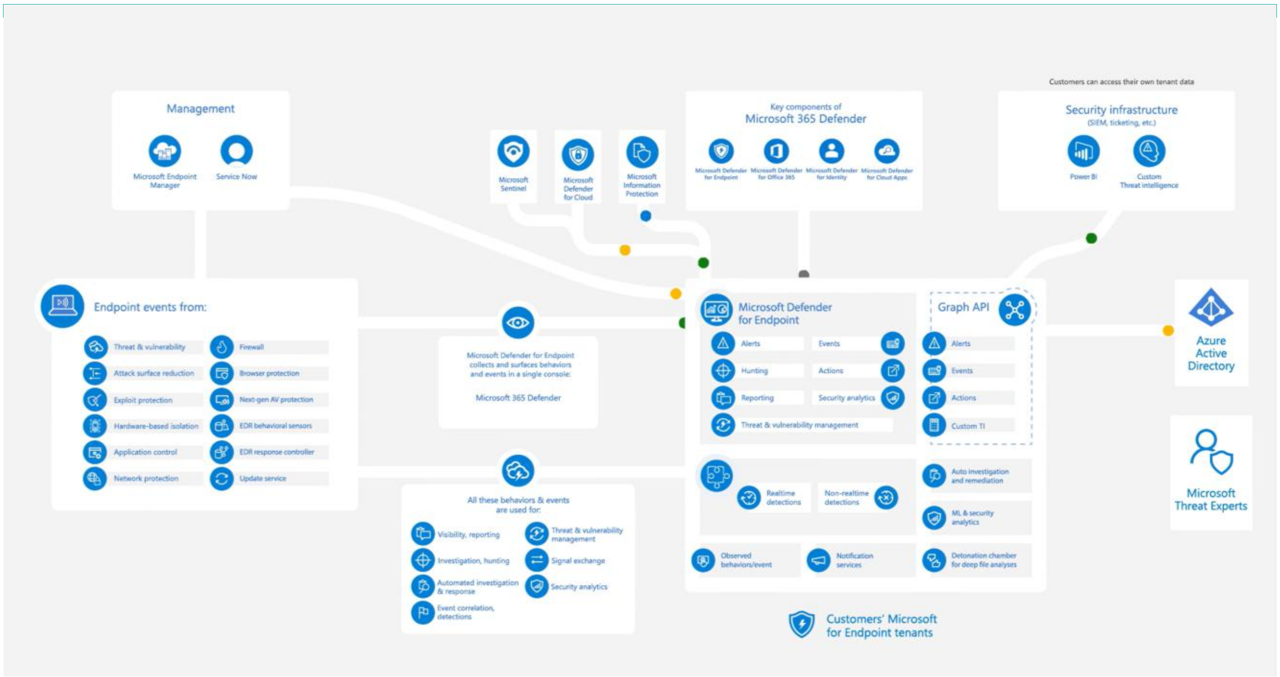
EDR behavioral sensors

Application control

EDR response controller

Network protection

Update service



Management

Microsoft Endpoint Manager

Service Now

Microsoft Sentinel

Microsoft Defender for Cloud

Microsoft Information Protection

Key components of
Microsoft 365 Defender

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Customers can access their own tenant data

Security infrastructure
(SIEM, ticketing, etc.)

Power BI

Custom Threat intelligence

Endpoint events from:

- Threat & vulnerability
- Attack surface reduction
- Exploit protection
- Hardware-based isolation
- Application control
- Network protection
- Firewall
- Browser protection
- Next-gen AV protection
- EDR behavioral sensors
- EDR response controller
- Update service

Microsoft Defender for Endpoint collects and surfaces behaviors and events in a single console:

Microsoft 365 Defender

All these behaviors & events are used for:

- Visibility, reporting
- Investigation, hunting
- Automated investigation & response
- Event correlation, detections
- Threat & vulnerability management
- Signal exchange
- Security analytics

Microsoft Defender for Endpoint

Alerts

Events

Hunting

Actions

Reporting

Security analytics

Threat & vulnerability management

Graph API

Alerts

Events

Actions

Custom TI

Realtime detections

Non-realtime detections

Auto investigation and remediation

ML & security analytics

Observed behaviors/event

Notification services

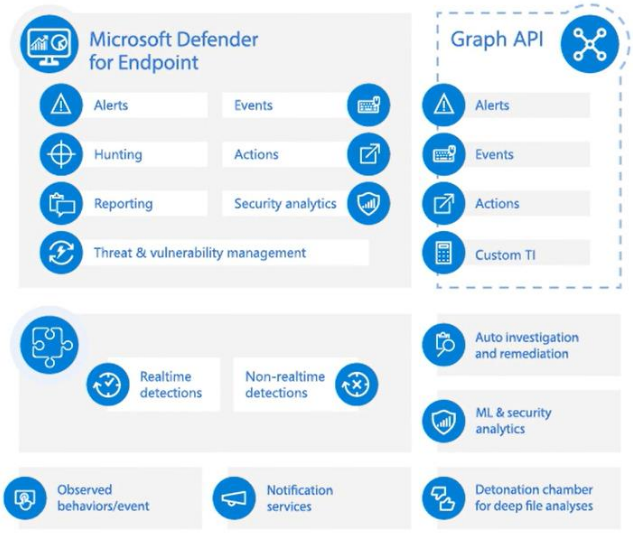
Detonation chamber for deep file analyses

