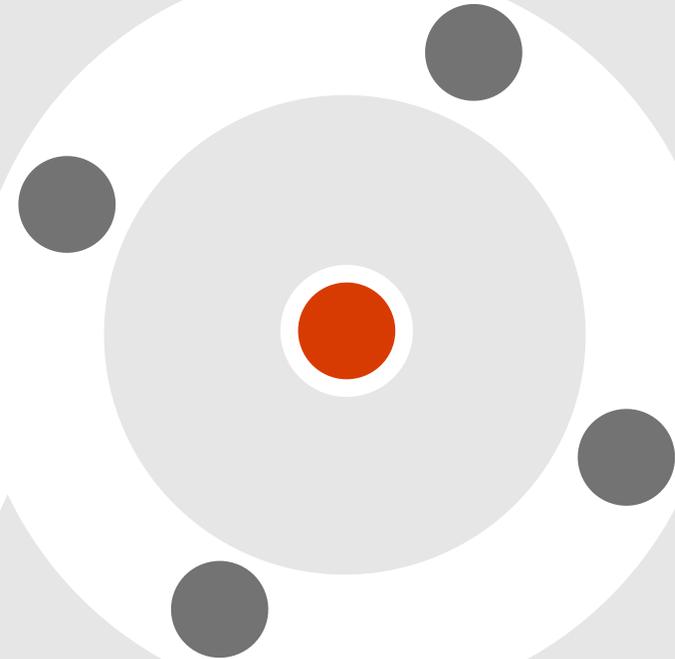


NIS2 Technology Mapping

Ellen van Meurs
Ronald Schouten
Tony Krijnen

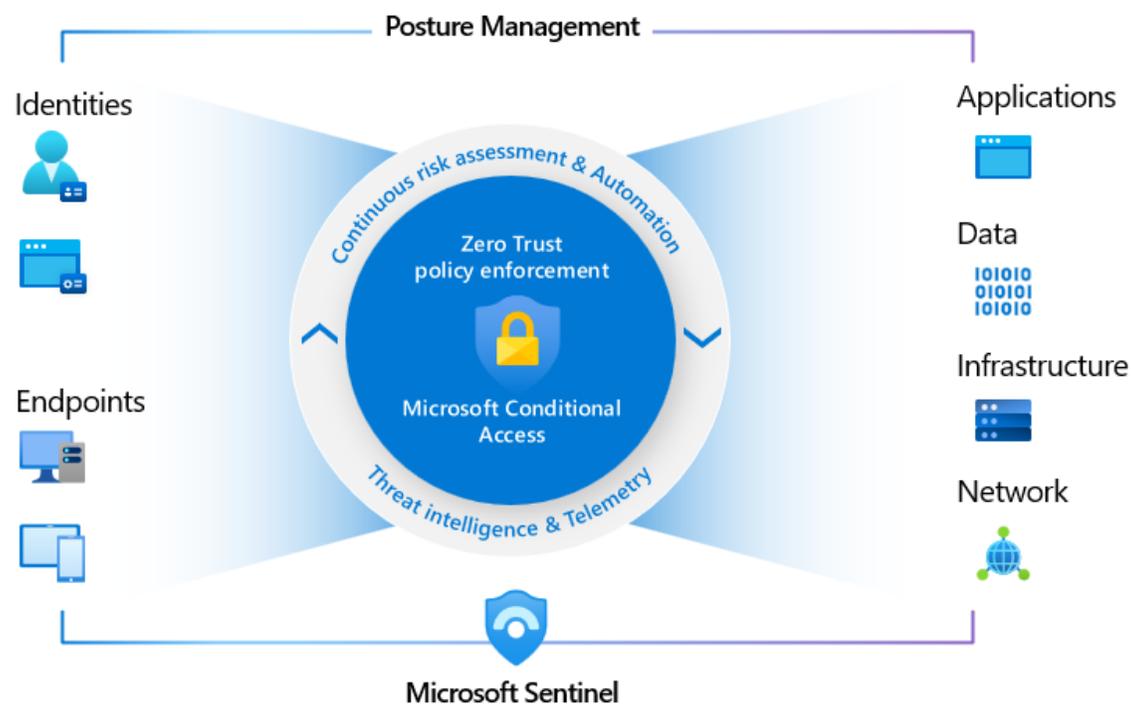


Purpose of this document

In the NIS 2.0 there are a number of duties defined that organizations that are subject to the NIS 2.0 directive will have to implement.

In this document we focus only on these duties and what an organization with Microsoft Office 365 and/or Microsoft Azure can do today. The purpose of this powerpoint is to visualize the technology components towards the NIS2, but is not exhaustive.

We will map the different duties on the Microsoft Zero Trust model. The Zero trust model covers the following areas:



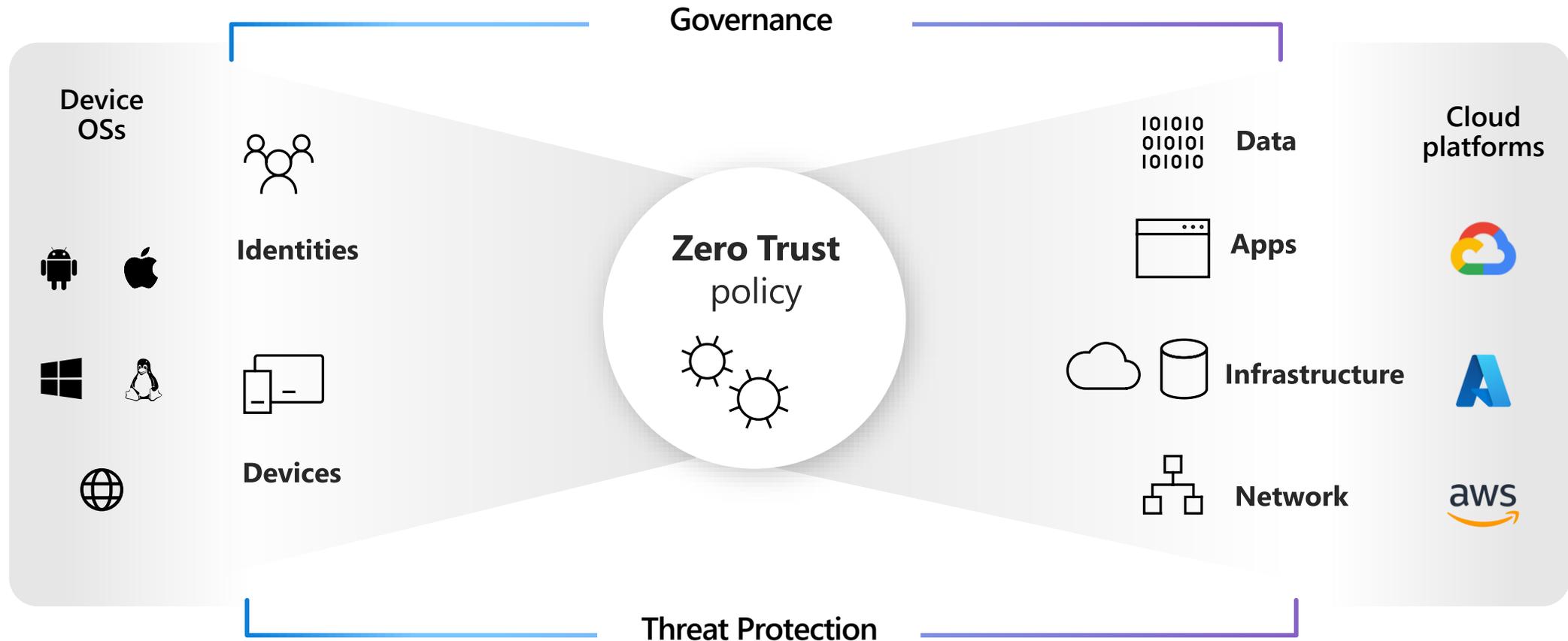
*This document is merely to demonstrate the capabilities of the platform with regards to the NIS 2.0 requirements. It is not complete nor will implementing this fulfill all NIS 2.0 requirements. More details will be added when the local implementation of the NIS 2.0 directive is clear.

NIS 2.0 Duties

- (a) policies on risk analysis and information system security;
- (b) incident handling;
- (c) business continuity, such as backup management and disaster recovery, and crisis management;
- (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- (g) basic cyber hygiene practices and cybersecurity training;
- (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- (i) human resources security, access control policies and asset management;
- (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

