NIS2: Bezpečnostní minimum

Petr Vlk
Microsoft MVP
Enterprise Architect
KPCS CZ
vlk@kpcs.cz

Kybernetická odolnost versus soulad

Bezpečnost je jen jedna

- Ve standardech a regulačních rámcích jde vždy u kybernetické bezpečnosti o stejné motivy a cíle:
  - Vybudovat funkční, efektivní a udržitelnou (=přiměřenou) obranu
  - Ekonomicky zvládnout (=financovat) asymetrickou situaci
    - útočník vs. obránce
  - Najít a vyškolit obránce

Sun Tzu

- Obecné principy bezpečnosti a obrany jsou tisíce let staré:
  - Poznej sám sebe
  - O čem nevím, to mohu těžko ubránit
  - Znám své slabiny = znám i možnou taktiku a cíle útočníka
- Poznej své nepřátele
  - Dívám se očima útočníka (hackera)
- Vytvoř strategii, taktiku a operativní plán obrany
  - Vím, co budu dělat
- Aplikuj jasné velení a vedení mezi obránci
  - Jedna vůle, jasné pokyny
  - Rozděl a panuj
  - Podám pomocnou ruku

Principy kybernetické bezpečnosti v regulaci a legislativě

- Ve standardech a legislativě pro kybernetickou bezpečnost se uplatňují následující principy:
  - Vyvážená linie obrany – rozvíjím více oblastí (domén) kybernetické bezpečnosti
    - systém, procesy a obránci
    - aktiva a rizika
    - přístupy a ověření
    - prevence-detekce-reakce-zotavení
    - stanice-servery-sítě-identity-data
- Prioritizace – dělej správné věci, „first things first“
  - prioritní aktiva
  - prioritní hrozby a zranitelnosti
  - prioritní rizika
  - prioritizace opatření
- Neustálé zlepšování – „cesta je cíl“
  - zvyšování plošného standardu zabezpečení od základní hygieny (Top 20 Critical Security Controls) po propracovanou bezpečnostní strategii (Zero Trust)
  - iterace a cykly, pravidelné revize, vyhodnocení, měření, zpětná vazba (= podněty pro zlepšování)

NIS 2 novelizace a její dopady (1)

- Nová regulace v EU - finální verze publikována v 2. polovině 2022
- V ČR bude implementovaná formou **novelizace VKB** (členské státy mají 21 měsíců na zavedení do legislativy)
- V průběhu r. **2024/5** budou NIS 2 požadavky a pravidla platit na dotčené organizace
- Očekáváme adaptační období 12 měsíců, tj. v průběhu r. **2025** by měly být dotčené organizace v souladu (mít realizovaná opatření)
- pro větší počet organizací (subjektů) než současná NIS - z 350 na **6000**
- cílí na nová odvětví (automotive)
- větší rozsah regulace v existujících odvětvích - cloudové služby, sociální sítě, zdravotnictví (plný rozsah)
- nová procedura identifikace organizace - nově bude kritériem velikost organizace (nad 50 zaměstnanců)
- zvýšení pokut (ala GDPR, 1/2 limitů GDPR) - 2% obratu nebo až 10 milionů EUR

- **NIS2 má stejná témata jako ISO, obsahuje i konkrétní typová opatření (MFA)**

NIS 2 novelizace a její dopady (2)

Opatření zahrnují:

- analýzu **rizik** a **politiku bezpečnosti** informačních systémů
- řešení **incidentů** (prevence, odhalování incidentů a reakce)
- řízení **kontinuity** provozu a krizové řízení
- zabezpečení **dodavatelského řetězce** včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho dodavateli nebo poskytovateli
- zabezpečení pořizování, vývoje a **údržby sítě a informačních systémů,** včetně zveřejňování informací o zranitelnostech a jejich řešení
- politiky a postupy (testování a audit) za účelem **posouzení** účelnosti opatření k **řízení rizik**
- **používání kryptografie a šifrování**
- **personální bezpečnost**
- **politiky řízení přístupů**
- **správu aktiv**
- **použití vícefaktorové autentizace (MFA)**

Kybernetický zákon a vyhláška (1)

- Úzká vazba na ISO
- Definuje terminologii – kybernetická bezpečnostní událost, kybernetický bezpečnostní incident, kybernetická mimořádná událost
- Definuje regulátora a národní kontaktní místa (NÚKIB, CZ NIC, Gov CERT)
- Požaduje nahlášení:
  - Kontaktních osob
  - Významných dodavatelů a poskytovatelů
  - Incidentů
- Požaduje kvalifikované obsazení základních bezpečnostních rolí a manažerských výborů:
  - Garant aktiva
  - Manažer KB
  - Architekt KB
  - Auditor KB
  - Výbor pro řízení KB

- **ZoKB a VKB obsahují současnou NIS řeší stejná témata jako ISO, např.:**
  - **Bezpečnostní cíle a potřeby**
  - **Rozsah ISMS**
  - **Bezpečnostní politiku**
  - **Vyhodnocování a audit**
  - **Aktiva a rizika**
  - **Řízení dodavatelů**
  - **Bezpečnosti lidských zdrojů a jejich osvětu a proškolení**
  - **Použití kryptografie**

Kybernetický zákon a vyhláška (2)

VKB navíc požaduje i obecná typová opatření v oblastech:

- **Identity/AD/AAD**
- **Antimalware/AV/EDR**
- **Konektivita/FW/NGFW**
- **Logy/SIEM/SOC**
- **IRP/CSIRT**
- **bezpečnost v OT (obecná, komplexní)**

What does NIS 2 mean for customers?

Cybersecurity Risk Management Measures

Risk Management	Security Policies	Incident handling (prevention, detection & response to incidents)	Business continuity and crisis management
Supply chain security consider supplier vulnerabilities	Vulnerability handling and disclosures	Regular assessments to determine the effectiveness of cybersecurity risk management measures (e.g., reflection of state of art – security posture)	
The use of cryptography and encryption where warranted	Basic cybersecurity hygiene & training	The use of MFA or continuous authentication	

Incident Reporting Obligations

Report incidents with significant* impact on the provision of services

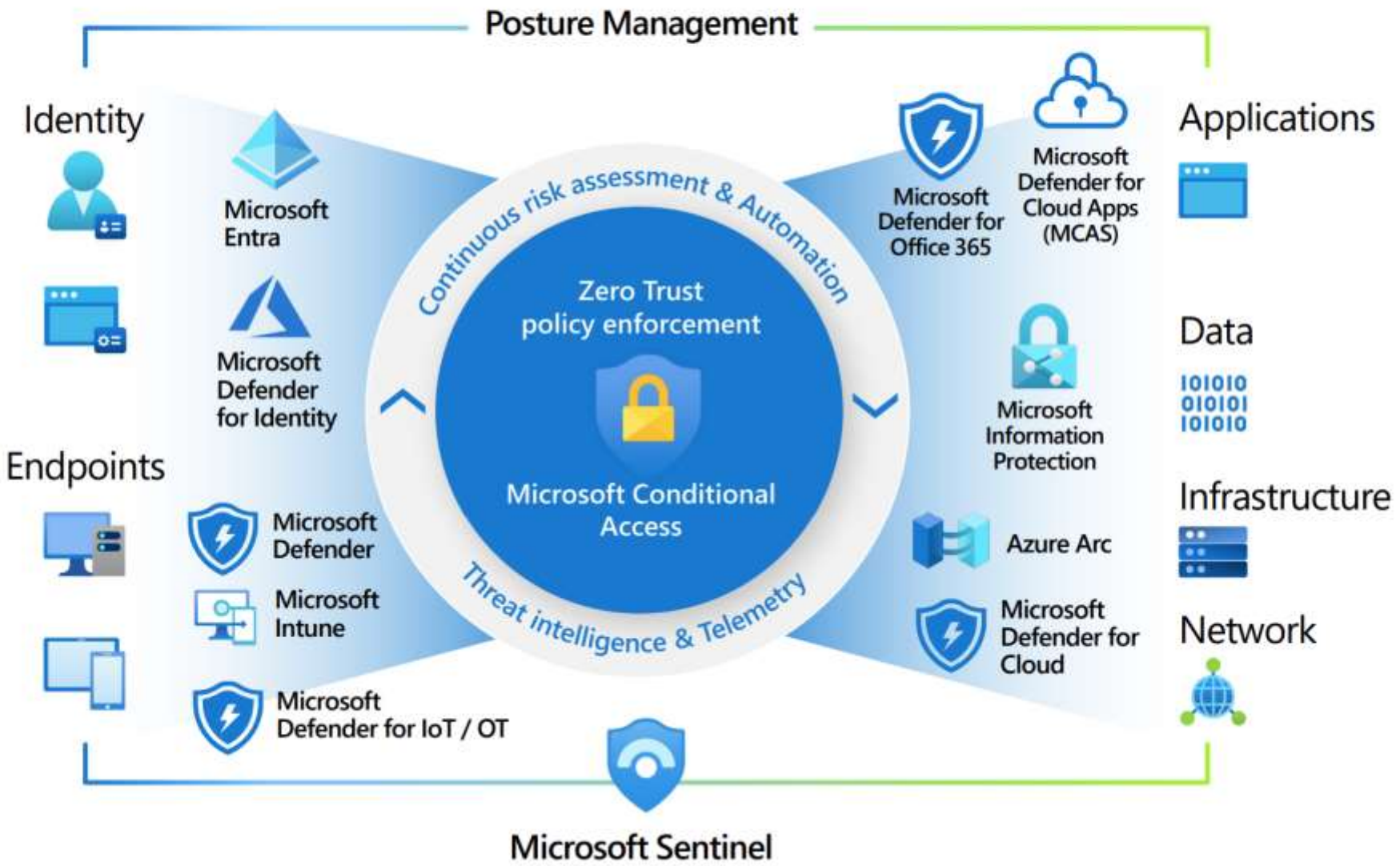
Within 24 hours	Within 72 hours an extensive report	Within 1 month a final report progress report

**=An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage*

Computer Security Incident Response Team (CSIRT)	Competent Authority	Recipients of services