Azure Active Directory

Microsoft Threat Experts

Customers' Microsoft for Endpoint tenants

MDE - Architecture



Microsoft Defender for Endpoint

Alerts

Events

Hunting

Actions

Reporting

Security analytics

Threat & vulnerability management

Graph API

Alerts

Events

Actions

Custom TI

Realtime detections

Non-realtime detections

Auto investigation and remediation

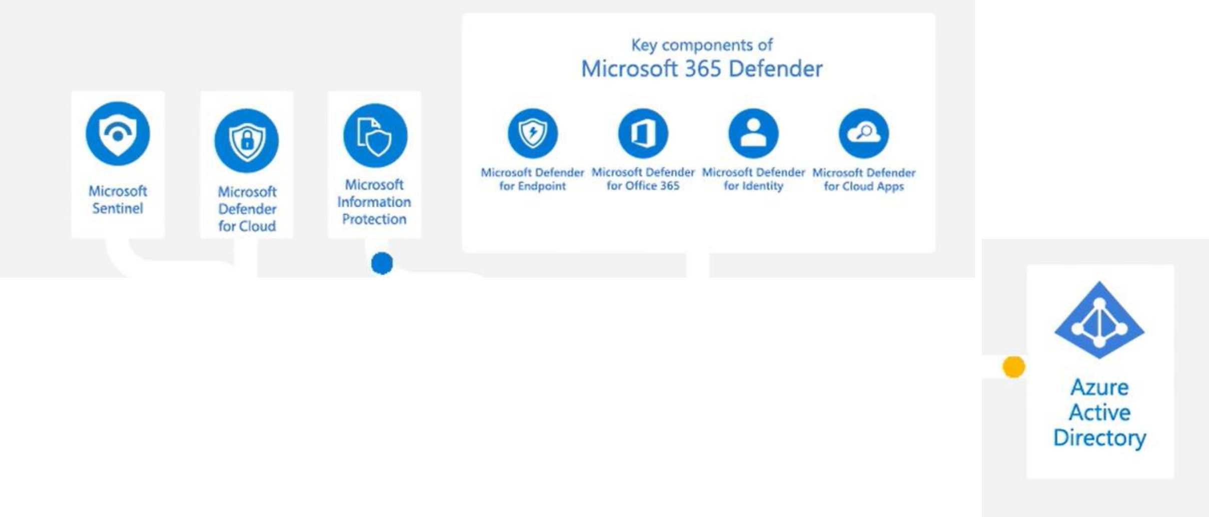
ML & security analytics

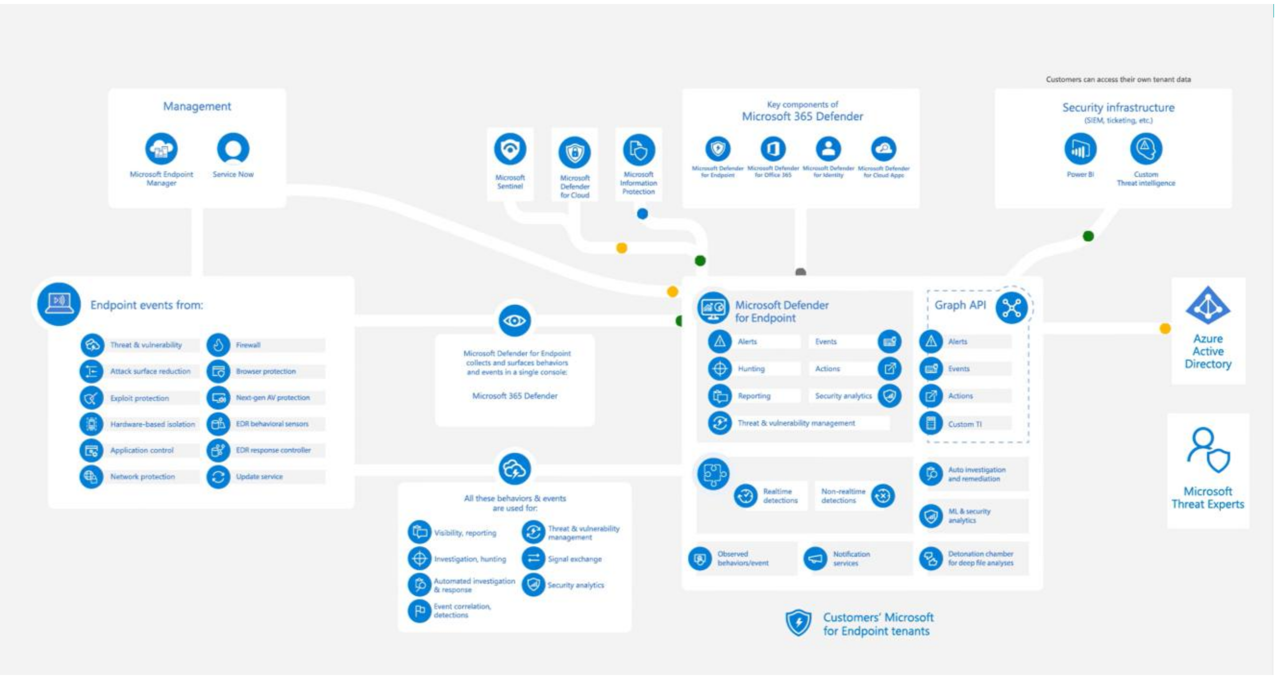
Observed behaviors/event

Notification services

Detonation chamber for deep file analyses

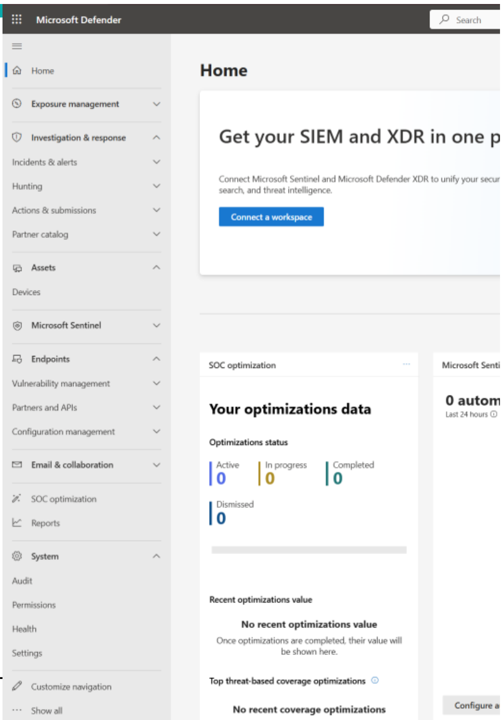
MDE - Architecture


Microsoft Sentinel
Microsoft Defender for Cloud
Microsoft Information Protection
Key components of
Microsoft 365 Defender
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Azure Active Directory