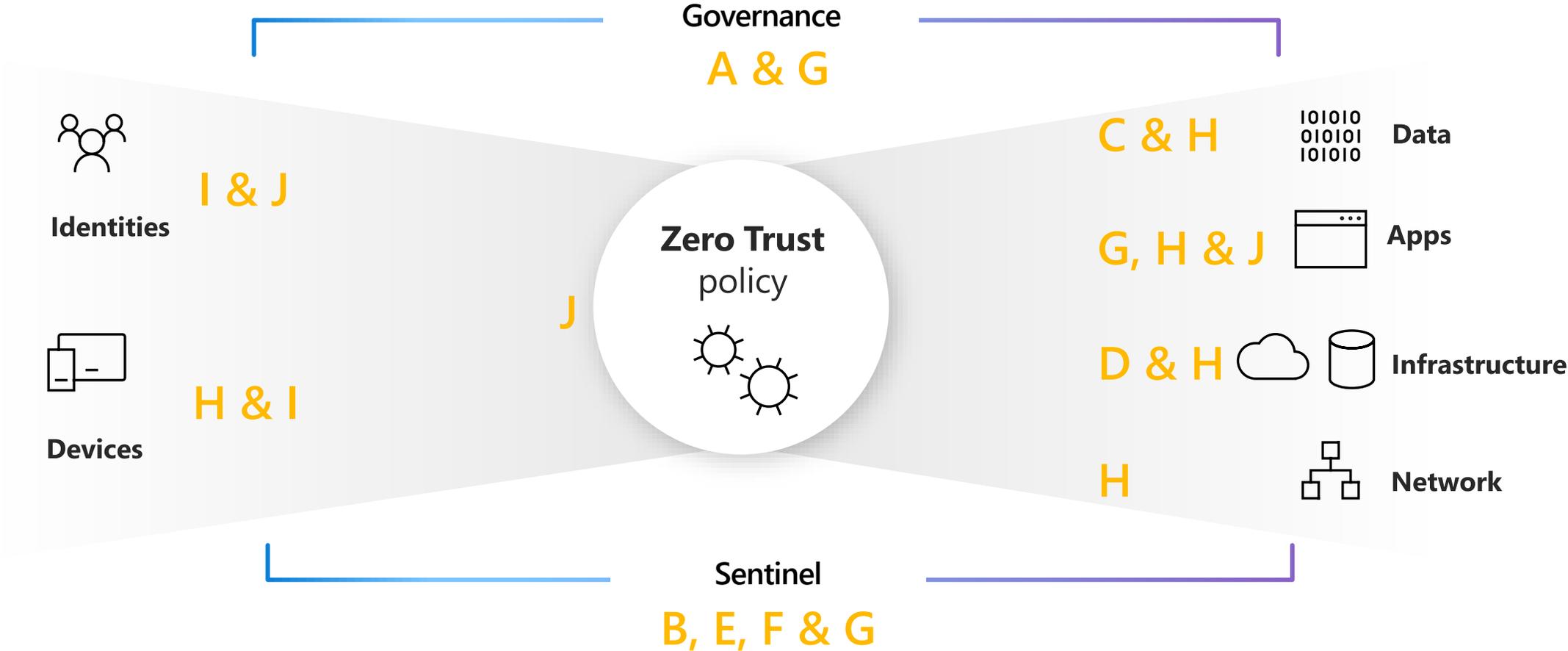
Microsoft Zero Trust product overview

Verify **explicitly** | Use **least-privileged access** | Assume **breach**



Mapping NIS 2.0 Duties to the Microsoft Zero Trust

Verify **explicitly** | Use **least-privileged access** | Assume **breach**



Policies on risk analysis and information system security



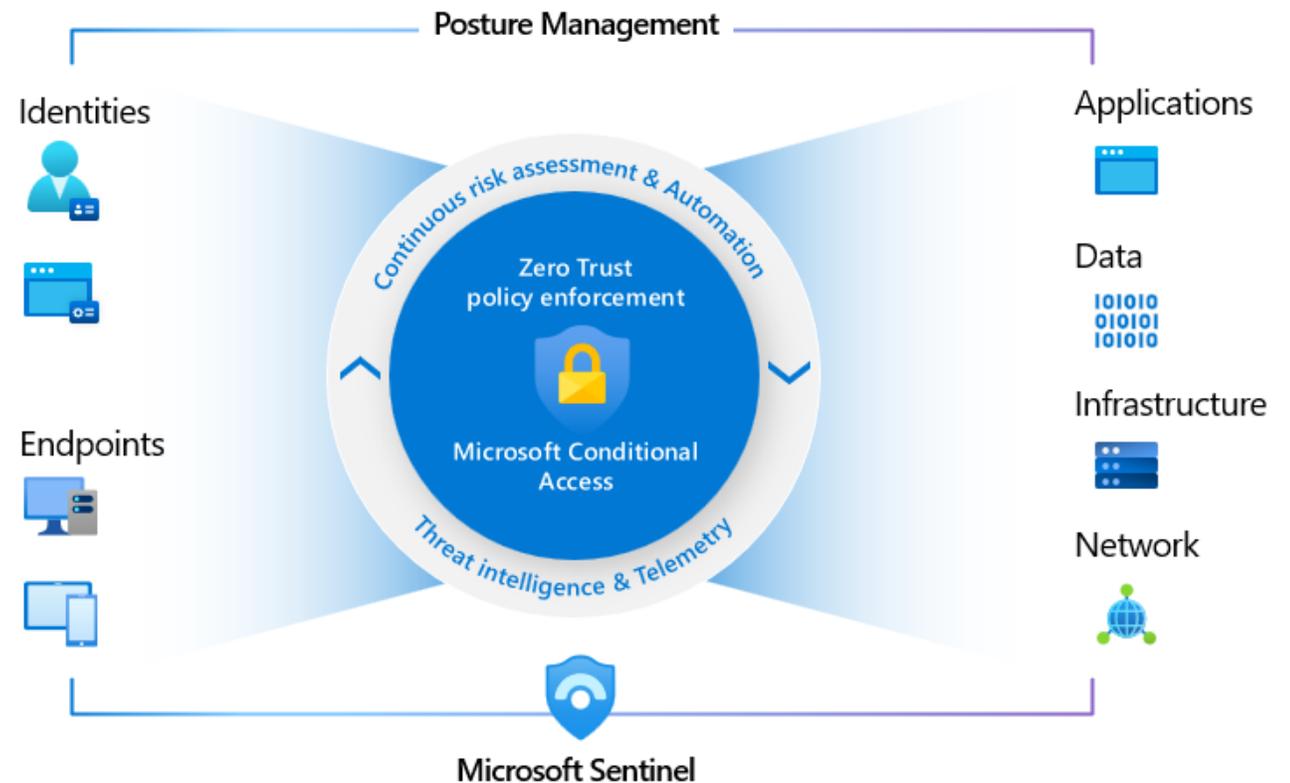
Explanation

Effective security policies must be implemented consistently across the organization to protect information systems and customers. Security policies must also account for variations in business functions and information systems to be universally applicable.



Zero Trust Framework

Zero Trust architecture recommends continuous risk assessment in the digital world where attacks happen at cloud speed. Each request shall be intercepted and verified explicitly by analyzing signals on user, location, device compliance, data sensitivity, and application type.



Incident handling

Security incident handling is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. It seeks to give a robust and comprehensive view of any security issues within an IT infrastructure.

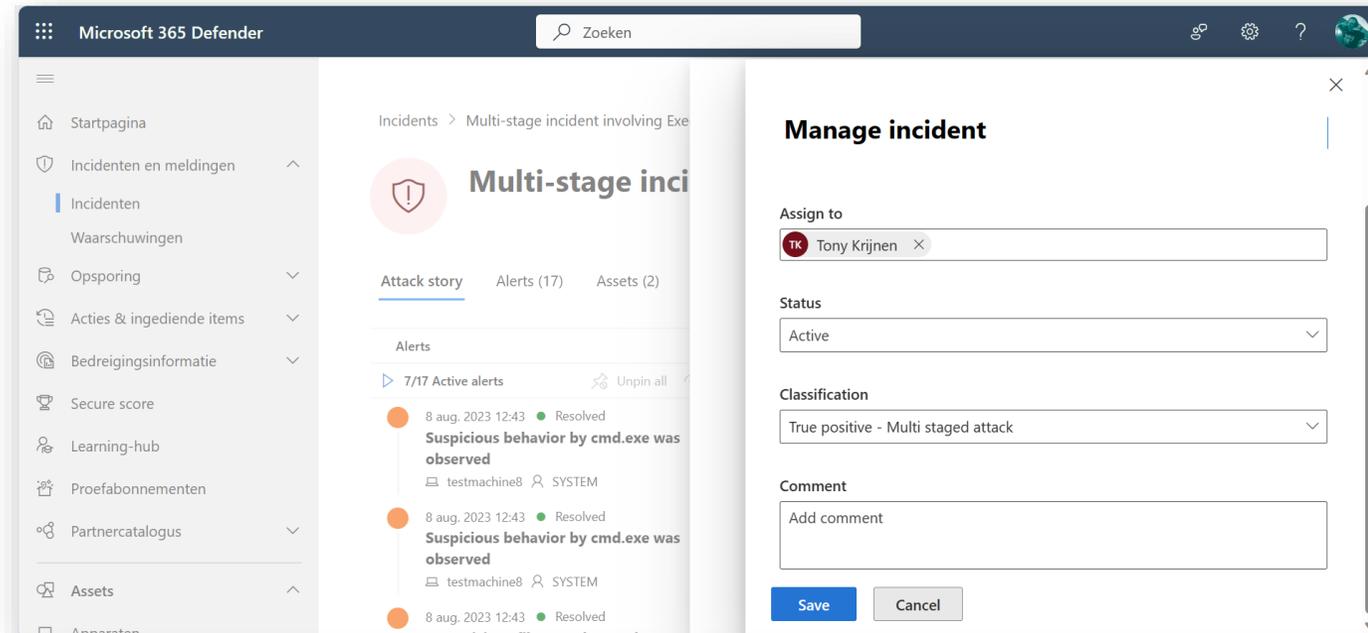
Incident handling with Microsoft Defender

The standard Microsoft Defender security incident homepage allows staff to assign, label, classify and comment on the incidents.

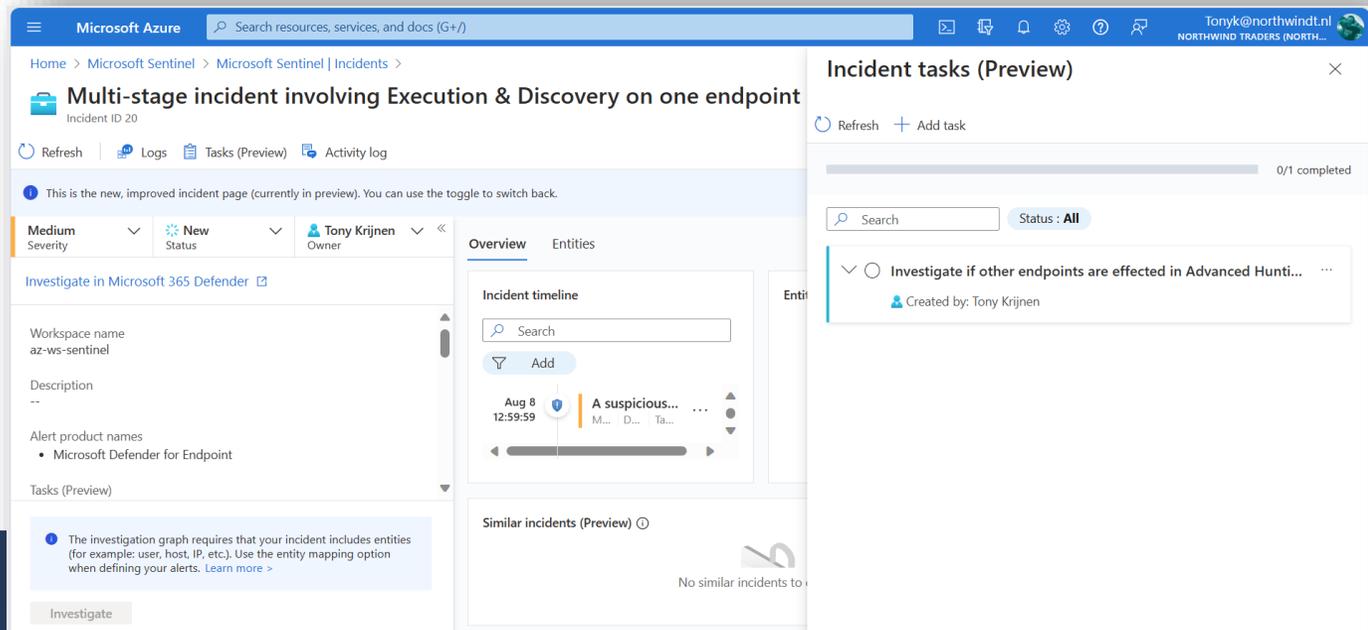
Incident handling with Microsoft Sentinel

Microsoft Sentinel is the Microsoft SIEM (Security Information and Event Management) solution. Sentinel analyzes the signals from all different sources in the organization and allows for full incident and event management, creating and assigning tasks, activity logs, etc.

More information on [Sentinel Incident handling](#)



The screenshot displays the Microsoft 365 Defender web interface. The left sidebar contains navigation options: Startpagina, Incidenten en meldingen, Incidenten, Waarschuwingen, Opsporing, Acties & ingediende items, Bedreigingsinformatie, Secure score, Learning-hub, Proefabonnementen, Partnercatalogus, Assets, and Apparaten. The main content area shows a 'Multi-stage incident involving Execution & Discovery on one endpoint'. Below this, there are tabs for 'Attack story', 'Alerts (17)', and 'Assets (2)'. The 'Alerts' section lists several alerts with the message 'Suspicious behavior by cmd.exe was observed'. On the right, a 'Manage incident' panel is open, allowing users to assign the incident to 'Tony Krijnen', set the status to 'Active', and classify it as 'True positive - Multi staged attack'. There is also a 'Comment' field and 'Save' and 'Cancel' buttons.



The screenshot shows the Microsoft Azure Sentinel interface. The top navigation bar includes 'Microsoft Azure' and a search bar. The main content area displays a 'Multi-stage incident involving Execution & Discovery on one endpoint' with an incident ID of 20. Below the incident title, there are tabs for 'Refresh', 'Logs', 'Tasks (Preview)', and 'Activity log'. The 'Tasks (Preview)' tab is active, showing a task titled 'Investigate if other endpoints are effected in Advanced Hunti...'. The task is created by Tony Krijnen and is currently 0/1 completed. The interface also shows an 'Incident timeline' and 'Similar incidents (Preview)' section.

Incident handling

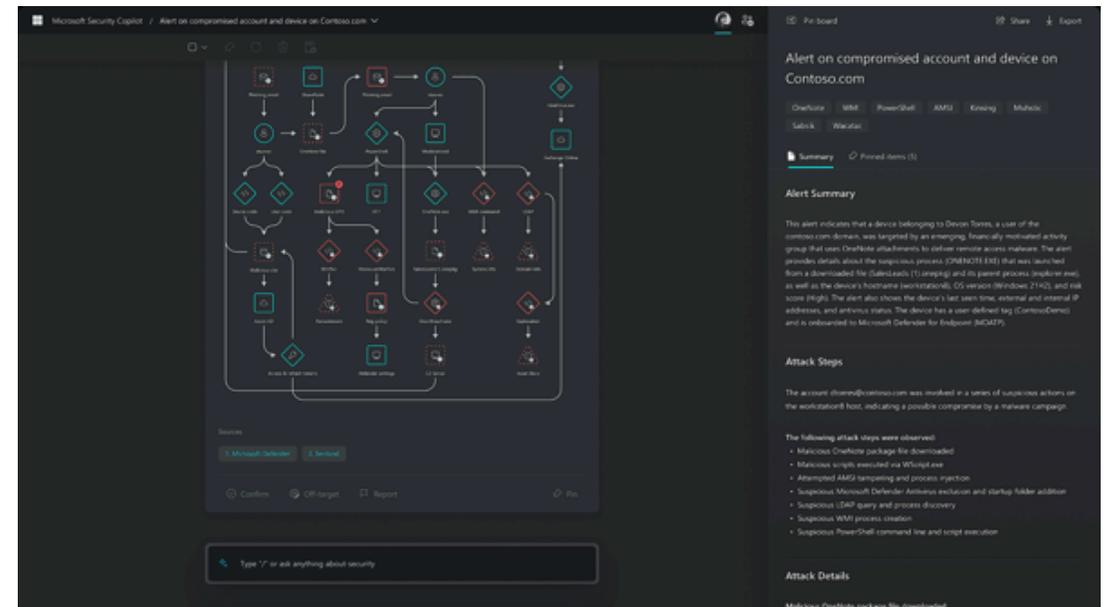
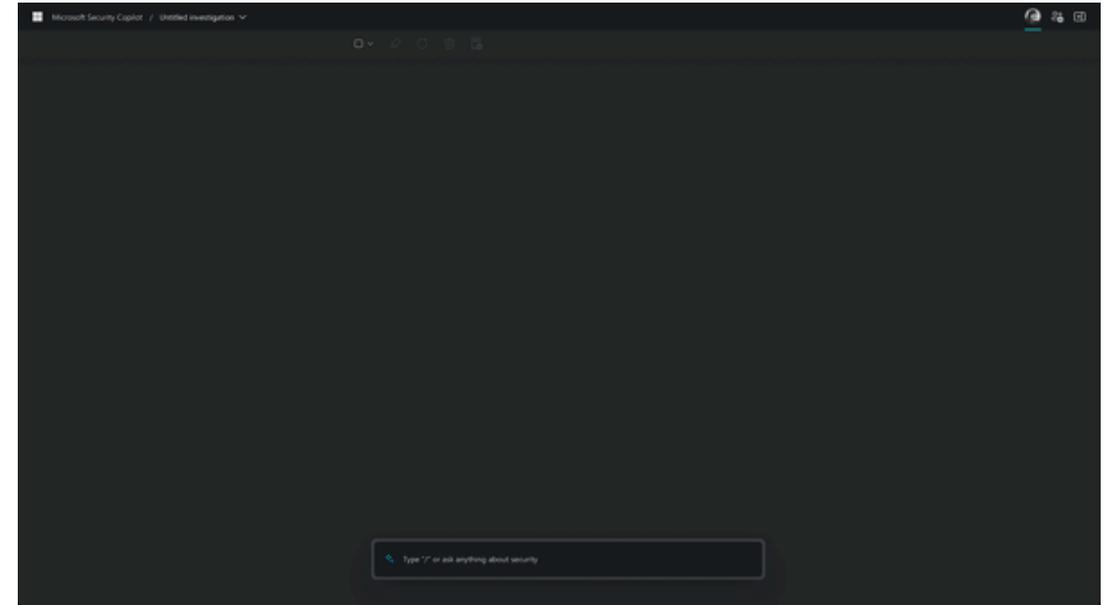
Security incident handling is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. Leveraging AI solutions will enable organizations to shorten time needed to analyze data and logs as well as stop attacks based on ML patterns.