Microsoft Security

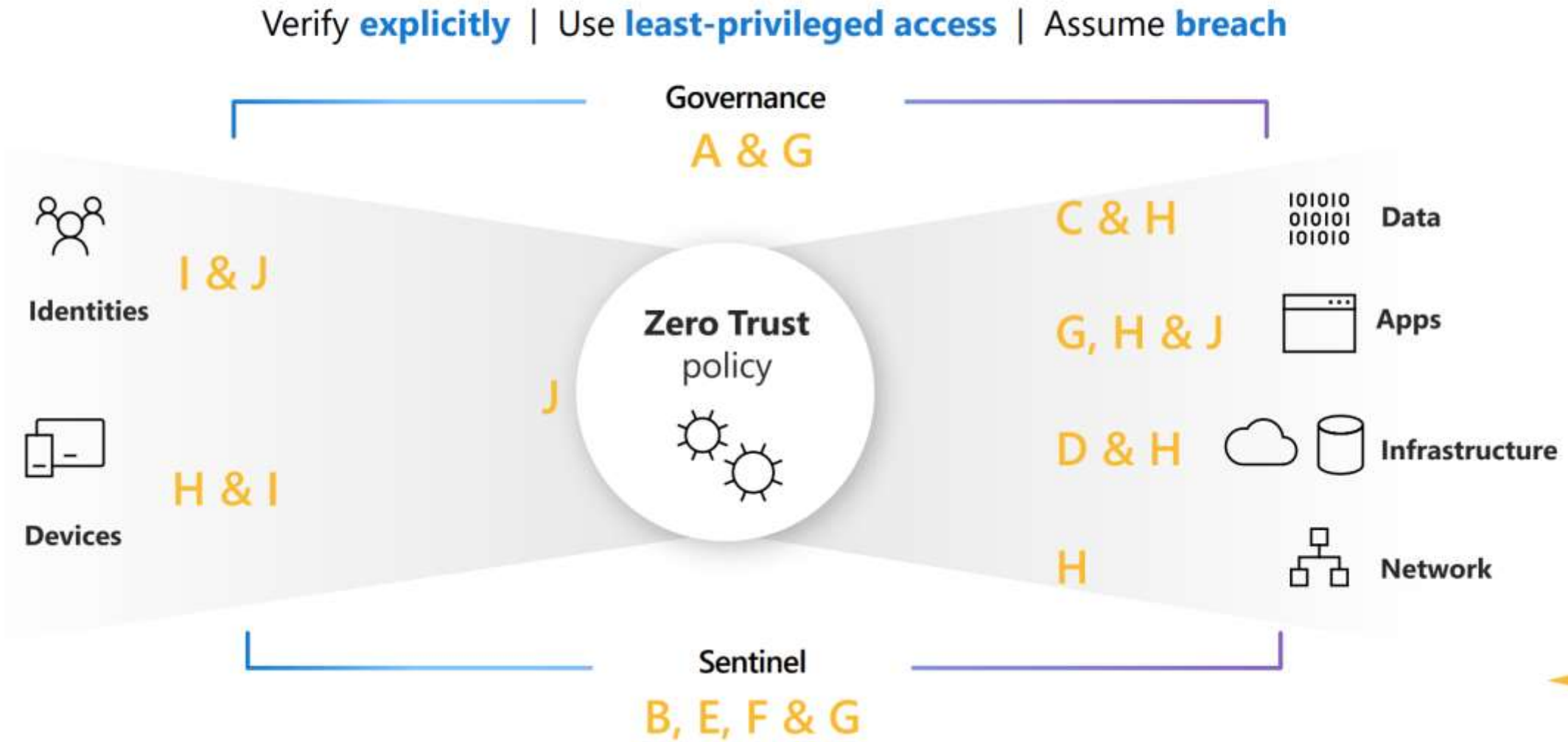
Microsoft Zero Trust Capabilities



NIS 2 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.

Mapping NIS 2.0 Duties to the Microsoft Zero Trust



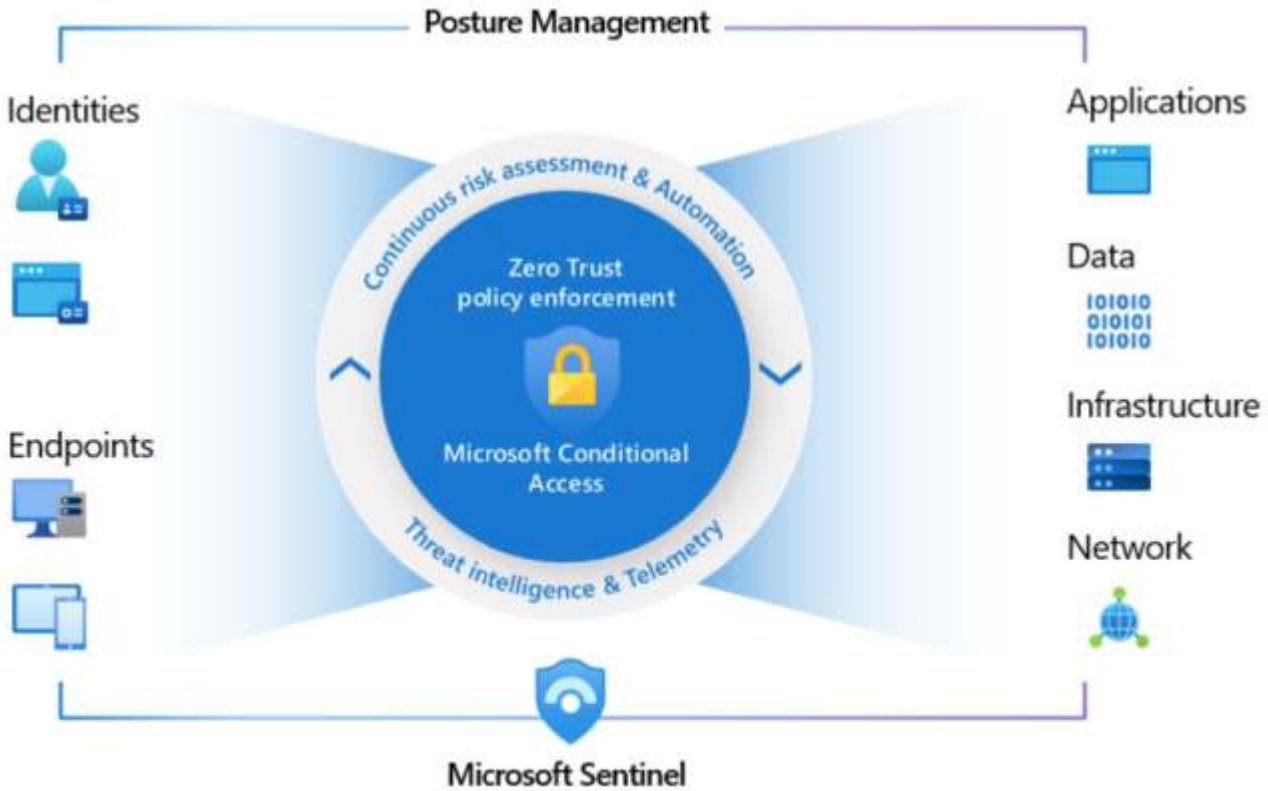
Policies on risk analysis and information system security

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

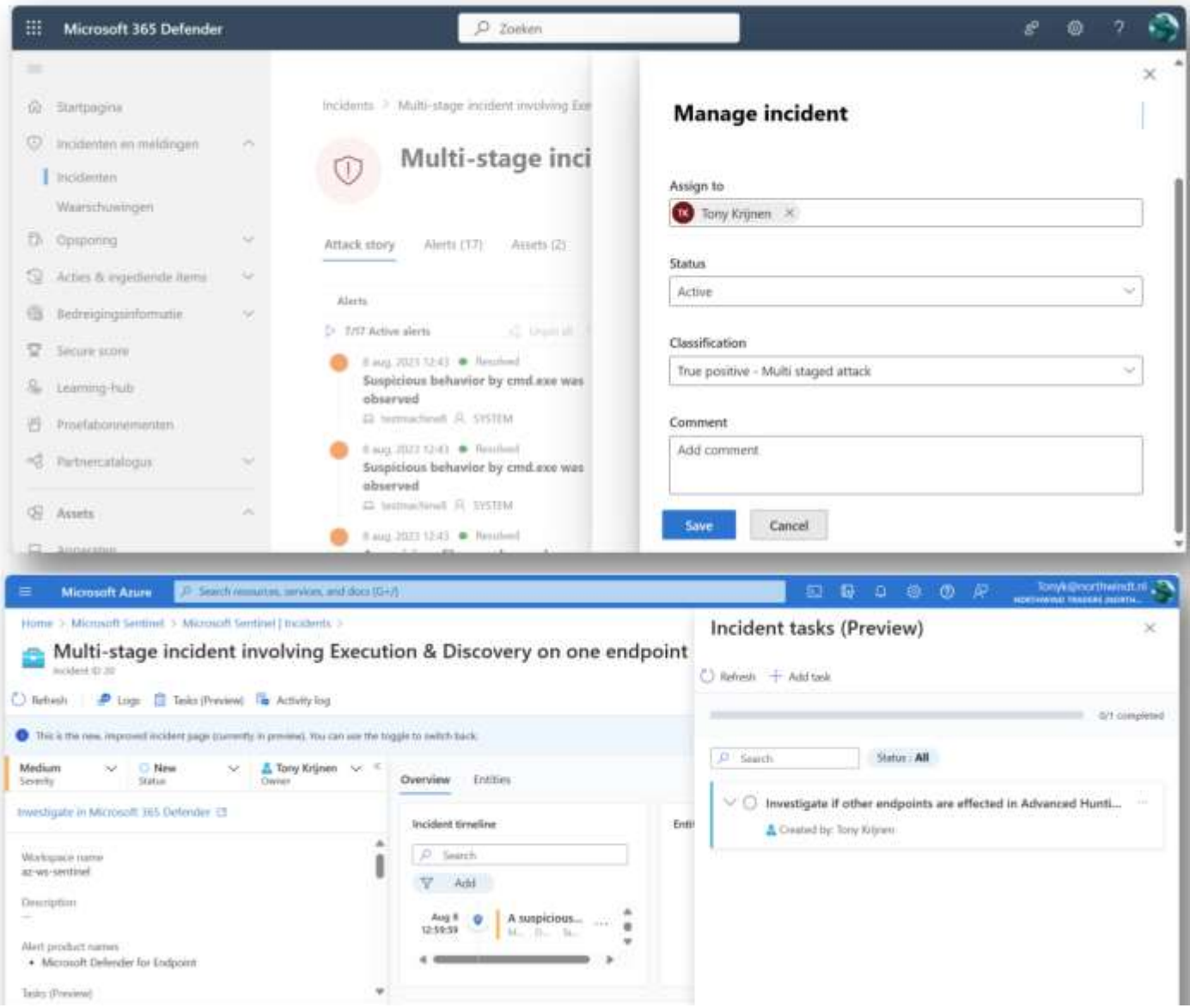
Security incident handling is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. It seeks to give a robust and comprehensive view of any security issues within an IT infrastructure.