MDE Portal

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



Home

Get your SIEM and XDR in one p

Connect Microsoft Sentinel and Microsoft Defender XDR to unify your secur
search, and threat intelligence.

SOC optimization

Your optimizations data

Optimizations status

Active	In progress	Completed
0	0	0

Dismissed: 0

Recent optimizations value

No recent optimizations value

Once optimizations are completed, their value will be shown here.

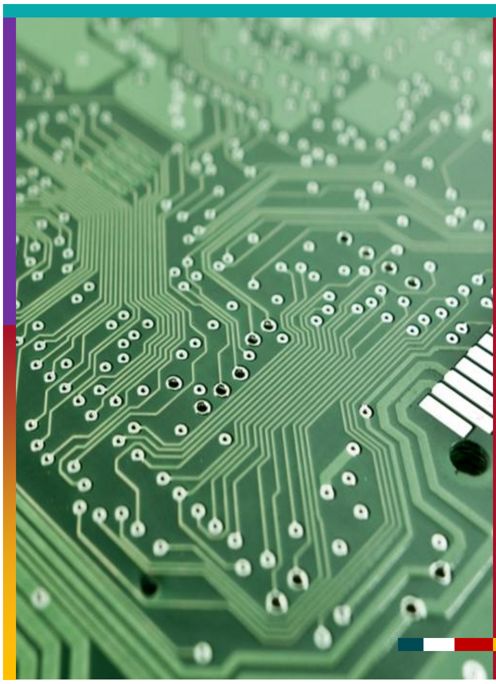
Top threat-based coverage optimizations

No recent coverage optimizations

Microsoft Senti

0 autom

Last 24 hours



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 notifications

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

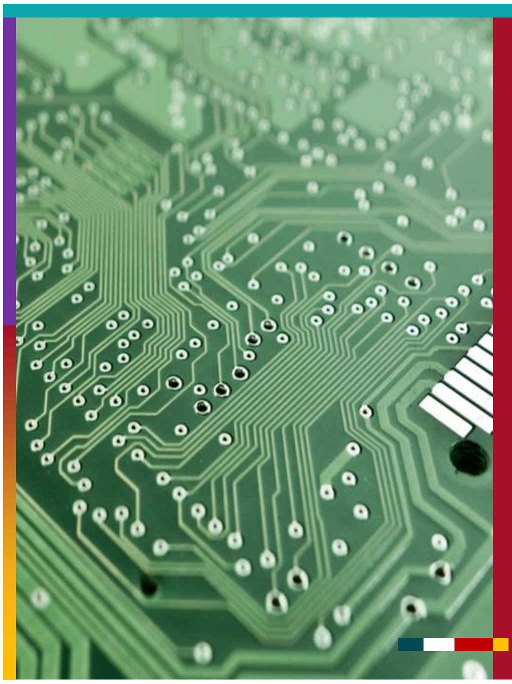
MDE Licenses

- 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

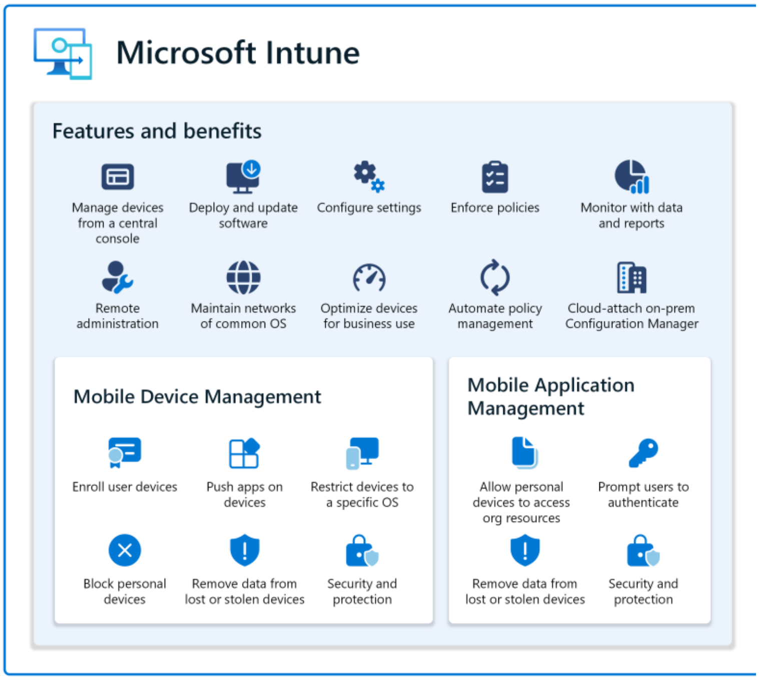
Source: https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/what-is-intune

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.'*



Microsoft Intune

Features and benefits

- Manage devices from a central console
- Deploy and update software
- Configure settings
- Enforce policies
- Monitor with data and reports
- Remote administration
- Maintain networks of common OS
- Optimize devices for business use
- Automate policy management
- Cloud-attach on-prem Configuration Manager