Security CoPilot

Microsoft Security Copilot is an AI-powered security analysis tool that enables analysts to respond to threats quickly, process signals at machine speed, and assess risk exposure in minutes.

Identify an ongoing attack, assess its scale, and get instructions to begin remediation based on proven tactics from real-world security incidents.

More information on [Security Copilot](#)



Business continuity – Backup management (1)

Business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyberattacks and communication failures. Aspects of business continuity are Backup management, Disaster recovery and Crisis management. We will cover each topic in a separate slide, this is the slide on Microsoft 365 backup management.

Microsoft 365 Backup

Microsoft 365 backup is a feature that allows you to recover your OneDrive, SharePoint, and Exchange data in case of data loss or corruption. You can backup all or select sites, accounts, and mailboxes in your tenant, and restore them to a prior point-in-time. You can access Microsoft 365 backup directly in the Microsoft 365 admin center or through a partner's application built on top of the Backup APIs1.

Microsoft 365 Archiving

Microsoft 365 Archive gives you a cold data storage tier that enables you to keep inactive or aging data within SharePoint at a cost-effective price point matching the value of that data's lifecycle stage. Because the content is archived in place, it retains Microsoft 365's valuable security, compliance, search, and rich metadata.

More information on
[Microsoft 365 Backup & Archive](#)

The image shows a composite of two screenshots from the Microsoft 365 admin center. The top screenshot is a promotional card for 'Microsoft 365 Backup', describing it as a reliable, secure, and scalable native backup solution for Microsoft 365 content across SharePoint, OneDrive, and Exchange. It highlights two options: 'Microsoft Provided Application' (an add-on service for enhanced restore coverage) and 'Platform for Partner Solution' (an API platform for third-party ISV partners). Below this, 'Key Capabilities' are listed: Content Backups (in-place backups at service-defined frequencies), Browse or Search (content discovery tools), Restore (restore content at desired granularity), and Monitoring (audit changes and control storage usage).

The bottom screenshot is a screenshot of the 'SharePoint admin center' interface. It features a navigation pane on the left and a main content area with several cards. The top card is 'Manage inactive sites with M365 Archive', which includes a 'View recommendation' button and a play button icon. Below it are 'Site search' (with a search input field), 'Message center' (showing '5 unread messages'), and 'Active storage used' (a line chart showing storage usage over time, with a note: 'So far you've used 1.32 TB of your available storage'). To the right, there is a 'SharePoint file activity report' card showing '17.8K SharePoint files' and a 'Free space by archiving inactive sites' card with '600 Inactive sites' and '450 GB Storage used'. A 'High risk' notification is also visible at the bottom.

Business continuity – Backup management (2)

Business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyberattacks and communication failures.

Aspects of business continuity are Backup management, Disaster recovery and Crisis management. We will cover each topic in a separate slide, this is the slide on Microsoft Azure backup management.



Microsoft Azure Backup

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.

Azure Backup helps protect your critical business systems and backup data against a ransomware attack by implementing preventive measures and providing tools that protect your organization from every step that attackers take to infiltrate your systems. It provides security to your backup environment, both when your data is in transit and at rest.

What is [Microsoft Azure Backup](#) ?

Home > northwindt-RecVault1

northwindt-RecVault1 | Backup ☆ ...
Recovery Services vault

Immutable Vault
northwindt-RecVault1

⚠ Enabling this property helps you ensure that recovery points once created cannot be deleted before their intended expiry. While this helps prevent data loss, you would not be able to perform certain operations on this vault and its protected items. [Learn more.](#)

The immutable vault property would further need to be 'locked' in order to make it permanent, after which it cannot be reverted to a disabled state. Hence, it is recommended that you take a well informed decision before enabling and then further locking this property. [Learn more.](#)

Enable vault immutability ⓘ

Lock immutability for this vault ⓘ
 Locked

Confirm locking immutability. Once locked, it cannot be disabled.

⚠ The storage replication is set to Geo-Redundant. This option cannot

Where is your workload running?
On-Premises

What do you want to backup?
0 selected

- Files and folders
- Hyper-V Virtual Machine
- VMWare Virtual Machine
- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Exchange
- System State
- Bare Metal Recovery

Backup items

Business continuity – Disaster Recovery

Business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyberattacks and communication failures. Aspects of business continuity are Backup management, Disaster recovery and Crisis management. We will cover each topic in a separate slide, this is the slide on Microsoft Disaster Recovery.



Microsoft Azure Site Recovery

Azure Site Recovery is a service that helps you keep your business running during IT outages. It allows you to replicate your workloads to Azure or another location, and fail over and recover them when needed. You can use it to protect Azure VMs, on-premises VMs, physical servers, and databases. Azure Site Recovery offers simple deployment and management, cost savings, reliable recovery, and security features

Home > Recovery Services vaults > Recovery | Site Recovery >

Enable replication

Hyper-V machines to Azure

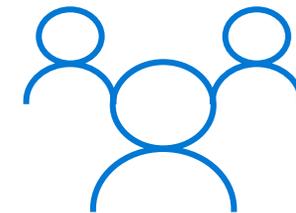
✔ Source environment ✔ Target environment **3 Virtual machine selection** ④ Replication set

i Only those machines which can be protected using managed disk are visible in this list. Unable to view/select other VM [more](#)

i Finished retrieving data.

Filter items...

- DCSERVER
- Navision
- BackupServer
- SERVER-2022
- SERVER1-2012R2-Ess



Supply chain security

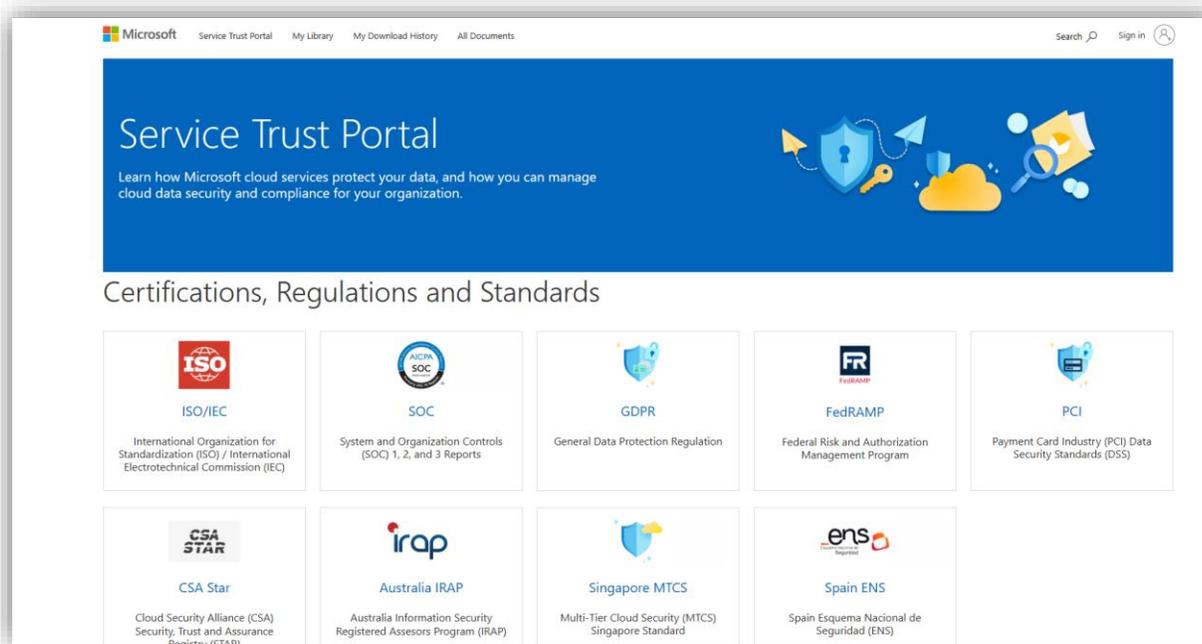
Digital supply chains are becoming more complex, more digital, and more interdependent, which means that any vulnerability or attack in one part of the supply chain can have a ripple effect on the entire chain. One example of this is how Microsoft is showcasing their compliance.

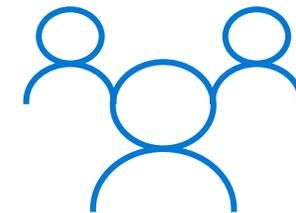
» Compliance (3rd party assurance/SOC verklaring)

Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

» External Access (technology)

Entra ID Connect is an on-premises Microsoft application that's designed to meet and accomplish your hybrid identity goals. Use Entra ID Connect to benefit from a modernized Active Directory and benefit from security features such as single sign on and conditional access policies.





Supply chain security

Digital supply chains are becoming more complex, more digital, and more interdependent, which means that any vulnerability or attack in one part of the supply chain can have a ripple effect on the entire chain. One example of this is the way partners can access a customer tenant through their Partnercenter environment.

DAP vs GDAP

DAP (Delegated Admin Privileges) is the old way of granting partners access to customers' tenants, which gives them too much power (Global Admin) and poses security risks. The new GDAP (Granular Delegated Admin Privileges) grants partners access to customers' tenants but only to the necessary roles and use permissions for a limited time. Customers should check if their partner tenant has access to their tenant leveraging GDAP instead of DAP to ensure that they have more control and visibility over their data and resources, and that they comply with the latest security best practices.

Partner relationships

These are the partners that you authorized to work with your organization. Each partner has different responsibilities for working with your organization, and some might have roles. [Learn more about working with a partner](#)

① Reduce your security risk by limiting the access your partners have to your organization. [Learn about Granular Delegated Administrative Privileges \(GDAP\)](#)

⚠ You should review the delegated administrative privileges (DAP) enabled for your partners to confirm if they still need DAP access to your organization's data.



Review your partner agreements

Make sure partners still need their approved roles.

Granular delegated administrative privileges (GDAP)

Partner and associated relationships ↓

Authorized roles

Role authorization ⓘ

Expiration date

Security in network and information systems acquisition, development and maintenance

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.