Incident handling with Microsoft Defender

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

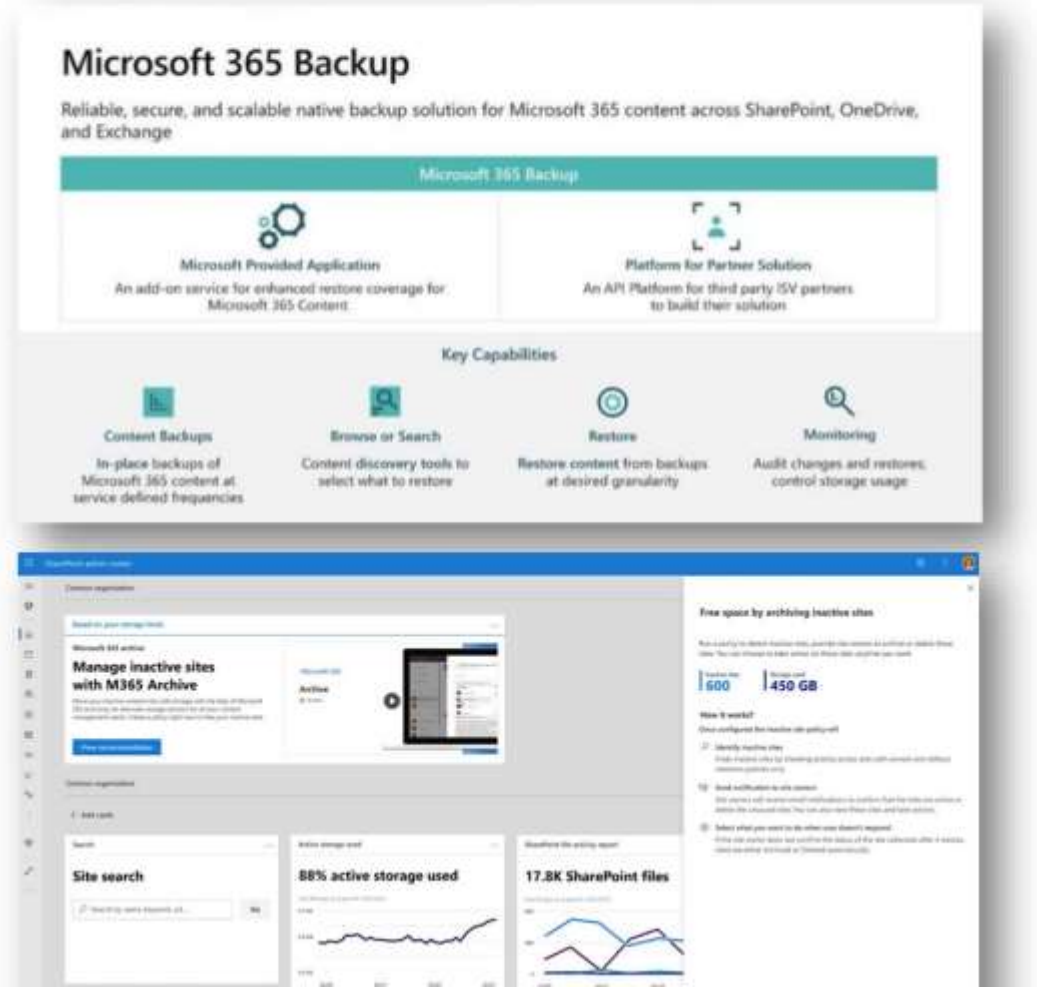
Incident handling with Microsoft Sentinel

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.



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

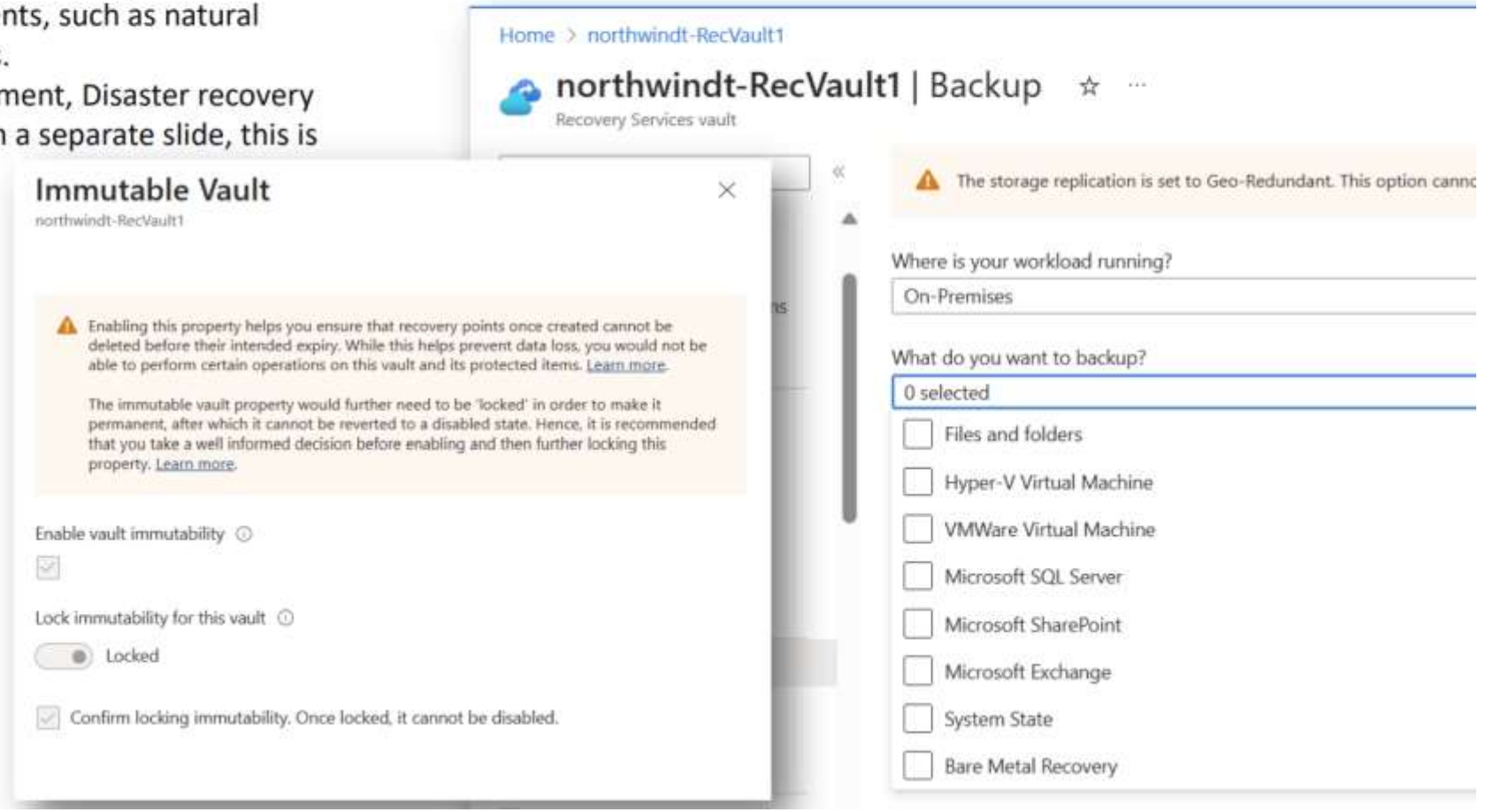
Microsoft 365 Archive gives you a cold data storage tier that enables you to keep inactive or aging data within SharePoint at a cost-effective price point matching the value of that data's lifecycle stage. Because the content is archived in place, it retains Microsoft 365's valuable security, compliance,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

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.