Mobile Device Management

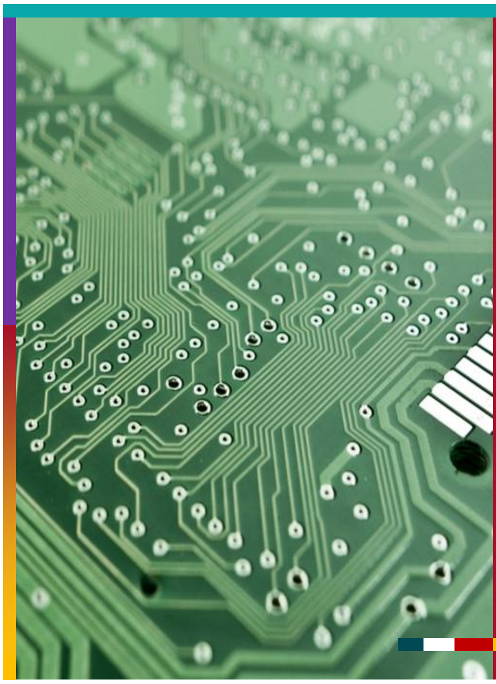
- Enroll user devices
- Push apps on devices
- Restrict devices to a specific OS
- Block personal devices
- Remove data from lost or stolen devices
- Security and protection

Mobile Application Management

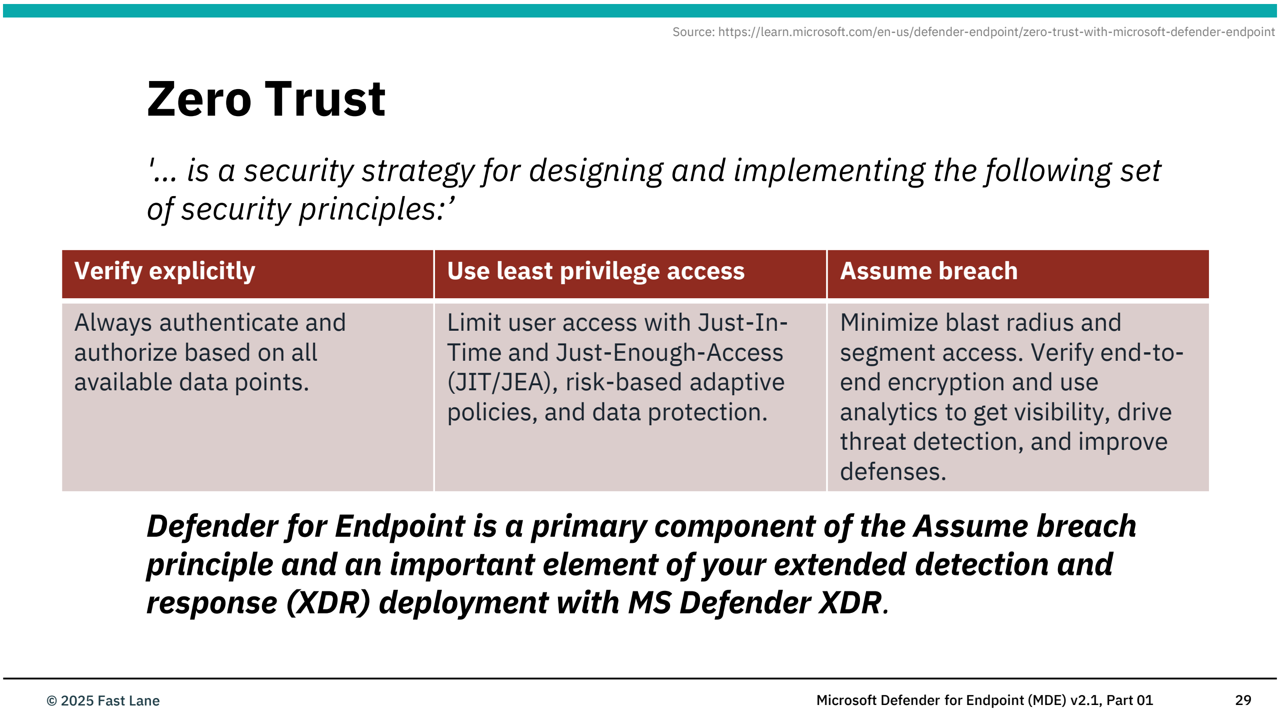
- Allow personal devices to access org resources
- Prompt users to authenticate
- Remove data from lost or stolen devices
- Security and protection