Defender Vulnerability Management

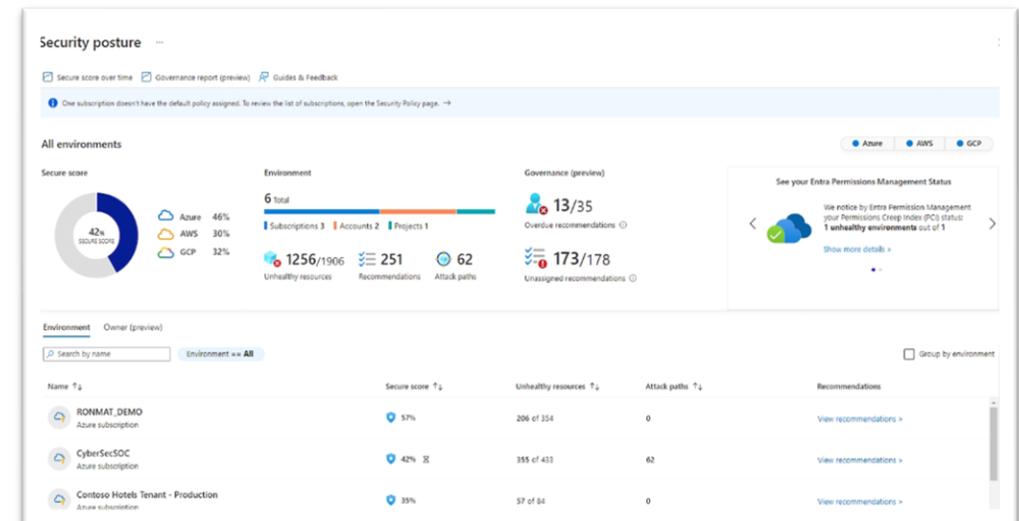
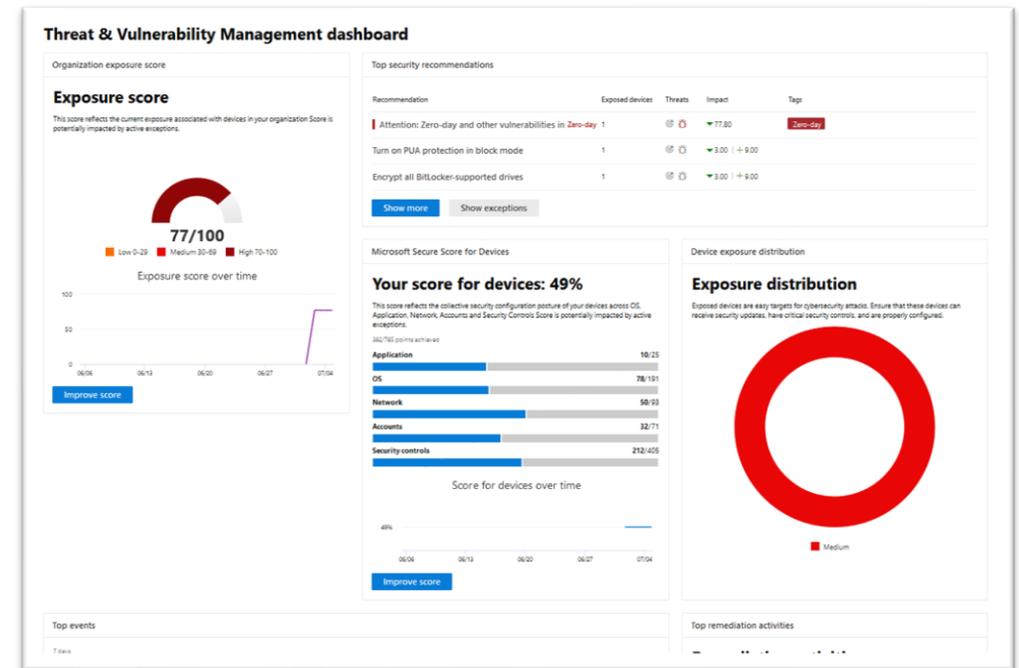
Defender Vulnerability Management (DVM) delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.



Cloud Security Posture Management

Cloud Security Posture Management (CSPM) provides you with hardening guidance that helps you efficiently and effectively improve your security. CSPM also gives you visibility into your current security situation.

Get started with [DVM](#) and [CSPM](#)



Security in network and information systems acquisition, development and maintenance

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.



Defender for IoT

Defender for IoT is a security solution that protects IoT and OT devices from physical and cyber threats. It provides asset discovery, vulnerability management, and threat detection for complex, digital, and interdependent environments. It also integrates with other security tools such as Sentinel, Splunk, and Defender for Endpoint

Home > Defender for IoT

Defender for IoT | Sites and sensors

Showing subscription 'NORTHWINDT10-2023 Demo Subscription'

Search Refresh Onboard sensor Sensor settings Sensor update Threat intelligence update (Preview)

General

Getting started

Device inventory

Alerts

Recommendations (Preview)

Workbooks

Firmware analysis (Preview)

Management

Sites and sensors

Plans and pricing

Troubleshooting + Support

Diagnose and solve problems

Search Add filter

1 All sensors 1 EIoT 0 OT - Cloud connected 0 OT - Locally managed 0 Unhealthy 0 Unsupported

Showing one sensor

<input type="checkbox"/>	Sensor name	Sensor type	Zone	Subscription name	Sensor ...	Sensor version
<input type="checkbox"/>	Enterprise-network - Enterprise network					
<input type="checkbox"/>	IOT-DenBosch-Site73	EIoT	default	NORTHWINDT10-20	Pen...	-

Security in network and information systems acquisition, development and maintenance

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.



Defender for DevOps

Defender for DevOps uses a central console to empower security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, such as GitHub and Azure DevOps. Findings from Defender for DevOps can then be correlated with other contextual cloud security insights to prioritize remediation in code.

Get started with [Defender for DevOps](#)

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | DevOps security (preview)

Showing subscription 'NORTHWINDT10-2023 Demo Subscription' | PREVIEW

Search Refresh Guides and Feedback

General

- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Data security (Preview)
- Firewall Manager
- DevOps security (preview)

Management

- Environment settings
- Security solutions
- Workflow automation

DevOps Security

Defender for DevOps addresses the intersection of DevOps with the current threat landscape. It provides end-to-end security including visibility into code and code management systems and security capabilities that help prevent, detect, and respond to current threats. By shifting cloud security left, risk is addressed earlier across every stage of the cloud application lifecycle—development, build, and operations.

For more information, please refer to the [documentation](#).

Get started

Onboarding GitHub t...

GitHub

Defender for DevOps addresses the interaction of DevOps in the current threat landscape. Follow the steps to Create a GitHub connector to your source code management systems. Discover DevOps resources and onboard them to Microsoft Defender for Cloud.

Onboarding Azure D...

Azure DevOps

Defender for DevOps addresses the interaction of DevOps in the current threat landscape. Follow the steps to Create an ADO connector to your source code management systems. Discover DevOps resources and onboard them to Microsoft Defender for Cloud.

1. Connect DevOps environments

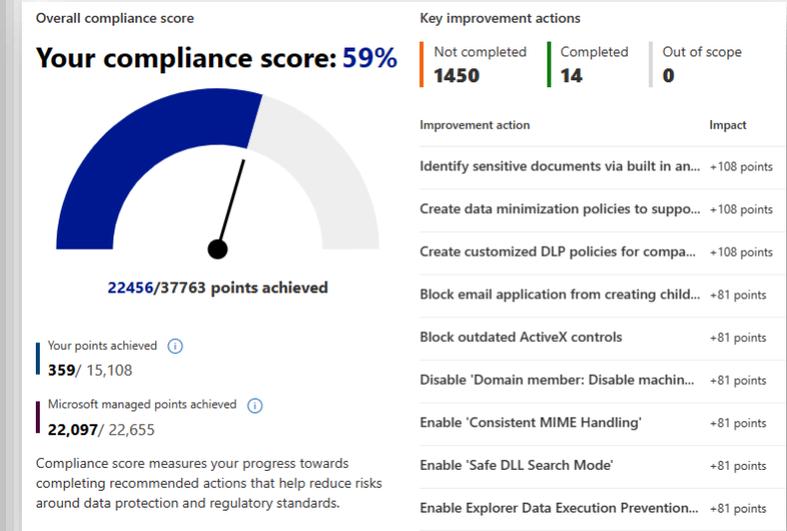
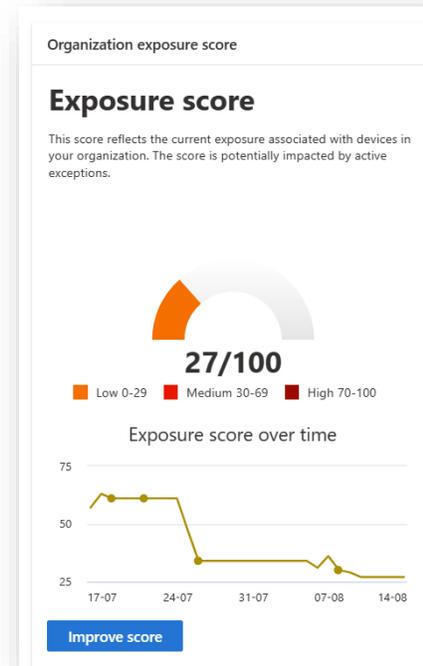
Create a connector to your source code management systems. Discover DevOps resources and onboard them to Microsoft Defender for Cloud.

Add connector

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (1)

Although there are many methods and frameworks for policies, procedures and assessing the effectiveness of cybersecurity risk-management measures, common steps are:

- Understand the security landscape of your organization, including its assets, systems, vendors, and regulations
- Identify gaps in your current cybersecurity controls, such as outdated software, weak passwords, or phishing vulnerabilities
- Create a team of qualified and experienced cybersecurity professionals who can monitor, respond, and improve your security posture
- Determine the informational value of your assets and prioritize them based on their importance and sensitivity
- Analyze and address the risks that pose the most threat to your assets, using tools such as penetration testing, risk scoring, and mitigation strategies



Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (2)

This slide focusses on how you can understand the security landscape of your organization. Microsoft Secure Score helps organizations by reporting on the current state of the organization's security posture; Improve security posture by providing discoverability, visibility, guidance, and control and compare with benchmarks and establish key performance indicators (KPIs).

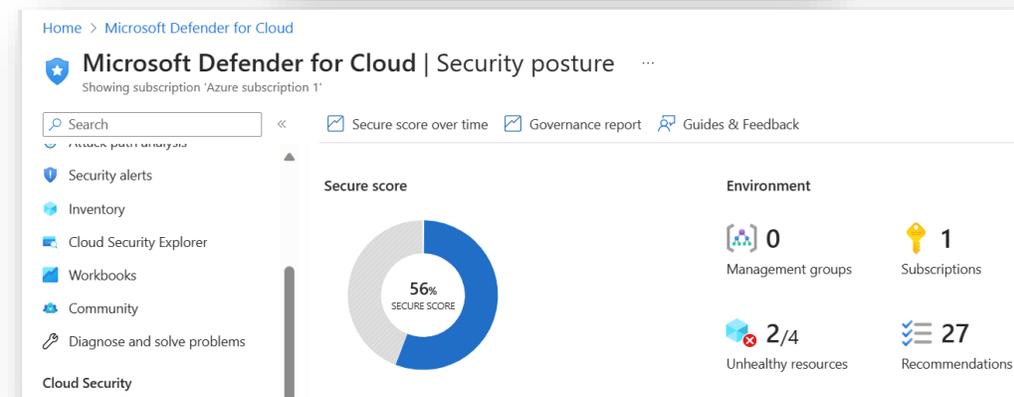
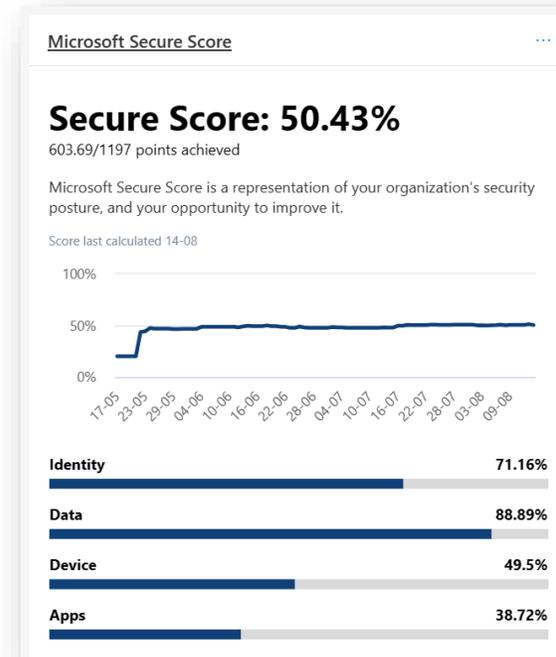
Microsoft Defender Secure Score

The Microsoft Defender Secure Score is applicable for Microsoft SaaS workloads, such as Microsoft 365, Identity, Devices and Apps. It evaluates your configuration settings and behaviors and gives you a score based on the alignment with security standards.

Microsoft Defender for Cloud Secure Score

The Microsoft Defender for Cloud Secure Score applies to PaaS, IaaS, hybrid and multi-cloud workloads. It assesses your cross-cloud resources for security issues and gives you a score based on the implementation of best practices. Defender for Cloud can provide recommendations for Microsoft Azure, Amazon Web Services, Google Cloud Suite, etc.

More information on [Secure Score](#)



Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (3)

This slide focusses on how you can identify gaps in your current cybersecurity controls, such as outdated software, weak passwords, or phishing vulnerabilities.



Microsoft Defender Exposure Score

Microsoft Defender exposure score is a metric that reflects how vulnerable your organization is to cybersecurity threats. Your exposure score is influenced by factors such as weaknesses, threats and security alerts on your devices.



Microsoft Defender for Identity

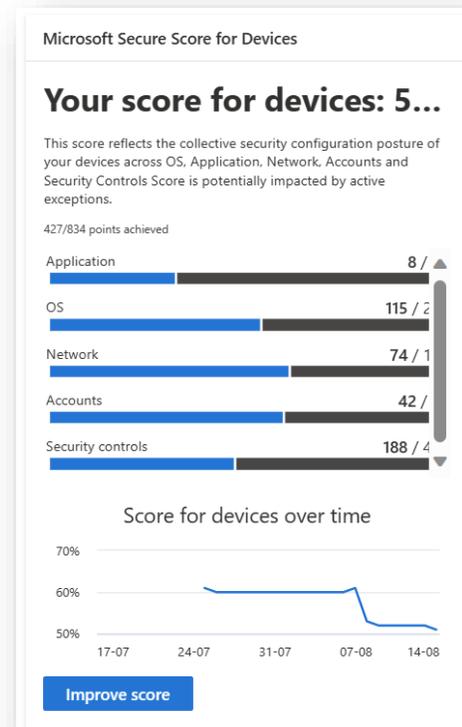
Defender for Identity can detect accounts with unsecure attributes that expose a security risk, such as PasswordNotRequired. It can also detect weak cipher usage on devices and accounts, such as RC4 or DES2. Additionally, it can alert you of credential access attempts by malicious actors.