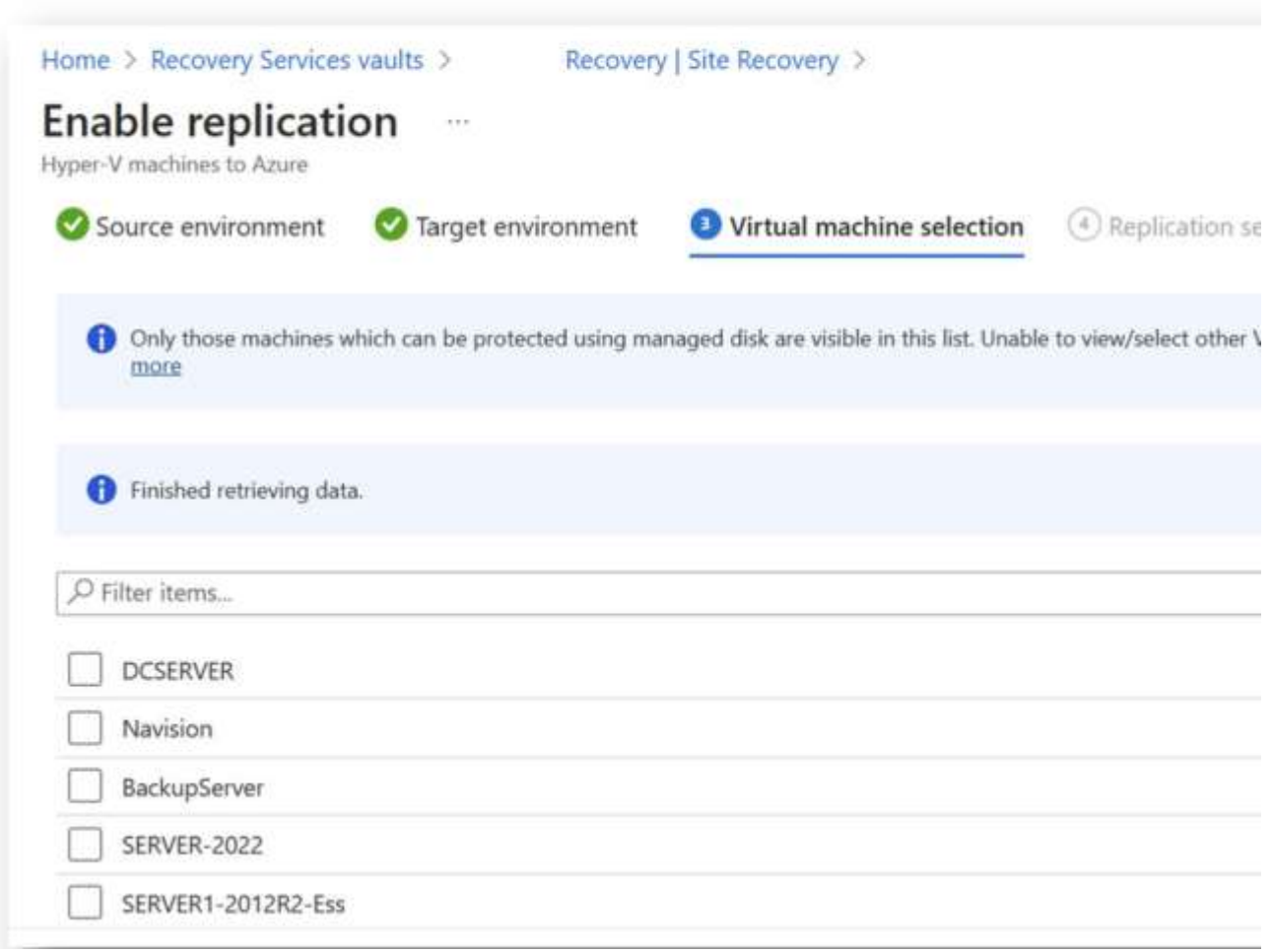


Business continuity – Disaster Recovery

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



Supply chain security

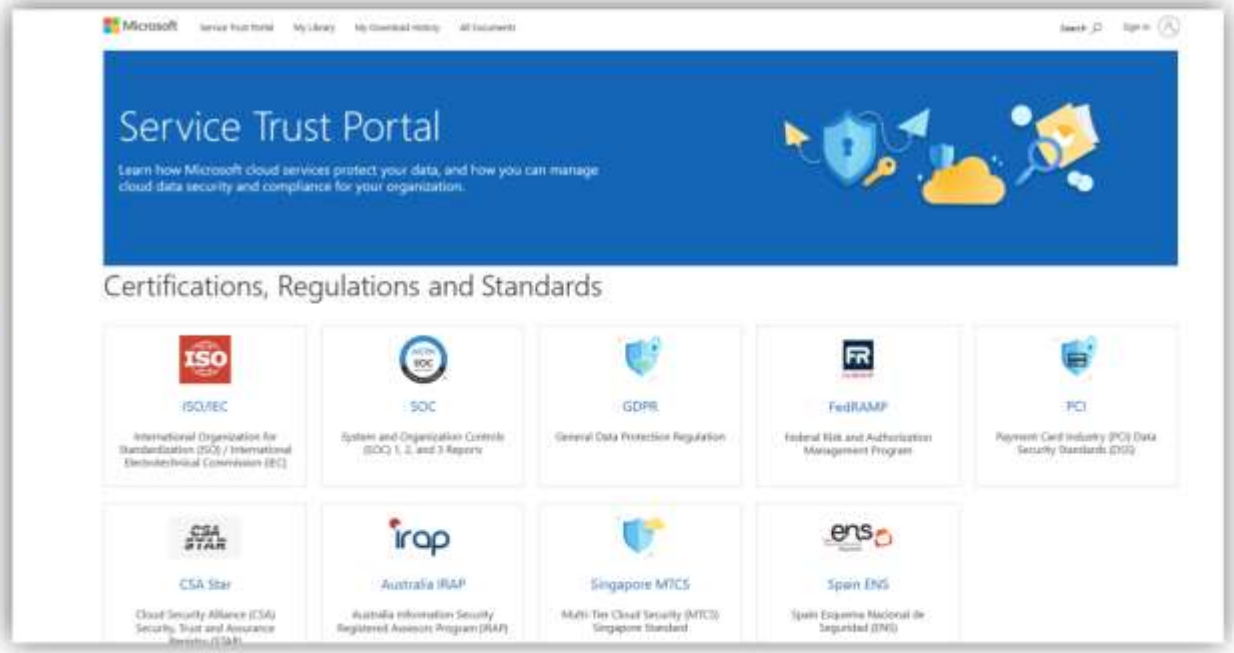
Digital supply chains are becoming more complex, more digital, and more interdependent, which means that any vulnerability or attack in one part of the supply chain can have a ripple effect on the entire chain. One example of this is how Microsoft is showcasing their compliance.

Compliance (3rd party assurance/SOC statement)

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.



E

NIS 2 COMPLIANCE IS A ZERO TRUST JOURNEY

Security in network and information systems acquisition, development and maintenance

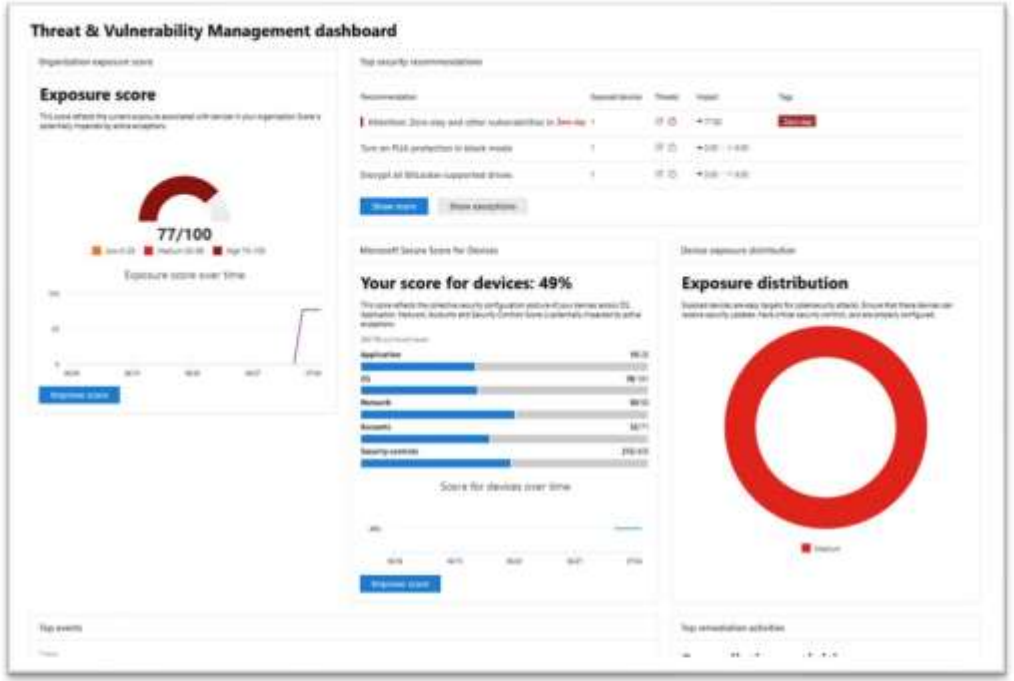
From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.

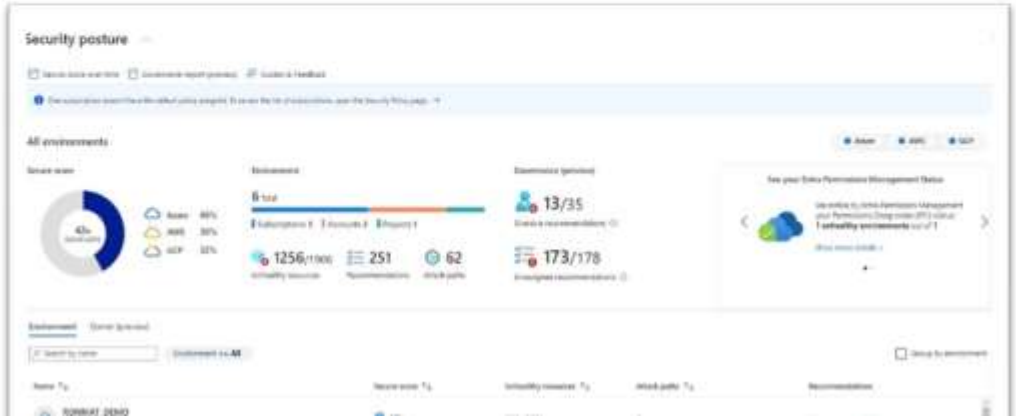
Defender Vulnerability Management

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.



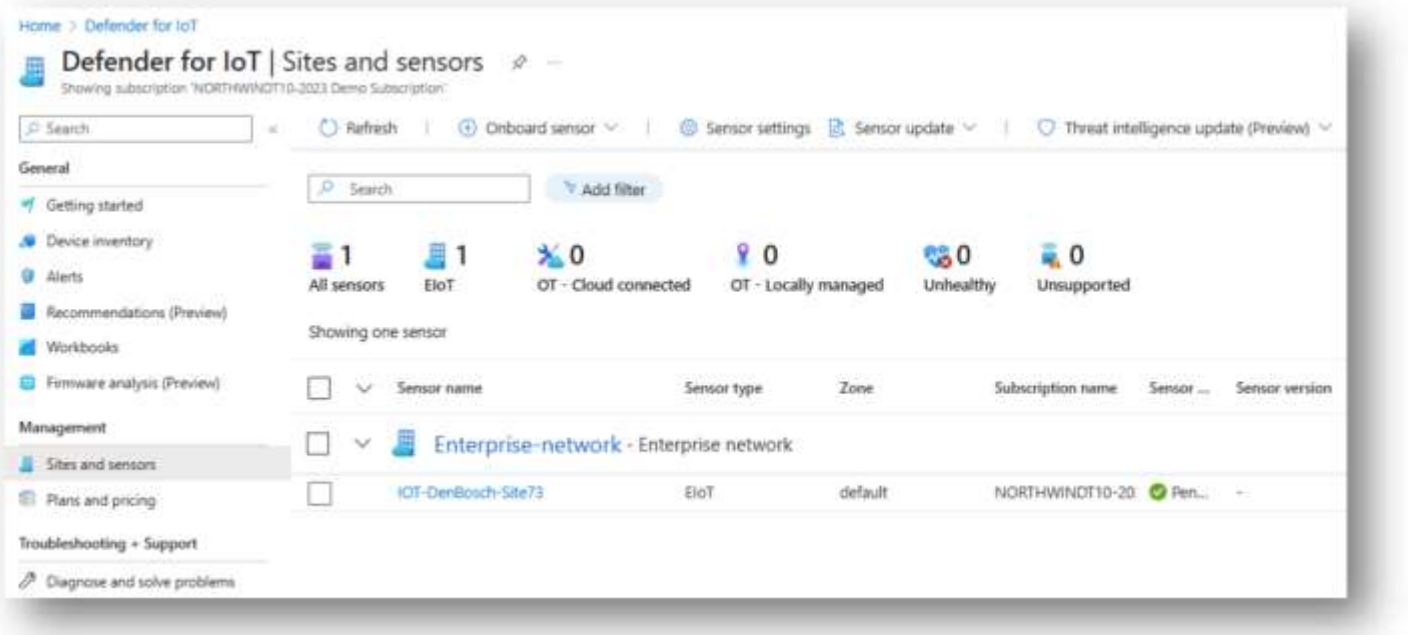


Security in network and information systems acquisition, development and maintenance