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



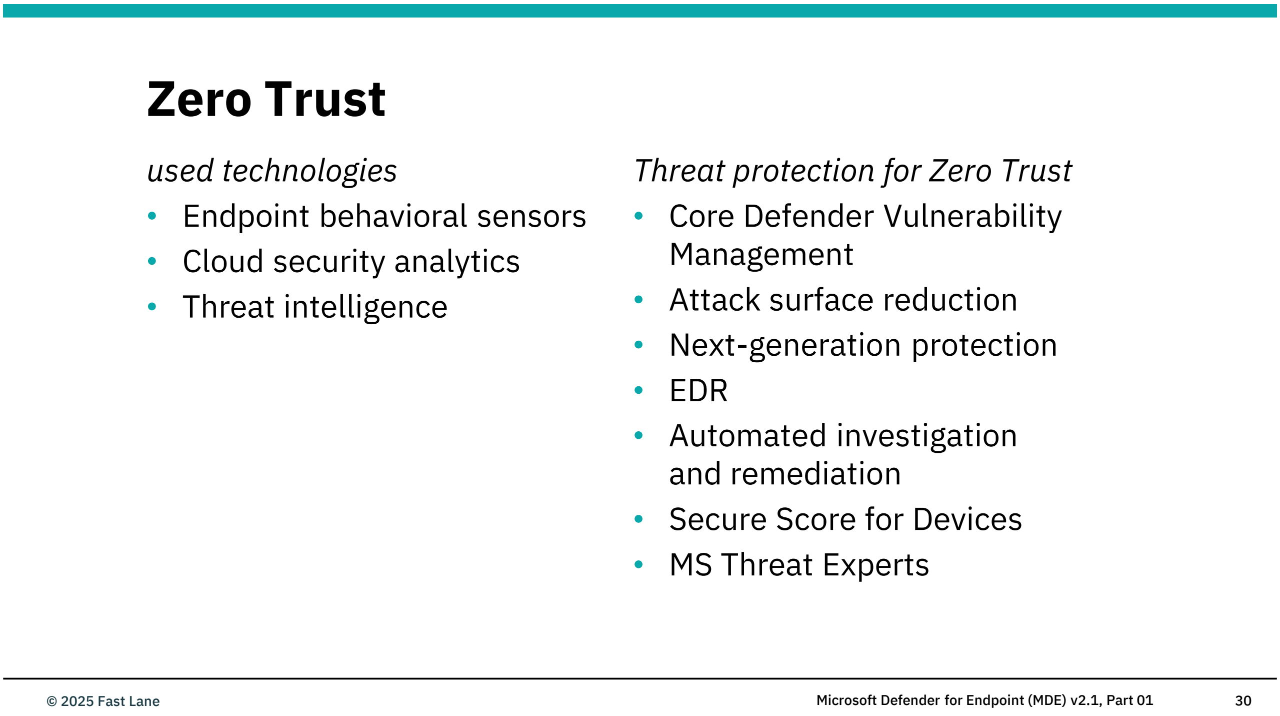
Source: https://learn.microsoft.com/en-us/defender-endpoint/zero-trust-with-microsoft-defender-endpoint

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

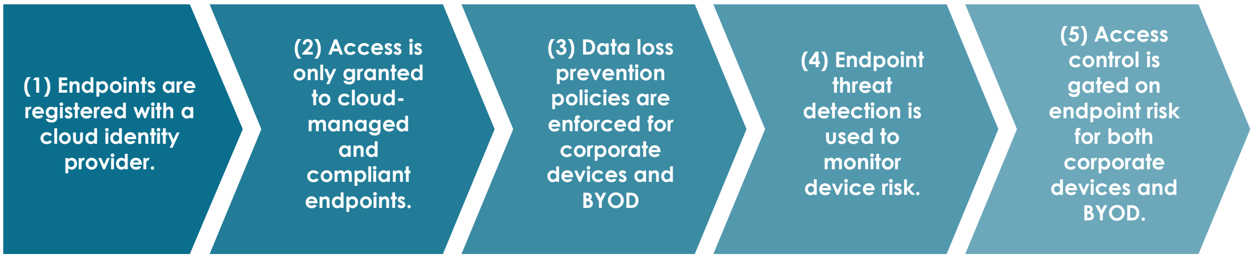
- Endpoint behavioral sensors
- Cloud security analytics
- Threat intelligence

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



(1) Endpoints are registered with a cloud identity provider.

(2) Access is only granted to cloud-managed and compliant endpoints.

(3) Data loss prevention policies are enforced for corporate devices and BYOD

(4) Endpoint threat detection is used to monitor device risk.

(5) Access control is gated on endpoint risk for both corporate devices and BYOD.