Compliance manager

Compliance score measures progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

More information on [Compliance Score](#)



Top vulnerable software

Software	OS platform	Weaknesses	Threats	Exposed devices
Windows 11	Windows	277	🔴	3 / 4
Office	Windows	8	🔴	3 / 3
.net Framework	Windows	8	🔴	3 / 5

Show more

Top exposed devices

Name	Security recommendations	Discovered vulnerabilities	Exposure level
ams-sbk-24	58	450	🔴 High
ams-srv-dc22	48	168	🔴 High
anh_android	4	133	🔴 Medium

Show more

Export actions | Update actions | Accept all updates | Assign to user

Regulations: Any | Solutions: Any | Groups: Any | Test Status: None, Not assessed, Failed low risk, +7 X

Improvement action	Points achi...	Service	Regulations
<input type="checkbox"/> Identify sensitive documents via built in and custo...	0/108	Microsoft 365	(4) Data Protection Bas...
<input type="checkbox"/> Create data minimization policies to support priva...	0/108	Microsoft 365	(4) Data Protection Bas...
<input type="checkbox"/> Create customized DLP policies for company sensi...	0/108	Microsoft 365	(4) Data Protection Bas...
<input type="checkbox"/> Block email application from creating child proces...	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Block outdated ActiveX controls	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Disable 'Domain member: Disable machine accou...	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Enable 'Consistent MIME Handling'	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Enable 'Safe DLL Search Mode'	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Enable Explorer Data Execution Prevention (DEP)	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Turn on scanning of downloaded files and attach...	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Enable 'MIME Sniffing Safety Feature'	0/81	Microsoft 365	(3) Data Protection Bas...
<input type="checkbox"/> Turn on email scanning for antivirus solution	0/81	Microsoft 365	(3) Data Protection Bas...

Basic cyber hygiene practices and cybersecurity training (1)

Cybersecurity training is the process of educating yourself and others about the risks and best practices of cyber hygiene. Training can help you develop the skills and knowledge to protect yourself and your organization from cyber threats.

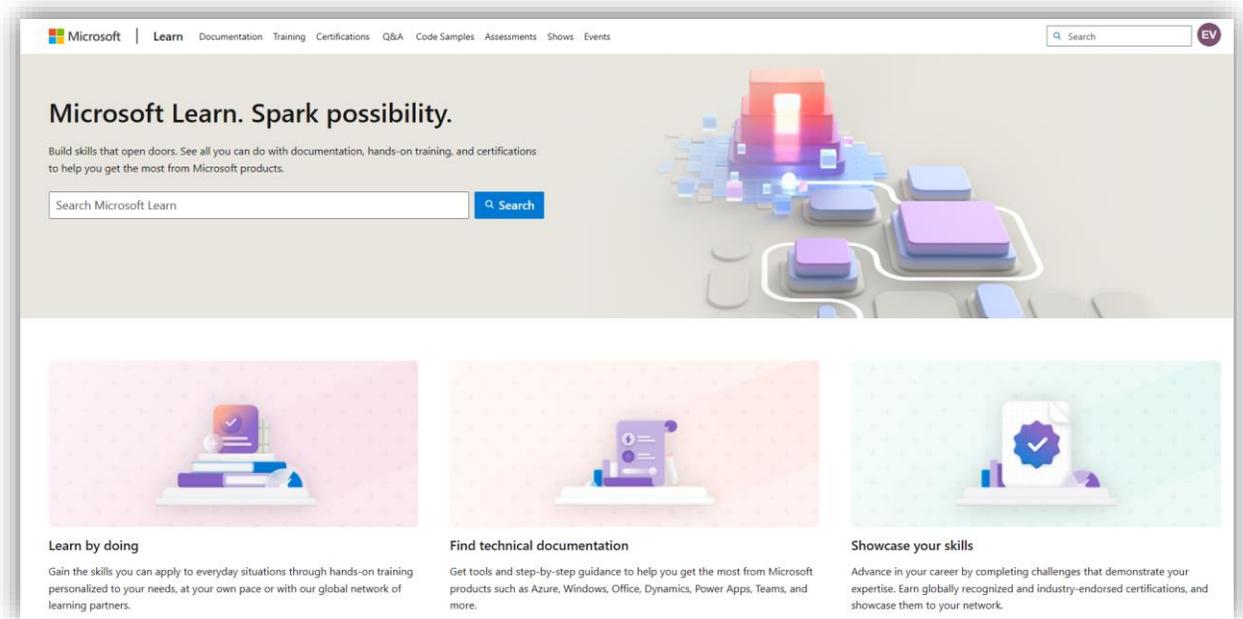
Microsoft 365 Learn

Microsoft Learn offers learning paths for Microsoft 365, Security and Microsoft Teams, as well as virtual training days and a community to connect with other learners and professionals. Microsoft Support provides video training, templates, quick starts, cheat sheets, infographics, and more for Microsoft 365.

Defender for Office 365

One of the key features of Defender for Office 365 is the Attack simulation training, which allows you to run realistic attack scenarios in your organization and identify vulnerable users. By using Attack simulation training, you can educate your users on how to recognize and report phishing, malware, and ransomware attacks, and improve their security awareness and behavior.

Get started with [Microsoft Learn](#)



Basic cyber hygiene practices and cybersecurity training (2)

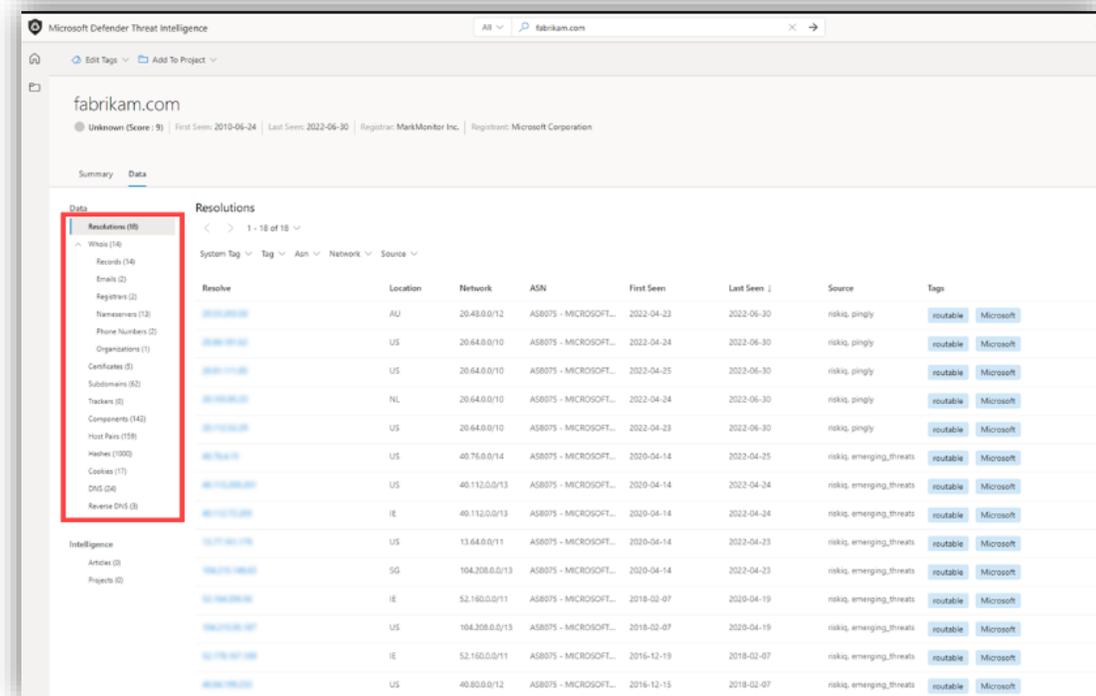
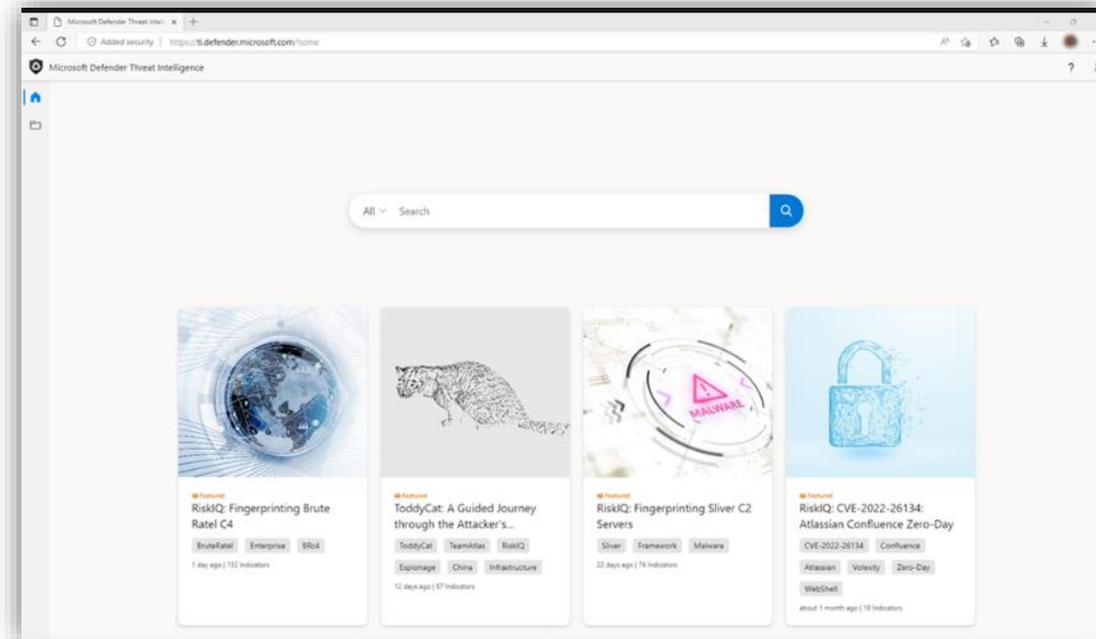
Cybersecurity training is the process of educating yourself and others about the risks and best practices of cyber hygiene. Training can help you develop the skills and knowledge to protect yourself and your organization from cyber threats.



Your cybersecurity weather forecast Defender Threat Intelligence

Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence. Analysts spend a significant amount of time on data discovery, collection, and parsing, instead of focusing on what actually helps their organization defend themselves-- deriving insights about the actors through analysis and correlation.

Get started with [Defender TI](#)



Policies and procedures regarding the use of cryptography and, where appropriate, encryption

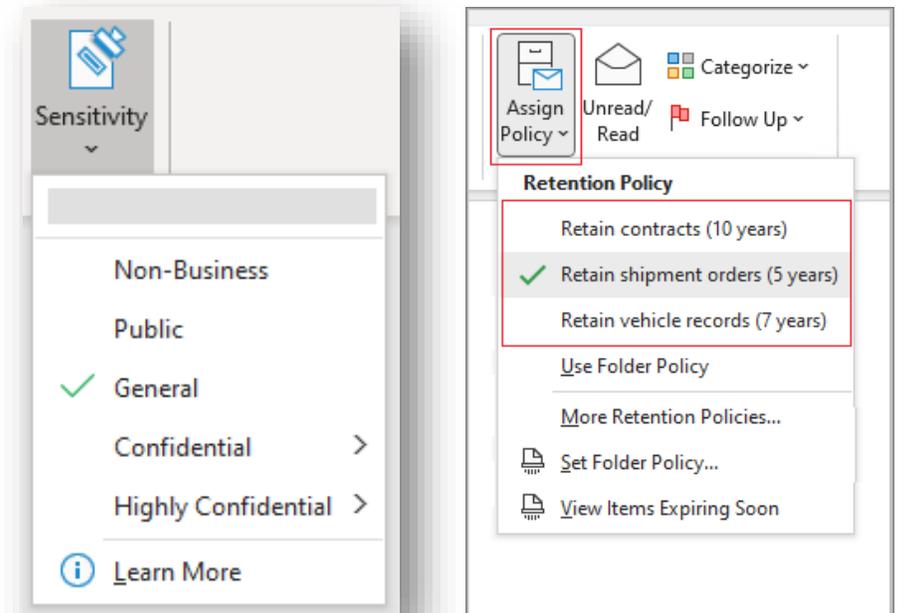
Encryption is an important part of your file protection and information protection strategy. Encryption by itself doesn't prevent content interception. Encryption is part of a larger information protection strategy for your organization. By using encryption, you help ensure that only authorized parties can use the encrypted data.

» Purview Information Protection Sensitivity Labels

Microsoft Purview Information Protection to help you discover, classify, and protect with the use of encryption the sensitive information wherever it lives or travels. Sensitivity labels let you classify and protect your organization's data in-rest and in-motion, while making sure that user productivity and their ability to collaborate isn't hindered.