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 / OT

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

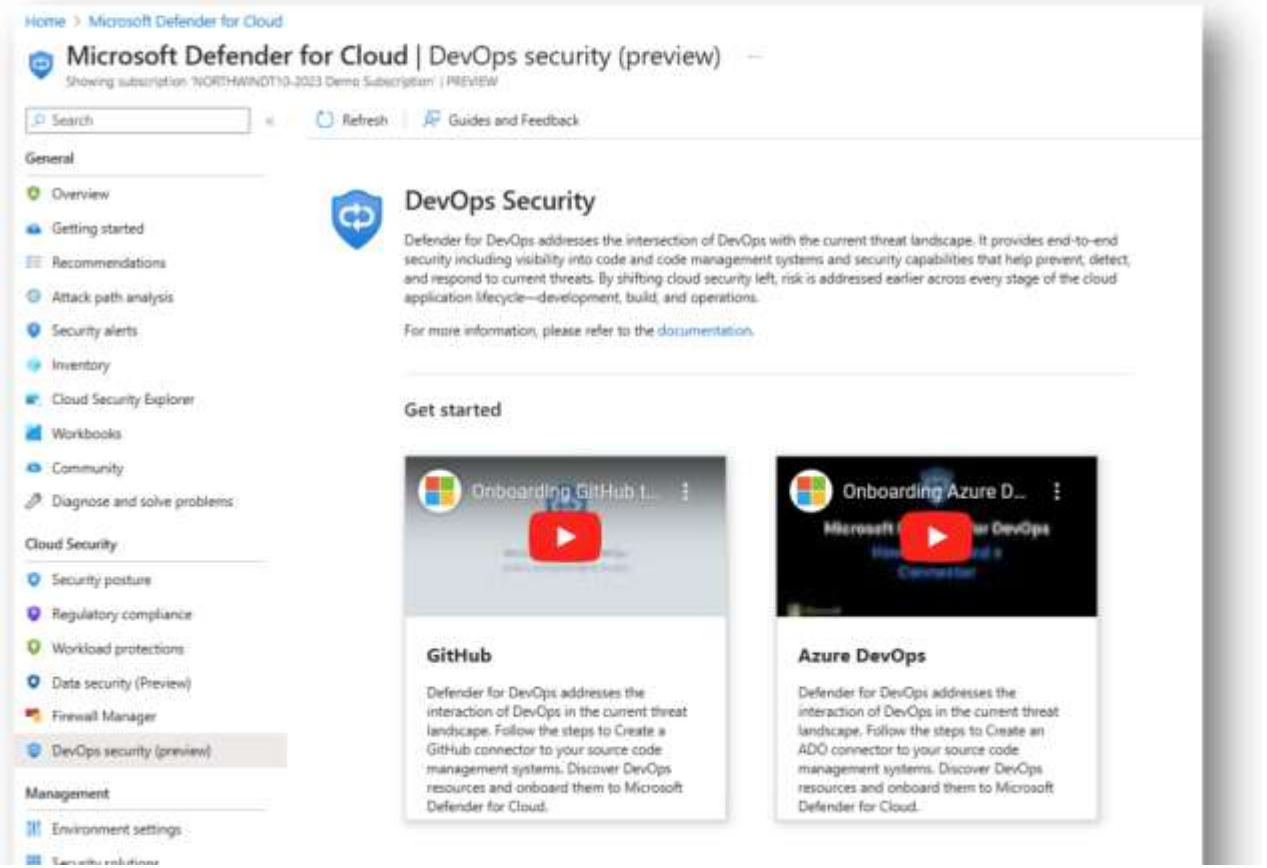


Security in network and information systems acquisition, development and maintenance

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

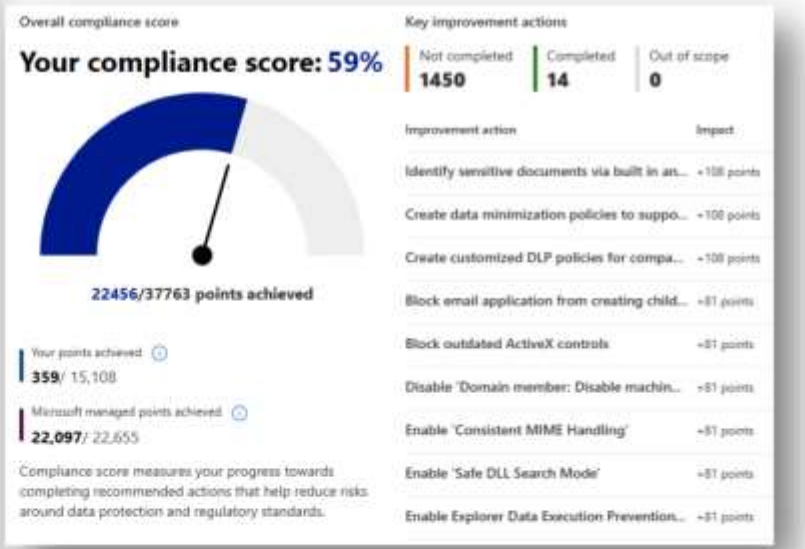
Defender for DevOps uses a central console to empower security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, such as GitHub and Azure DevOps. Findings from Defender for DevOps can then be correlated with other contextual cloud security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



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.

F

NIS 2 COMPLIANCE IS A ZERO TRUST JOURNEY

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

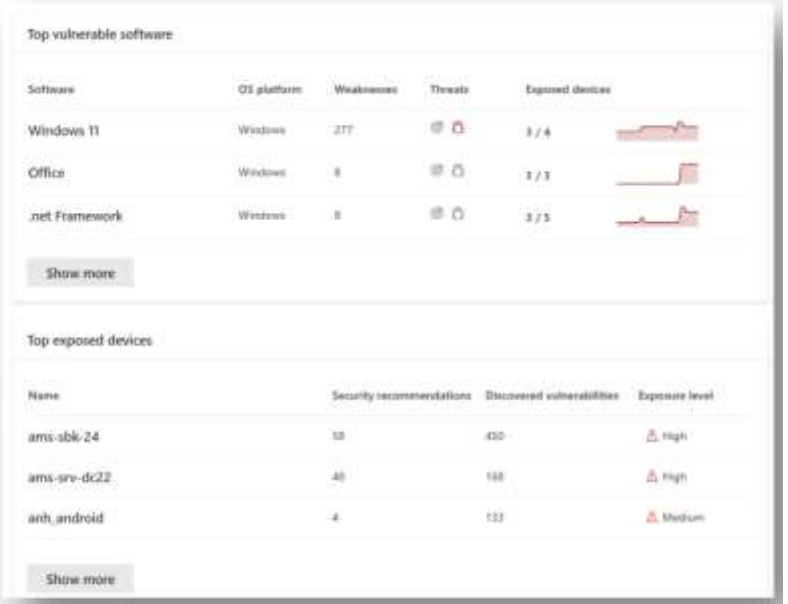
Microsoft Defender exposure score is a metric that reflects how vulnerable your organization is to cybersecurity threats. Your exposure score is influenced by factors such as weaknesses, threats and security alerts on your devices.

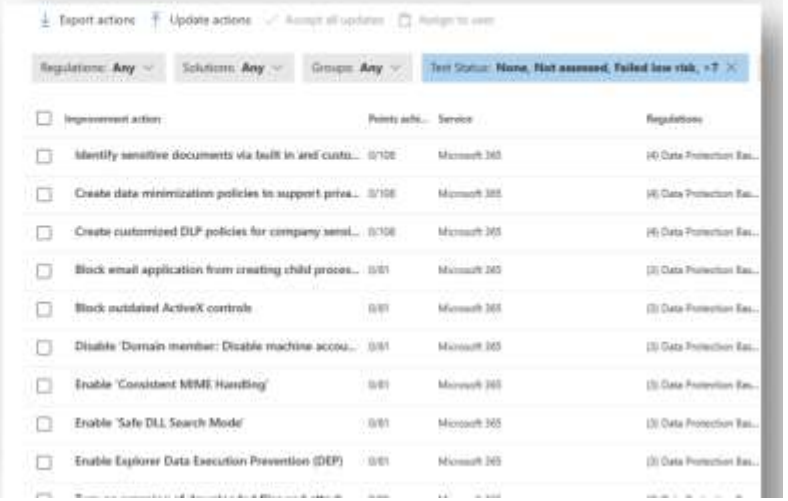
Microsoft Defender for Identity

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.