Device Identities

- registered
- joined
- hybrid joined

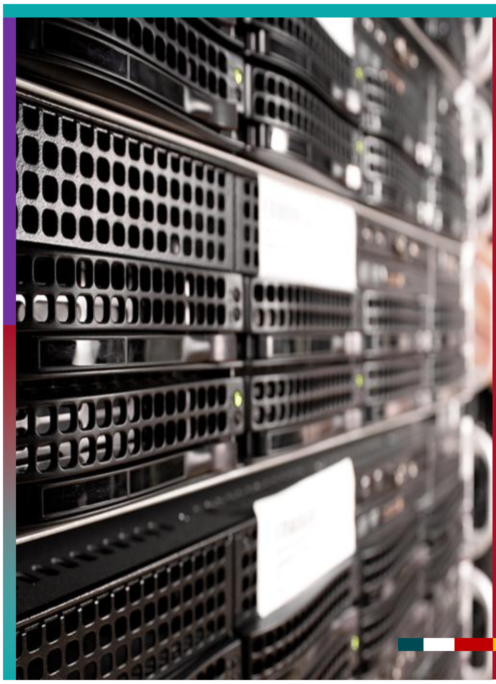
Intune enrollment

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

MDE Capabilities

Entra ID

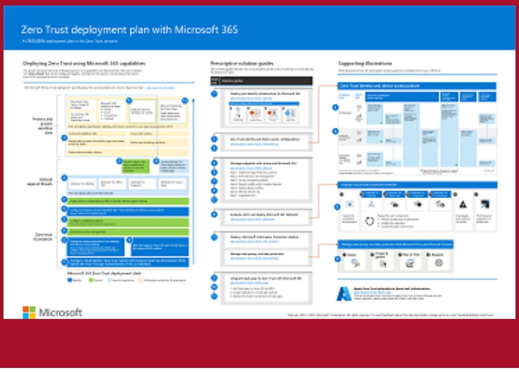
- Conditional Access Policies



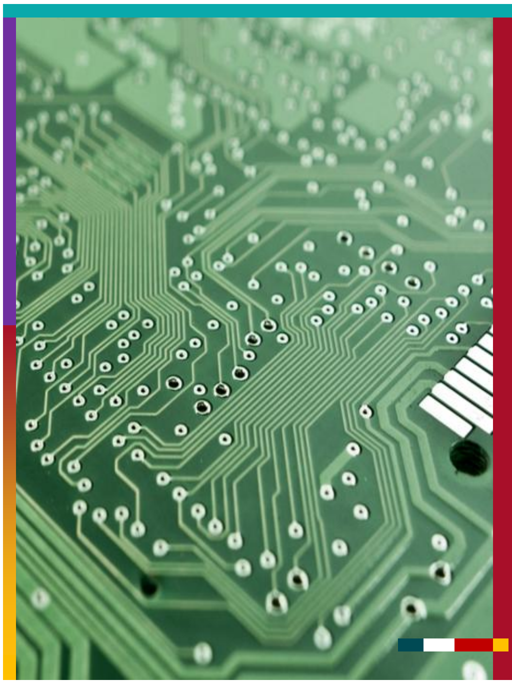
Pro Tip

MDE Zero Trust Deployment guide is part of

Zero Trust Deployment Guide



Zero Trust deployment plan with Microsoft 365



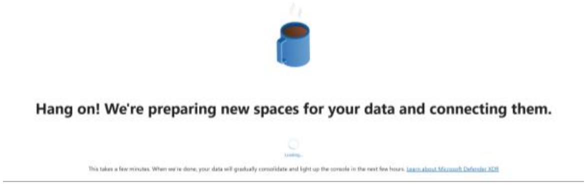
MDE Deployment

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

MDE Deployment

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



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

Loading...

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

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

MDE Deployment

Set up

- Data center location
  - same as for Defender XDR
  - cannot be changed
- Data retention
  - retained for 180 days
  - for advanced hunting queries only 30 days
  - use Sentinel e.g. to exceed this limits

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

Loading...

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

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)

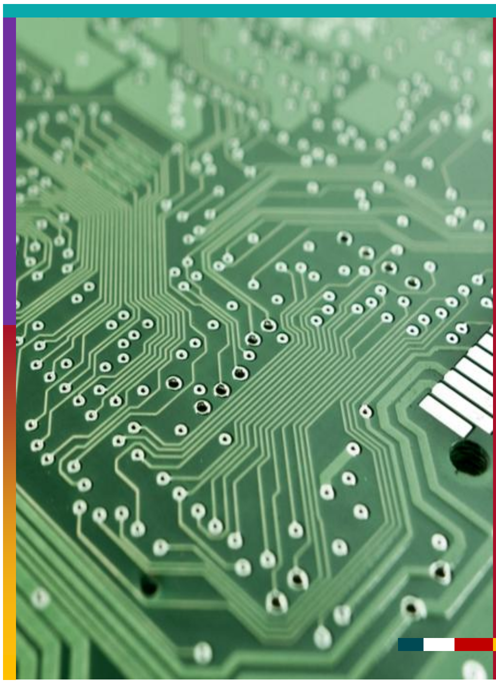
Onboard Devices

- 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

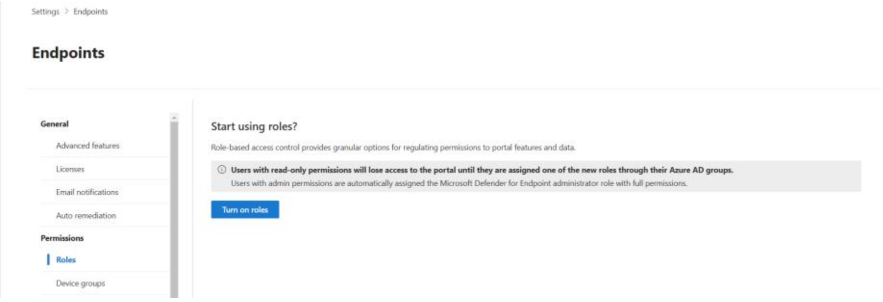
MDE Permissions

Role-based access control (RBAC)

- Configured in MDE settings
- Roles & Device groups
- suitable if tiering is necessary

- 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 cont.



Start using roles?

Role-based access control provides granular options for regulating permissions to portal features and data.

ⓘ **Users with read-only permissions will lose access to the portal until they are assigned one of the new roles through their Azure AD groups.**
Users with admin permissions are automatically assigned the Microsoft Defender for Endpoint administrator role with full 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

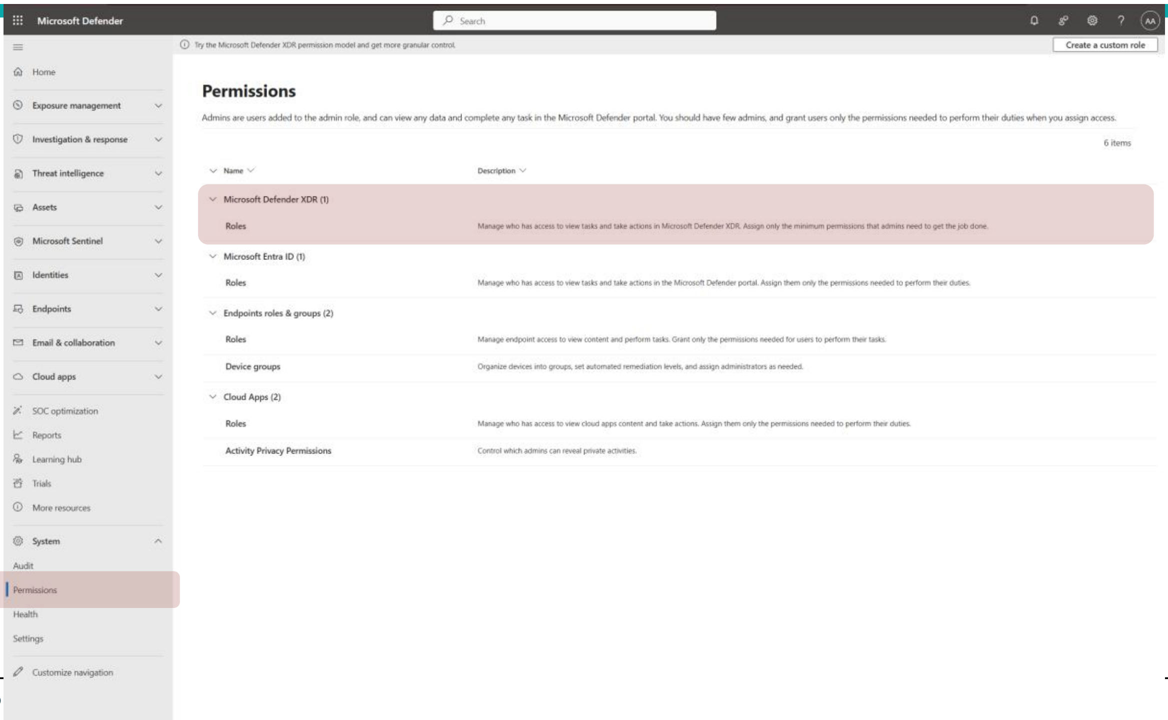
'The Microsoft Defender XDR Unified role-based access control (RBAC) model provides a single permissions management experience that provides one central location for administrators to control user permissions across different security solutions.'