» Data Lifecycle Management

Microsoft Purview Data Lifecycle Management provides you with tools and capabilities to retain the content that you need to keep and delete the content that you don't. Retaining and deleting content is often needed for compliance and regulatory requirement, but deleting content that no longer has business value also helps you manage risk and liability



Policies and procedures regarding the use of cryptography and, where appropriate, encryption

Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

Remove encryption if the file is encrypted

Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

Users and groups	Permissions
No data available	

Use Double Key Encryption ⓘ

Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

Remove encryption if the file is encrypted

Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

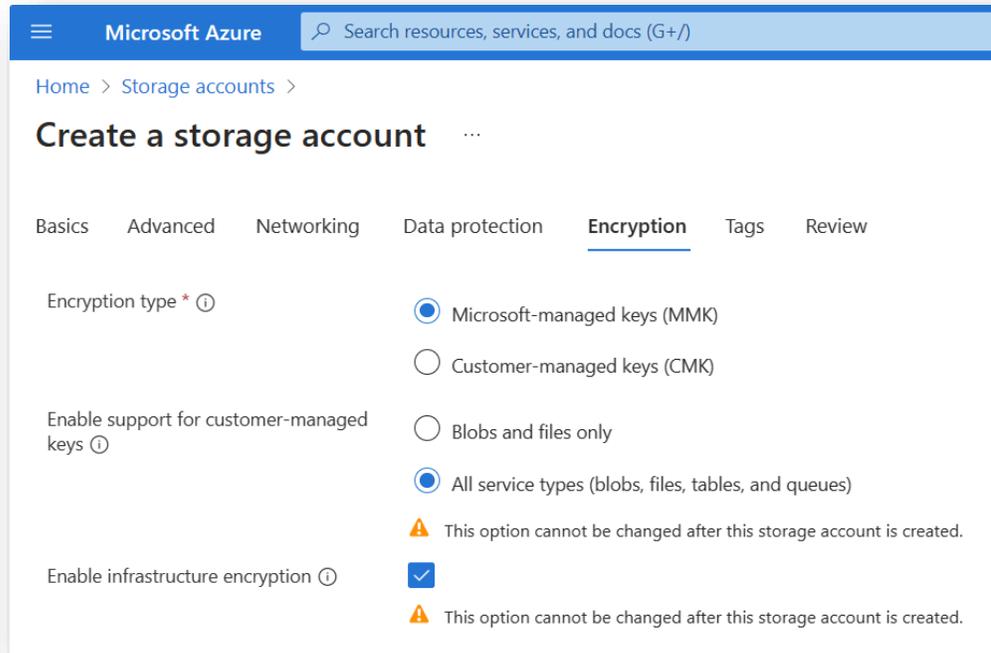
Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

Users and groups	Permissions
No data available	

Use Double Key Encryption ⓘ

Policies and procedures regarding the use of cryptography and, where appropriate, encryption



The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal. The 'Encryption' tab is selected, showing options for encryption type and infrastructure encryption. The 'Microsoft-managed keys (MMK)' option is selected, and 'All service types (blobs, files, tables, and queues)' is chosen. Both options have a warning icon indicating they cannot be changed after creation.

Microsoft Azure Search resources, services, and docs (G+)

Home > Storage accounts >

Create a storage account

Basics Advanced Networking Data protection **Encryption** Tags Review

Encryption type * ⓘ

Microsoft-managed keys (MMK)

Customer-managed keys (CMK)

Enable support for customer-managed keys ⓘ

Blobs and files only

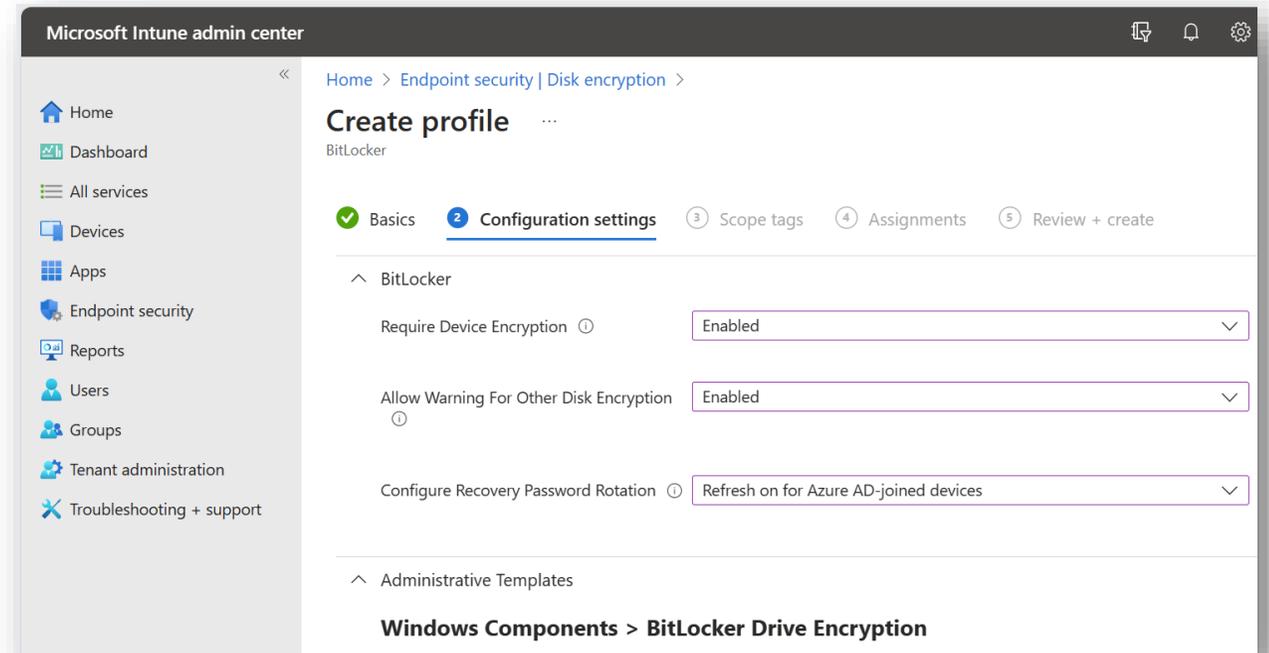
All service types (blobs, files, tables, and queues)

⚠ This option cannot be changed after this storage account is created.

Enable infrastructure encryption ⓘ

⚠ This option cannot be changed after this storage account is created.

ENCRYPTION SETTINGS IN A MICROSOFT AZURE STORAGE ACCOUNT



The screenshot shows the 'Create profile' page in the Microsoft Intune admin center, specifically for BitLocker. The 'Configuration settings' tab is selected, showing three settings: 'Require Device Encryption' (Enabled), 'Allow Warning For Other Disk Encryption' (Enabled), and 'Configure Recovery Password Rotation' (Refresh on for Azure AD-joined devices).

Microsoft Intune admin center

Home > Endpoint security | Disk encryption >

Create profile

BitLocker

Basics **2 Configuration settings** 3 Scope tags 4 Assignments 5 Review + create

BitLocker

Require Device Encryption ⓘ Enabled

Allow Warning For Other Disk Encryption ⓘ Enabled

Configure Recovery Password Rotation ⓘ Refresh on for Azure AD-joined devices

Administrative Templates

Windows Components > BitLocker Drive Encryption

ENFORCING HARDDISK DRIVE ENCRYPTION THROUGH DEVICE POLICIES

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

Create Azure Key Vault Managed HSM

Basics Administrators Networking Tags Review + create

Azure Key Vault Managed HSM provides single-tenant, zone-resilient (where available), highly available HSMs to store and manage your cryptographic keys. Most suitable for applications and usage scenarios that handle high value keys. Also helps to meet most stringent security, compliance, and regulatory requirements. Managed HSM uses FIPS 140-2 Level 3 validated HSMs. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ NORTHWINDT10-2023 Demo Subscription
Resource group * ⓘ RG-Security
[Create new](#)

MICROSOFT AZURE KEY VAULT FOR MANAGED HSM

test-serv-key-rotate | Transparent data encryption

SQL server

Search (Ctrl+/) Save Discard Feedback

Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption
- Identity
- Auditing

Intelligent Performance

- Automatic tuning
- Recommendations

Transparent data encryption encrypts your databases, backups, and logs at rest without any client-side encryption, go to each database. [Learn more](#)

Transparent data encryption ⓘ Service-managed key Customer-managed key

Key selection method Select a key Enter a key identifier

Key * [new-key/](#)
[Change key](#)

Make this key the default TDE protector

Auto-rotate key ⓘ

DATA ENCRYPTION AT REST

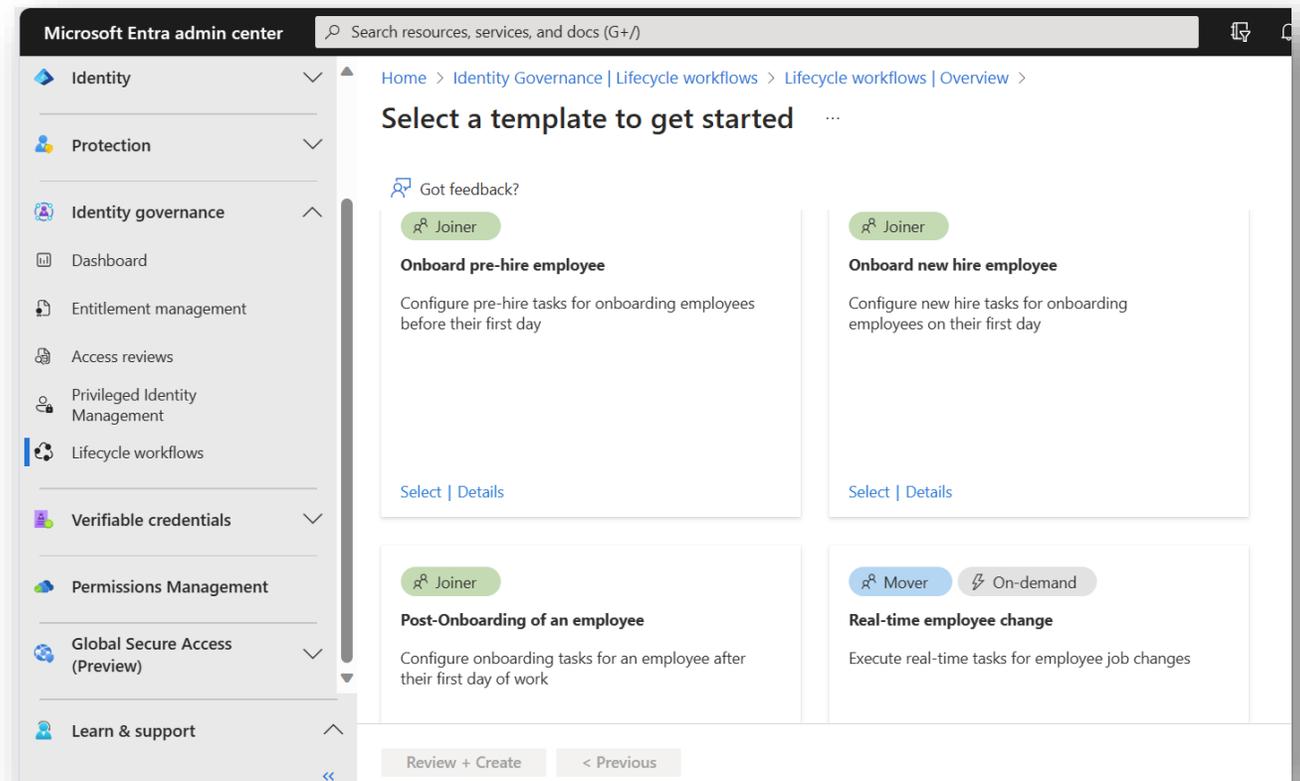
Human resources security, access control policies and asset management (1)

Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.

Microsoft Entra Lifecycle Management

Entra lifecycle management is a feature of Microsoft Entra ID Governance that helps you manage users by automating their joiner, mover, and leaver processes. You can create and manage workflows that consist of tasks and execution conditions to perform actions on users based on their attributes, group memberships, or status changes.

Lifecycle workflows can even integrate with the ability of Microsoft logic apps tasks to extend workflows for more complex scenarios that require integration with existing systems and procedures.