Basic cyber hygiene practices and cybersecurity training (1)

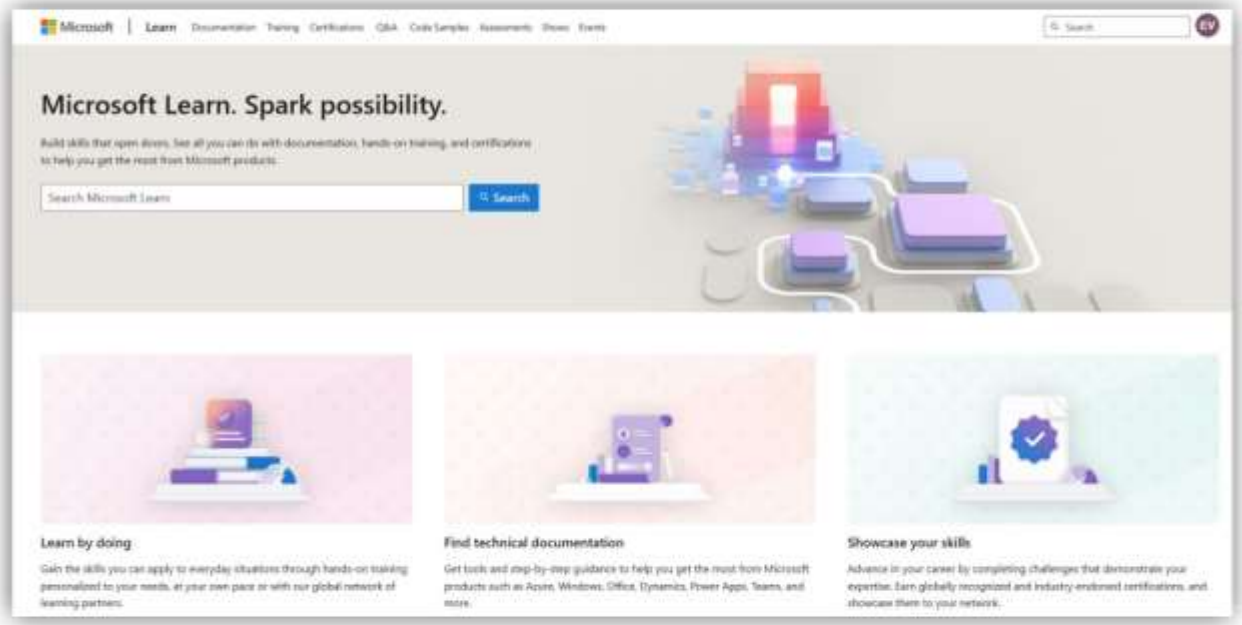
Cybersecurity training is the process of educating yourself and others about the risks and best practices of cyber hygiene. Training can help you develop the skills and knowledge to protect yourself and your organization from cyber threats.

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

On 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.



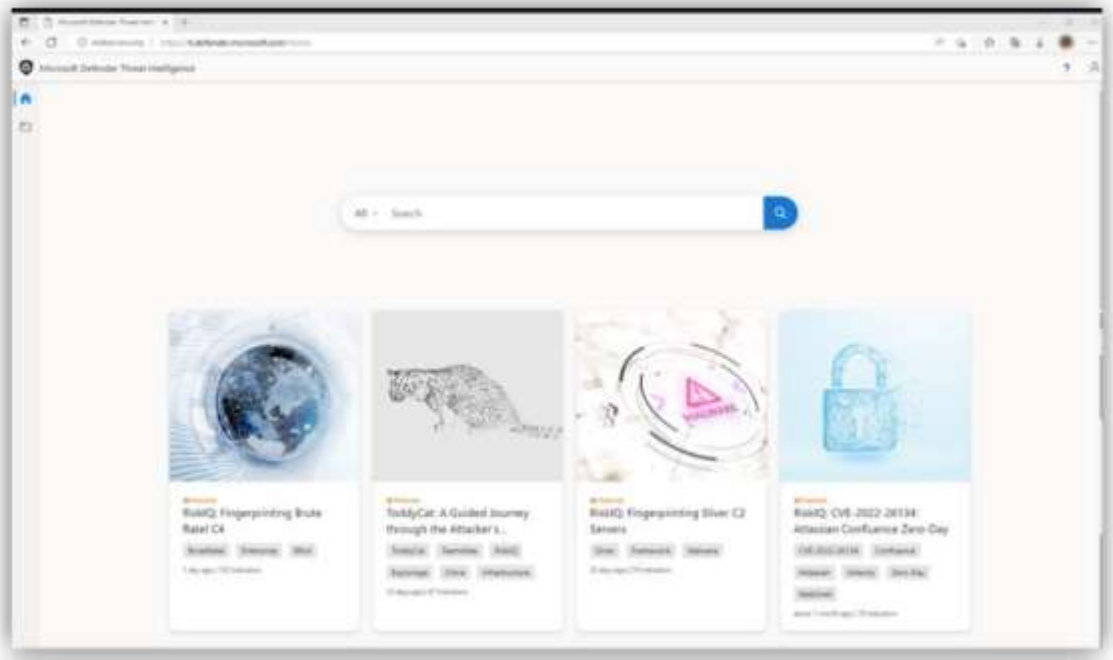
G NIS 2 COMPLIANCE IS A ZERO TRUST JOURNEY

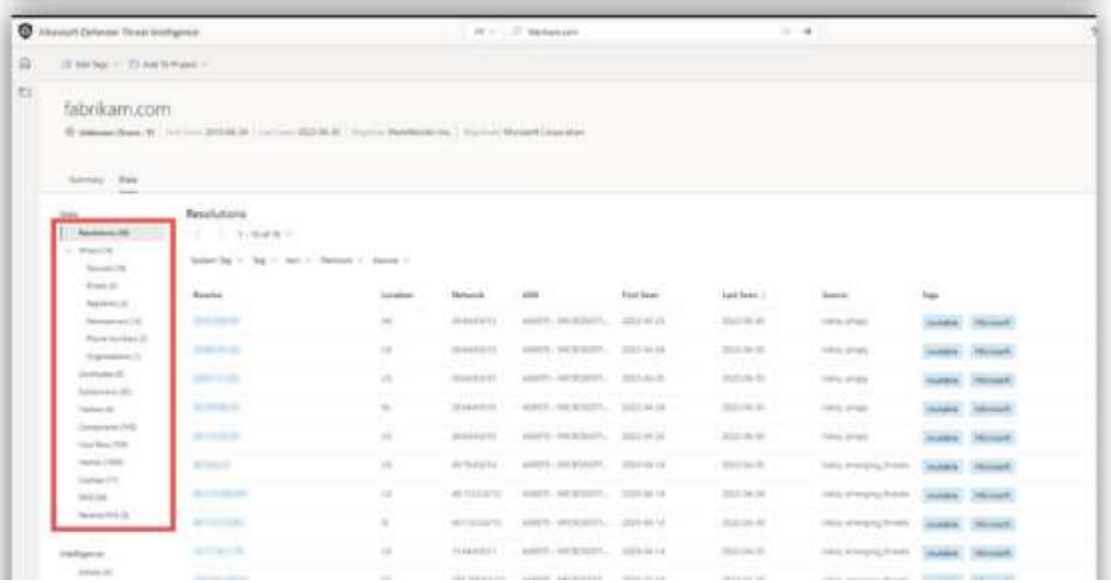
Basic cyber hygiene practices and cybersecurity training (2)

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.



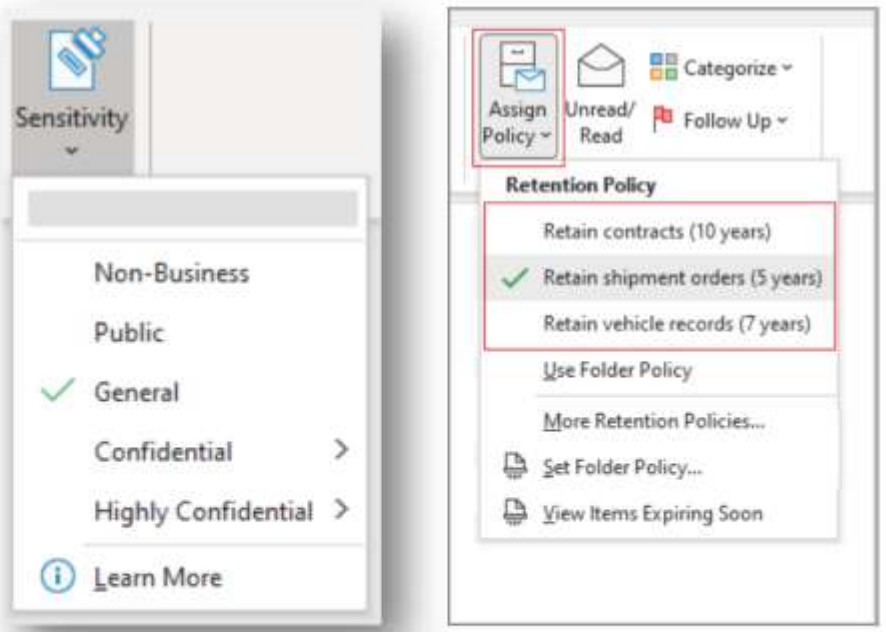


Policies and procedures regarding the use of cryptography and, where appropriate, encryption

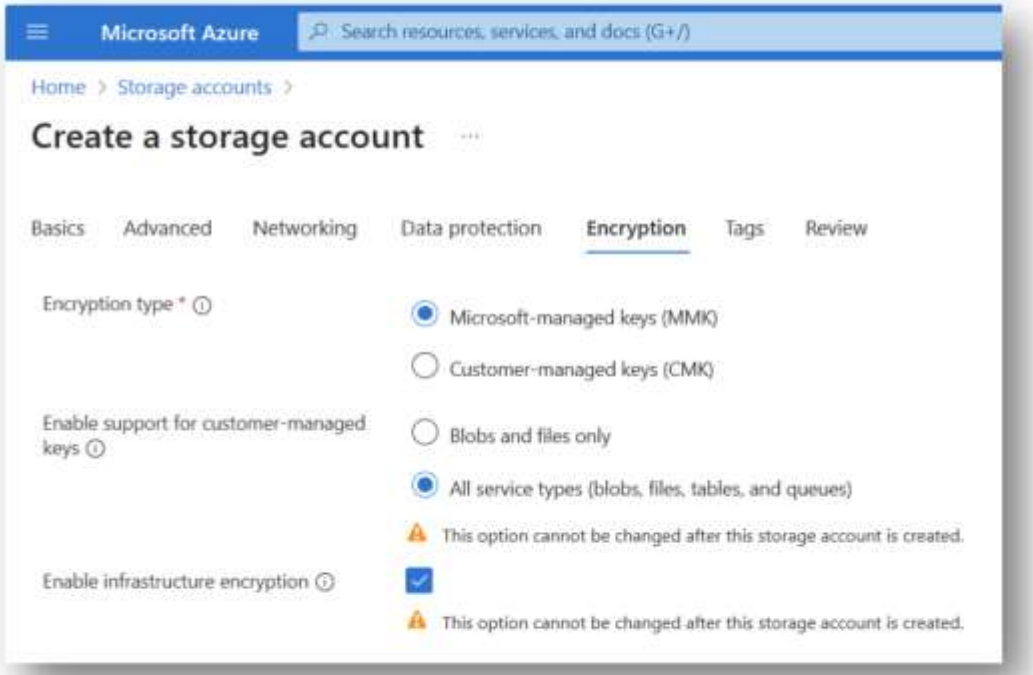
Encryption is an important part of your file protection and information protection strategy. Encryption by itself doesn't prevent content interception. Encryption is part of a larger information protection strategy for your organization. By using encryption, you help ensure that only authorized parties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