- 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



Try the Microsoft Defender XDR permission model and get more granular control.

Permissions

Admins are users added to the admin role, and can view any data and complete any task in the Microsoft Defender portal. You should have few admins, and grant users only the permissions needed to perform their duties when you assign access.

6 items

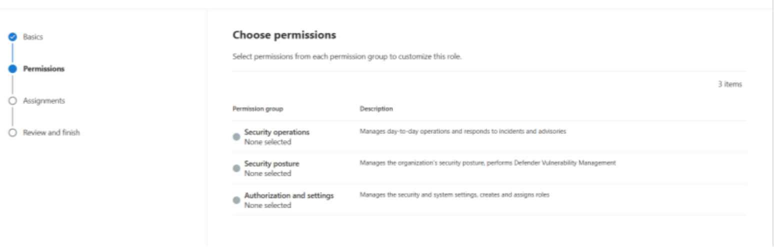
Name	Description
Microsoft Defender XDR (1)	
Roles	Manage who has access to view tasks and take actions in Microsoft Defender XDR. Assign only the minimum permissions that admins need to get the job done.
Microsoft Entra ID (1)	
Roles	Manage who has access to view tasks and take actions in the Microsoft Defender portal. Assign them only the permissions needed to perform their duties.
Endpoints roles & groups (2)	
Roles	Manage endpoint access to view content and perform tasks. Grant only the permissions needed for users to perform their tasks.
Device groups	Organize devices into groups, set automated remediation levels, and assign administrators as needed.
Cloud Apps (2)	
Roles	Manage who has access to view cloud apps content and take actions. Assign them only the permissions needed to perform their duties.
Activity Privacy Permissions	Control which admins can reveal private activities.

MDE Permissions - Unified RBAC

Role settings

- Name
- Description

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



● Basics
● **Permissions**
○ Assignments
○ Review and finish

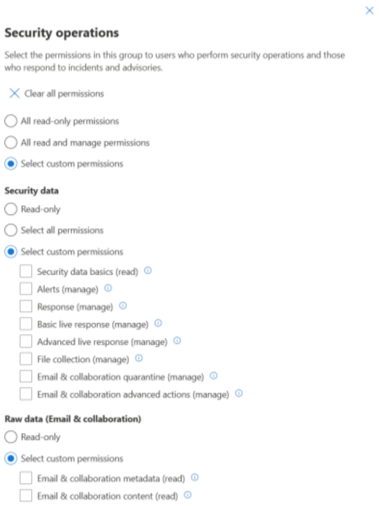
Choose permissions

Select permissions from each permission group to customize this role.

3 items

Permission group	Description
Security operations None selected	Manages day-to-day operations and responds to incidents and advisories
Security posture None selected	Manages the organization's security posture, performs Defender Vulnerability Management
Authorization and settings None selected	Manages the security and system settings, creates and assigns roles

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

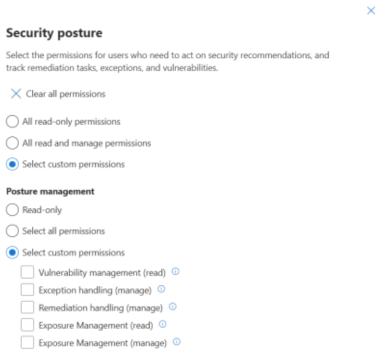
○ All read-only permissions
○ All read and manage permissions
● Select custom permissions

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

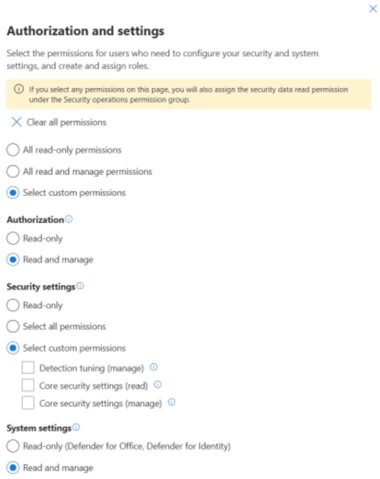
Select the permissions for users who need to act on security recommendations, and track remediation tasks, exceptions, and vulnerabilities.