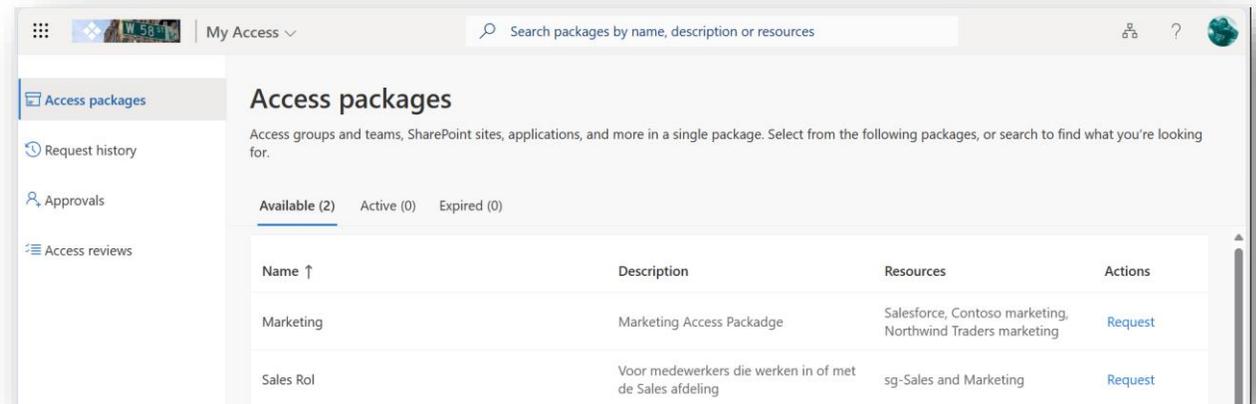
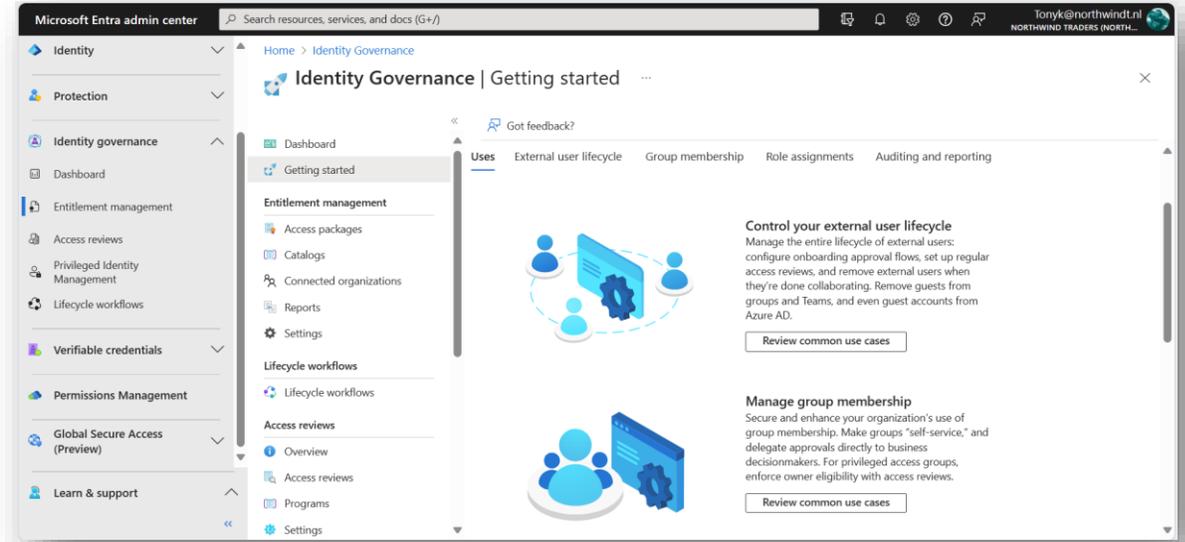


Human resources security, access control policies and asset management (2)

With the new Entra ID (Azure Active Directory) Governance features organizations have more control over standard procedures as well as timed access reviews.

Microsoft Entra Entitlement Management

Also a feature of the Microsoft Entra ID Governance, Microsoft Entra Entitlement Management is a feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration. It can help you more efficiently manage access to groups, applications, and SharePoint Online sites for internal users, and also for users outside your organization who need access to those resources. It also provides comprehensive visibility and control over permissions for any identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP).



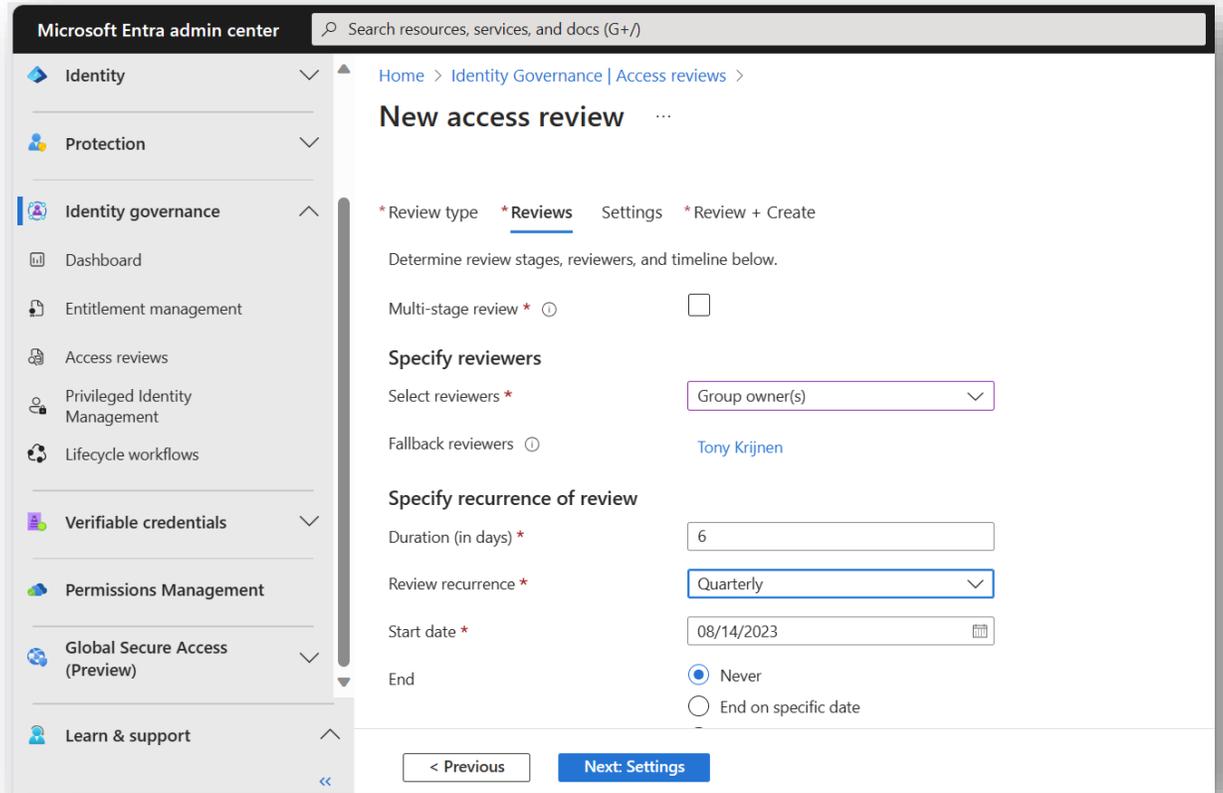
What is Microsoft Entra [entitlement manager](#)?

Human resources security, access control policies and asset management (2)

With the new Entra ID (Azure Active Directory) Governance features organizations have more control over standard procedures as well as timed access reviews.

Microsoft Entra Access Reviews

Also a feature of the Microsoft Entra ID Governance, Microsoft Entra access reviews helps you manage the access to your resources, such as groups and applications, by reviewing them regularly. You can create and perform access reviews for users or guests, and ask them or a decision maker to confirm or revoke their access based on their needs. You can also use access reviews to comply with policies, audit requirements, or security best practices.



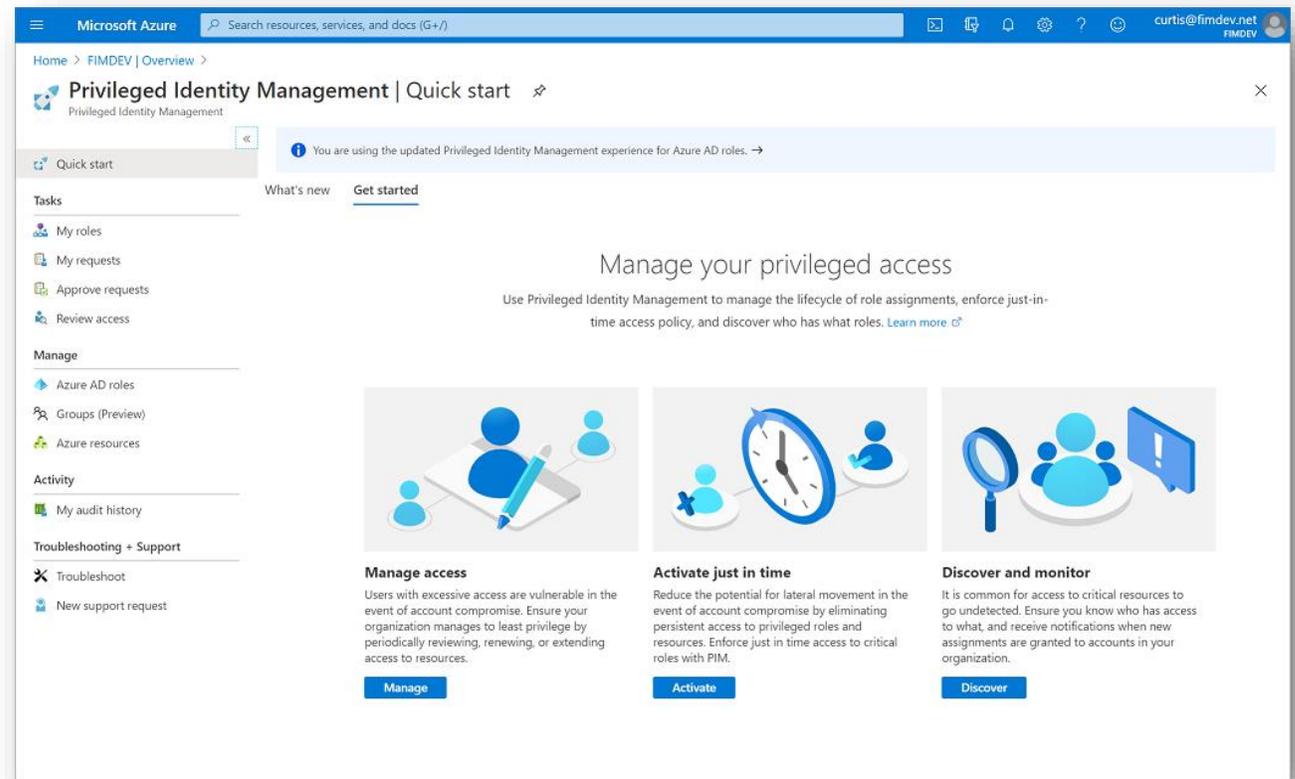
The screenshot shows the Microsoft Entra admin center interface for creating a new access review. The left sidebar contains navigation options: Identity, Protection, Identity governance (selected), Dashboard, Entitlement management, Access reviews, Privileged Identity Management, Lifecycle workflows, Verifiable credentials, Permissions Management, Global Secure Access (Preview), and Learn & support. The main content area is titled 'New access review' and includes a search bar at the top. Below the title, there are tabs for 'Review type', 'Reviews' (selected), 'Settings', and 'Review + Create'. The page instructs the user to 'Determine review stages, reviewers, and timeline below.' The configuration options include: 'Multi-stage review' (checkbox), 'Specify reviewers' (with a dropdown for 'Group owner(s)' and a link for 'Tony Krijnen' as a fallback reviewer), 'Specify recurrence of review' (with fields for 'Duration (in days)' set to 6, 'Review recurrence' set to 'Quarterly', and 'Start date' set to '08/14/2023'), and 'End' options (radio buttons for 'Never' and 'End on specific date'). At the bottom, there are buttons for '< Previous' and 'Next: Settings'.

Human resources security, access control policies and asset management

Microsoft Conditional access and Microsoft Privileged Identity Management help organizations to limit access to administrative roles until that access is needed and only when conditions are met.

Privileged Identity Management

Privileged Identity Management (PIM) is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization (Microsoft Entra ID, Azure, Microsoft 365 and other Microsoft Online Services). It provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.



The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity



Explanation

The modern security perimeter extends beyond an organization's network perimeter to include user and device identity. Organizations now use identity-driven signals as part of their access control decisions.



Zero Trust Mapping

Zero Trust requires that every transaction between systems (user identity, device, network, and applications) be validated and proven trustworthy before the transaction can occur.



Conditional Access

Azure AD Conditional Access brings signals together, to make decisions, and enforce organizational policies. Conditional Access is Microsoft's Zero Trust policy engine taking signals from various sources into account when enforcing policy decisions. This feature helps organizations to align their identities with the three guiding principles of a Zero Trust architecture: verify explicitly, use least privilege and assume breach.