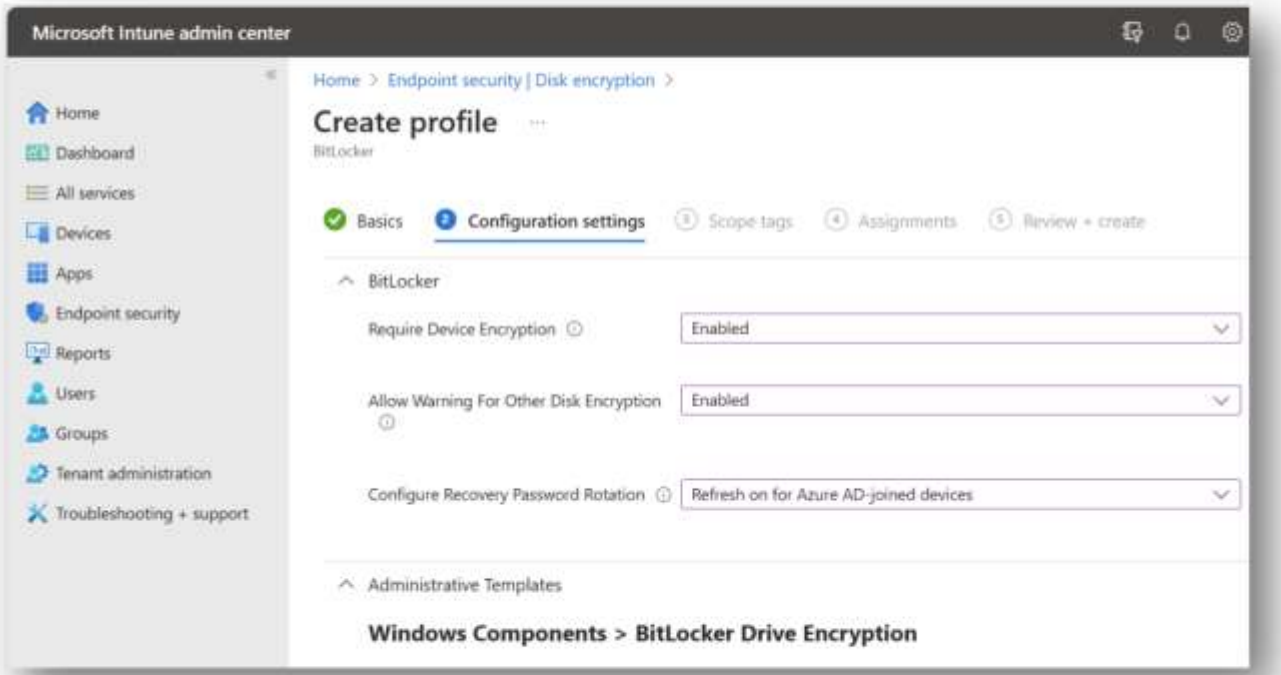
Data Lifecycle Management
Microsoft Purview Data Lifecycle Management provides you with tools and capabilities to retain the content that you need to keep and delete the content that you don't. Retaining and deleting content is often needed for compliance and regulatory requirement, but deleting content 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 SETTINGS IN A MICROSOFT AZURE STORAGE ACCOUNT



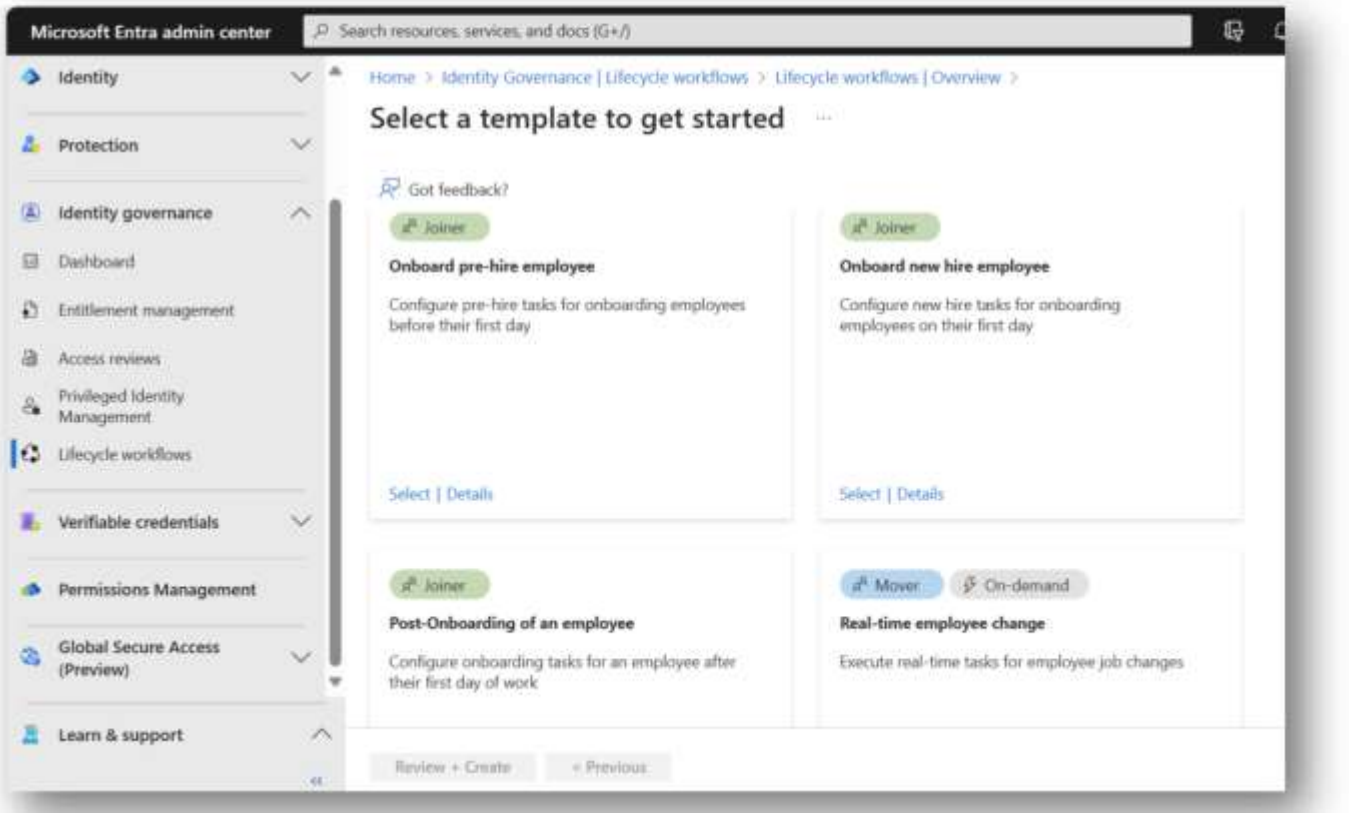
ENFORCING HARDDISK DRIVE ENCRYPTION THROUGH DEVICE POLICIES

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.

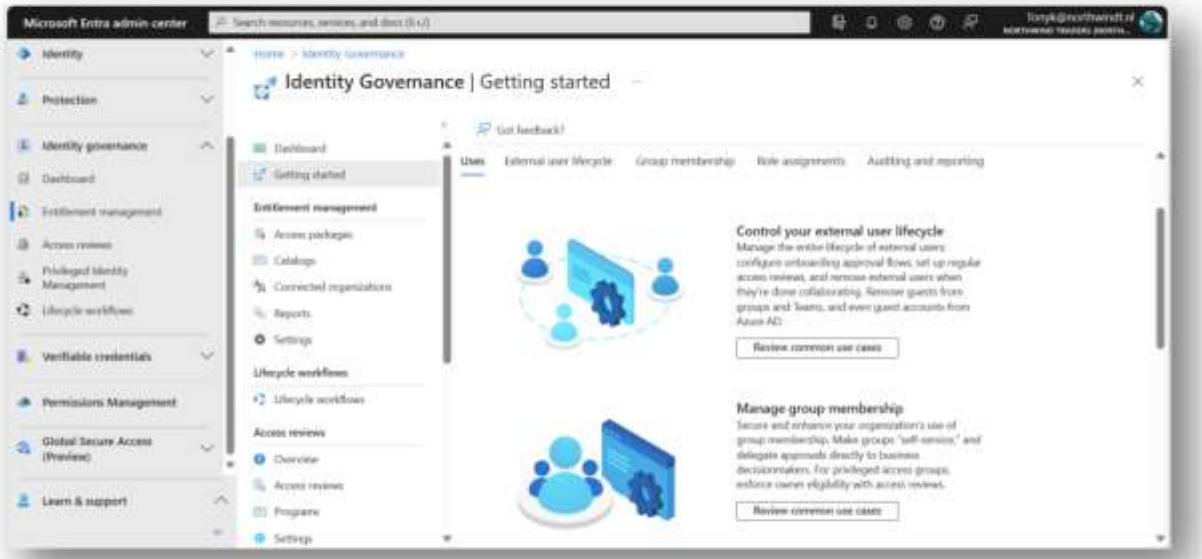


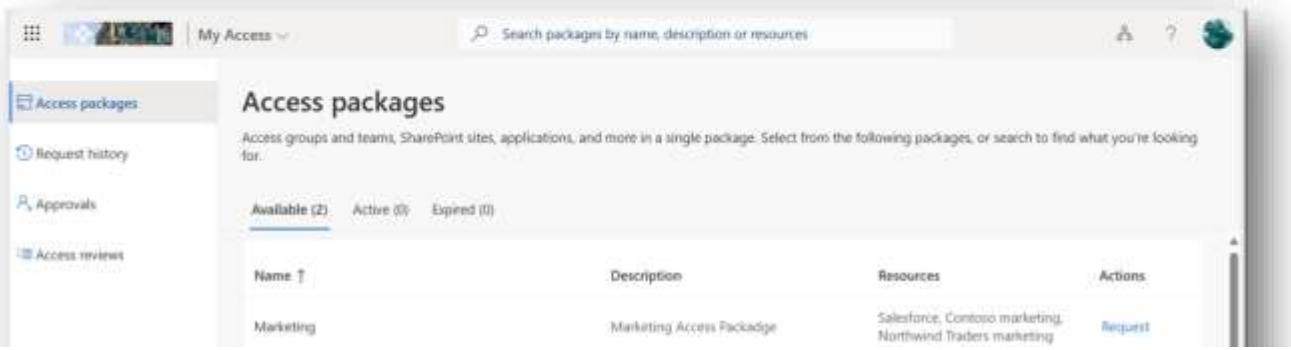
Human resources security, access control policies and asset management (2)

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).