× 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

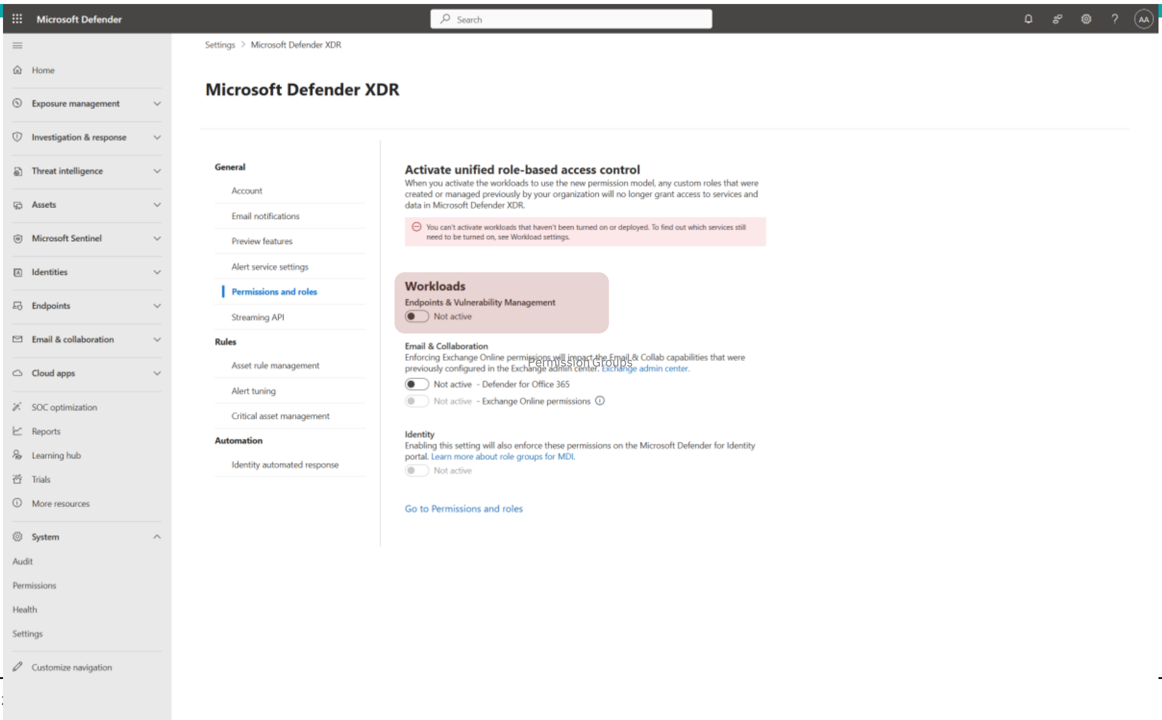
○ Read-only
● Read and manage

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



Microsoft Defender XDR

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

Permission Groups

MDE Permission

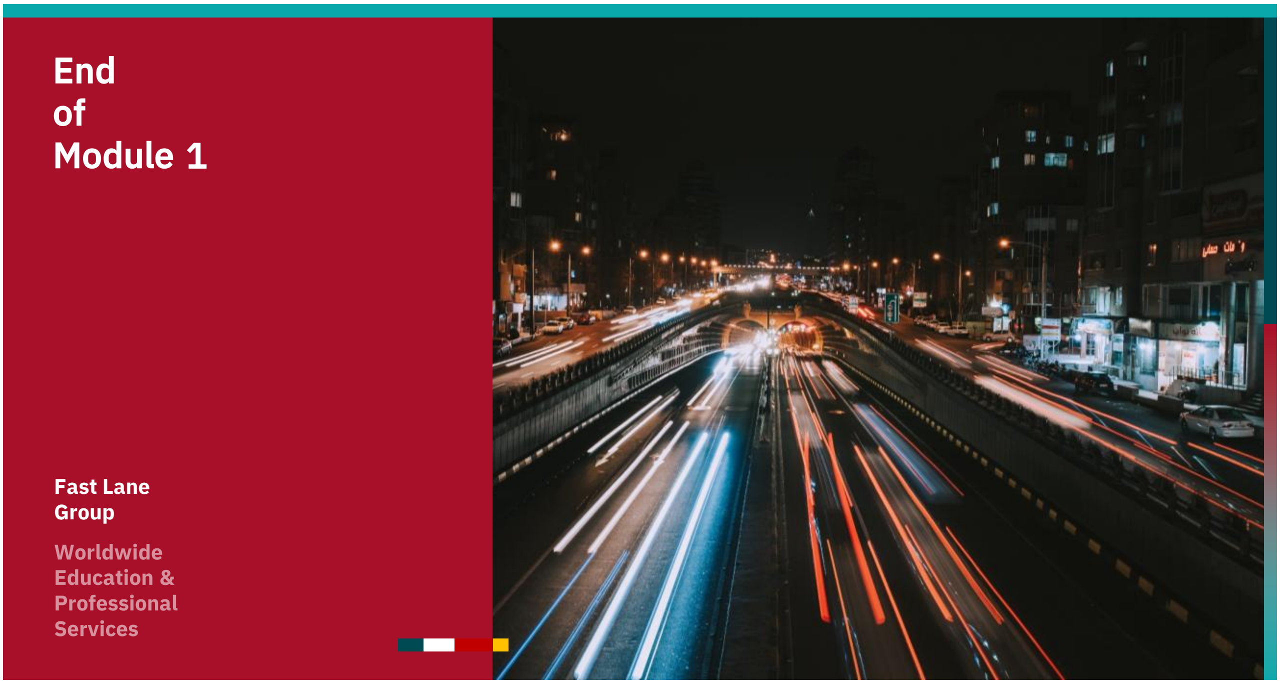
References

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

Questions?

Fast Lane Group

Worldwide Education & Professional Services



End of Module 1

Fast Lane Group

Worldwide Education & Professional Services