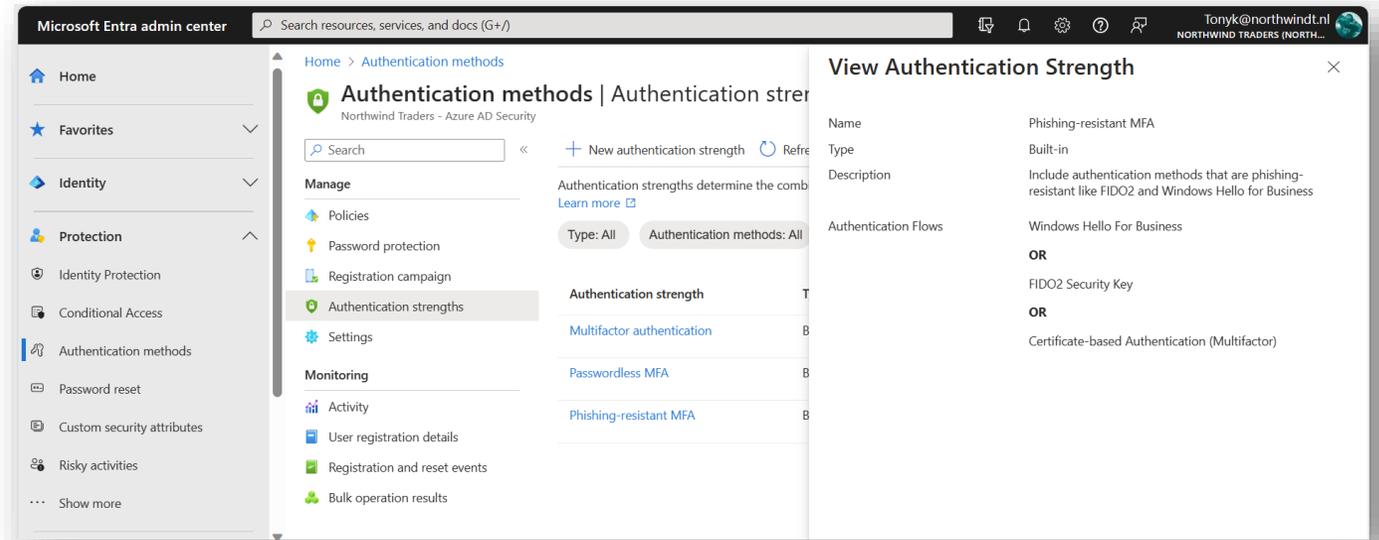


Risk based Conditional Access

Most users have a normal behavior that can be tracked, when they fall outside of this norm it could be risky to allow them to just sign in. You may want to block that user or maybe just ask them to perform multifactor authentication to prove that they're really who they say they are. A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.

The use of multi-factor authentication or continuous authentication solutions

Token interception through an Adversary-in-the-middle attacks is the most common way to bypass MFA and allow attacks to leverage a token replay to gain full access. Microsoft Entra Authentication Strengths can help to mitigate these attacks.

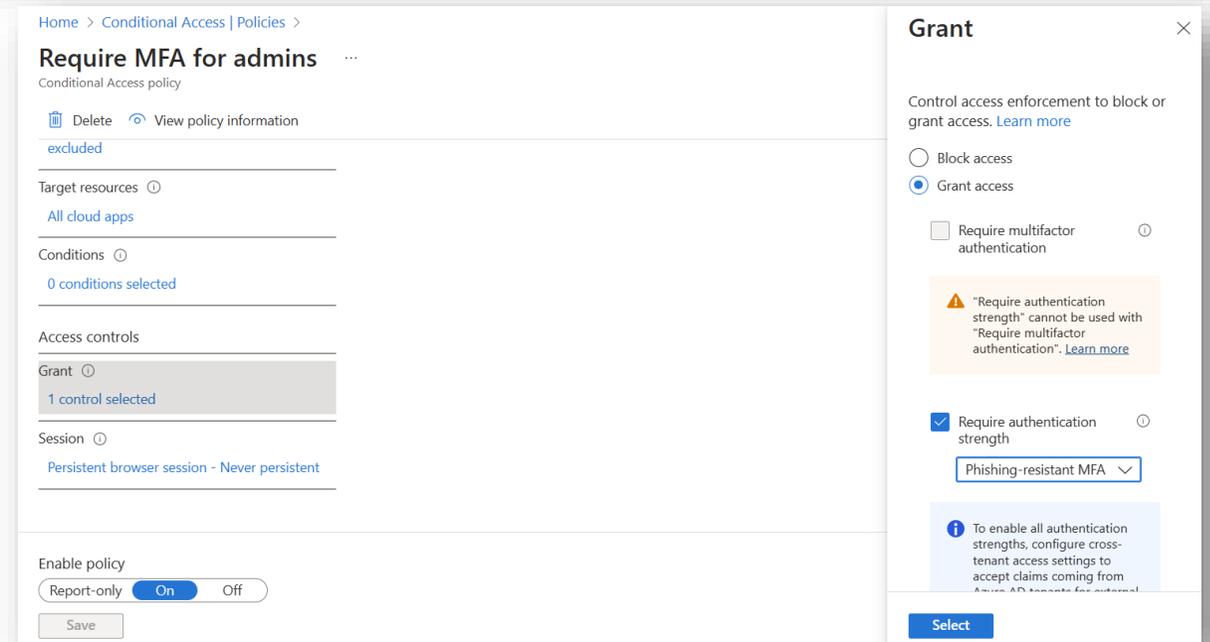


Microsoft Entra Authentication Strengths

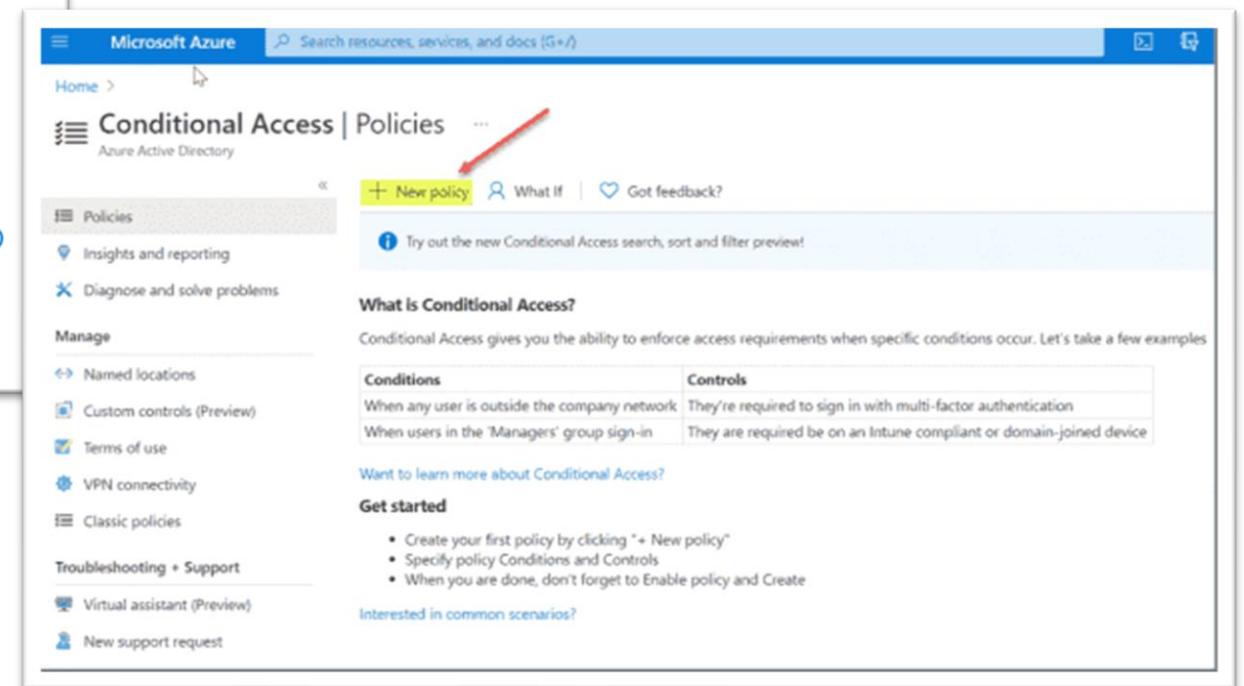
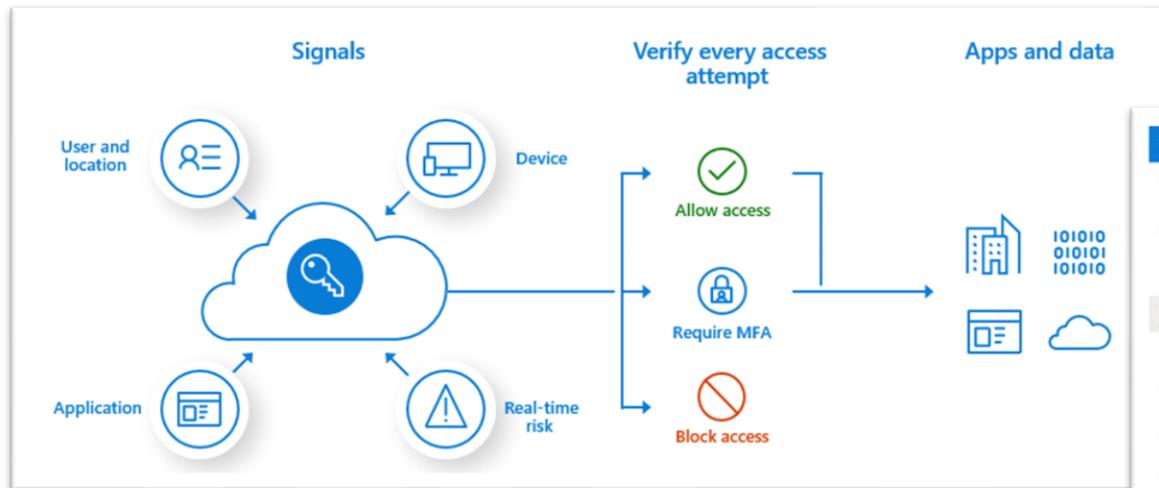
The new Entra Authentication Strengths (a feature of Microsoft Entra ID) allows you to specify which combination of authentication methods can be used to access a resource. For example, you can require phishing-resistant methods (FIDO2 keys, Windows Hello, Smartcards for sensitive resources.

Enforce Authentication Strengths through CA

You can use authentication strengths in conditional access policies to define a minimum level of authentication strength required for access, based on factors such as the user's sign-in risk level, the sensitivity of the resource being accessed, the user's location, and more



The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity



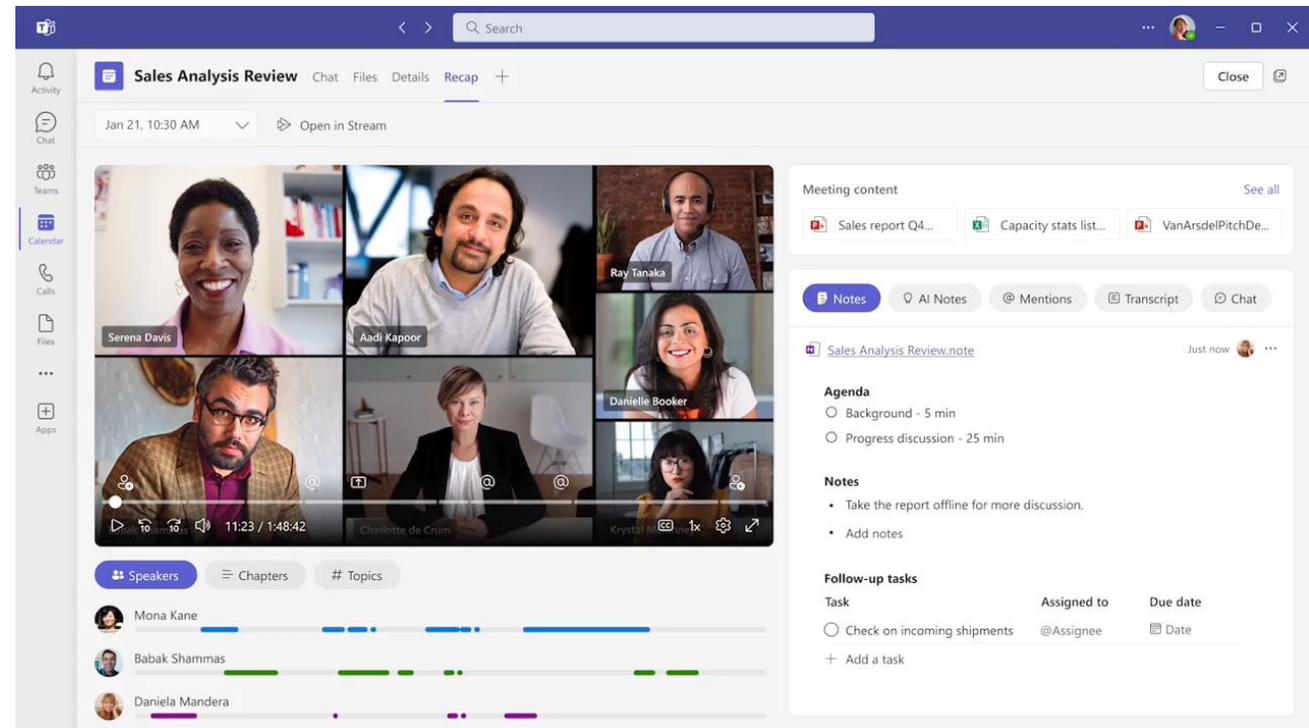
Get started with [Conditional Access](#)

The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity



Teams Premium

Microsoft Teams Premium is an enhanced version of the popular collaboration platform, Microsoft Teams. It offers advanced communication tools, improved security, seamless integration with Microsoft 365 apps, increased storage, and priority support. Customers should use it for boosted productivity, enhanced security, and tailored collaboration solutions to fit their specific needs.





Thank you



[Ellen van Meurs](#)
[Ronald Schouten](#)
[Tony Krijnen](#)