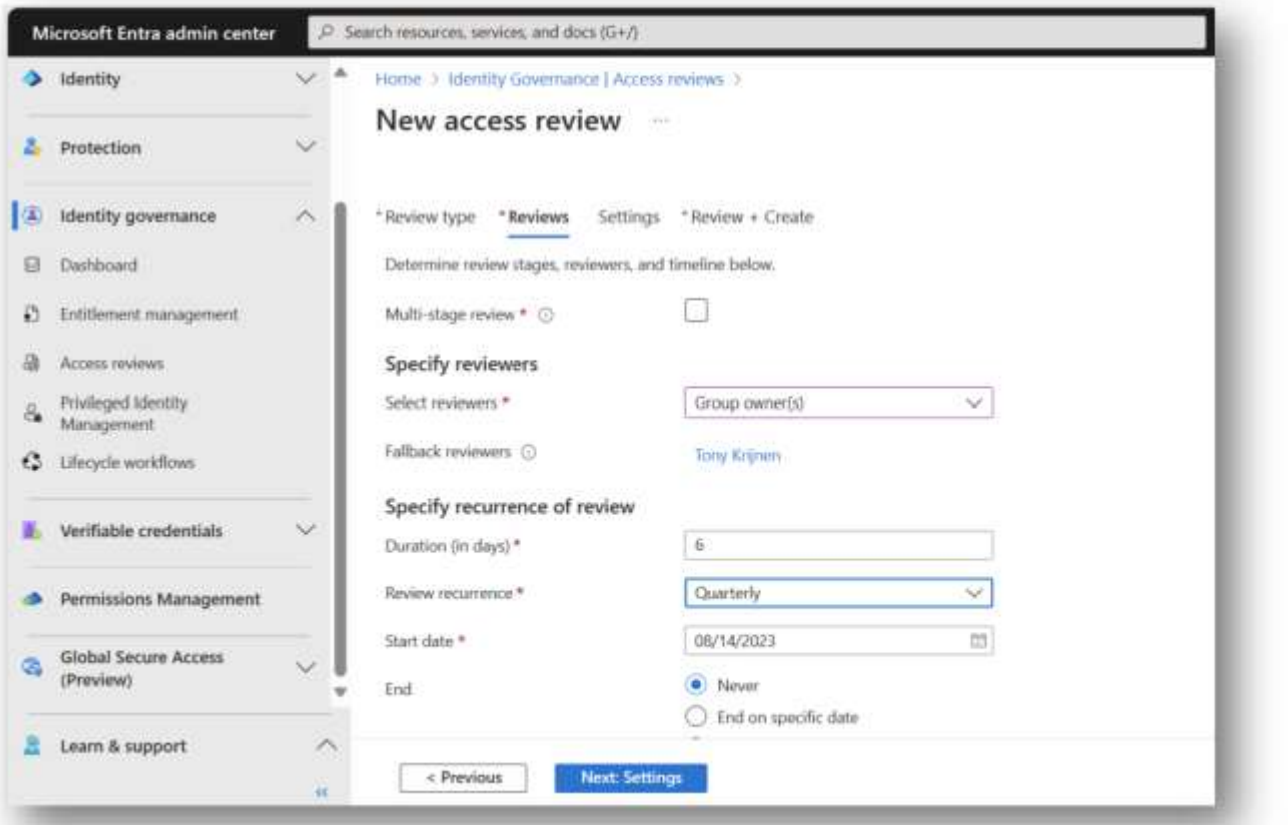


Human resources security, access control policies and asset management (2)

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.



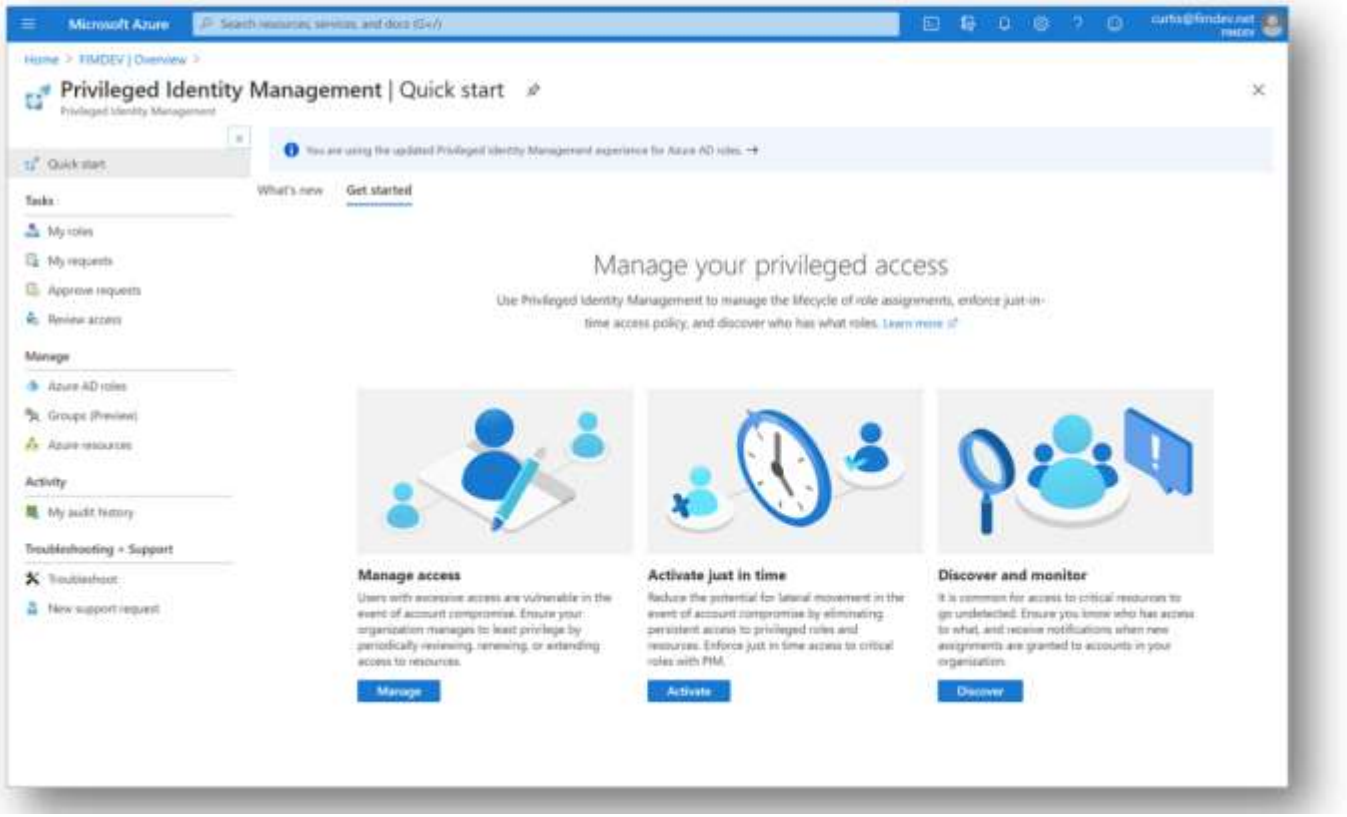
Human resources security, access control policies and asset management

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.

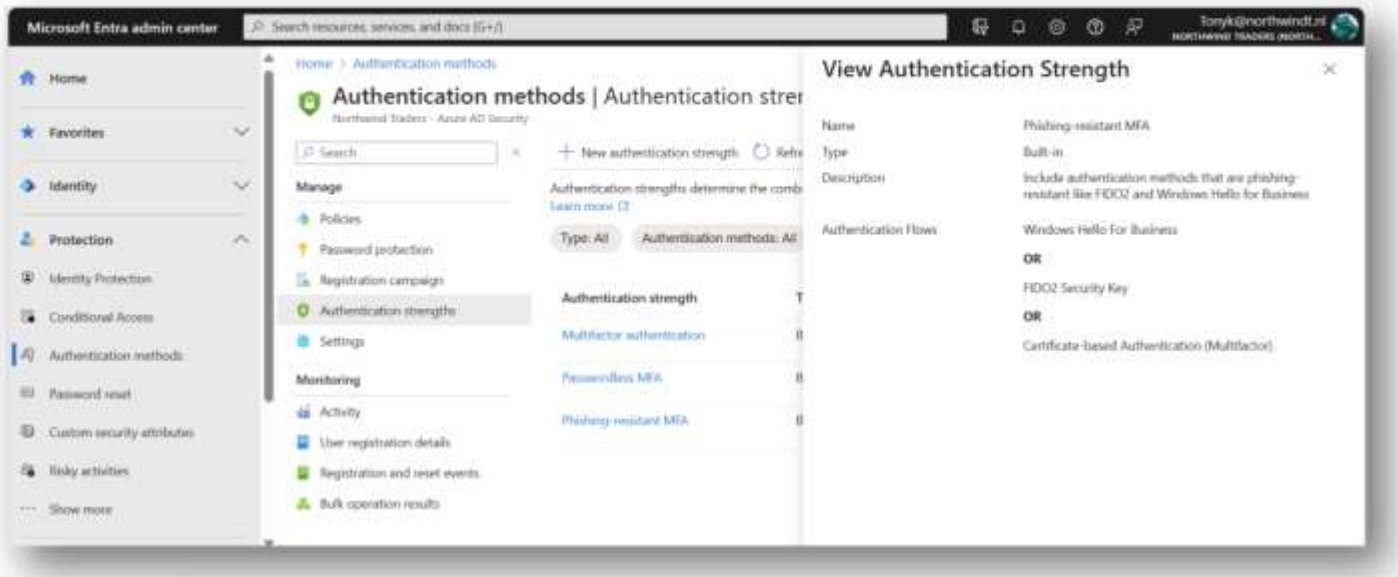


J

NIS 2 COMPLIANCE IS A ZERO TRUST JOURNEY

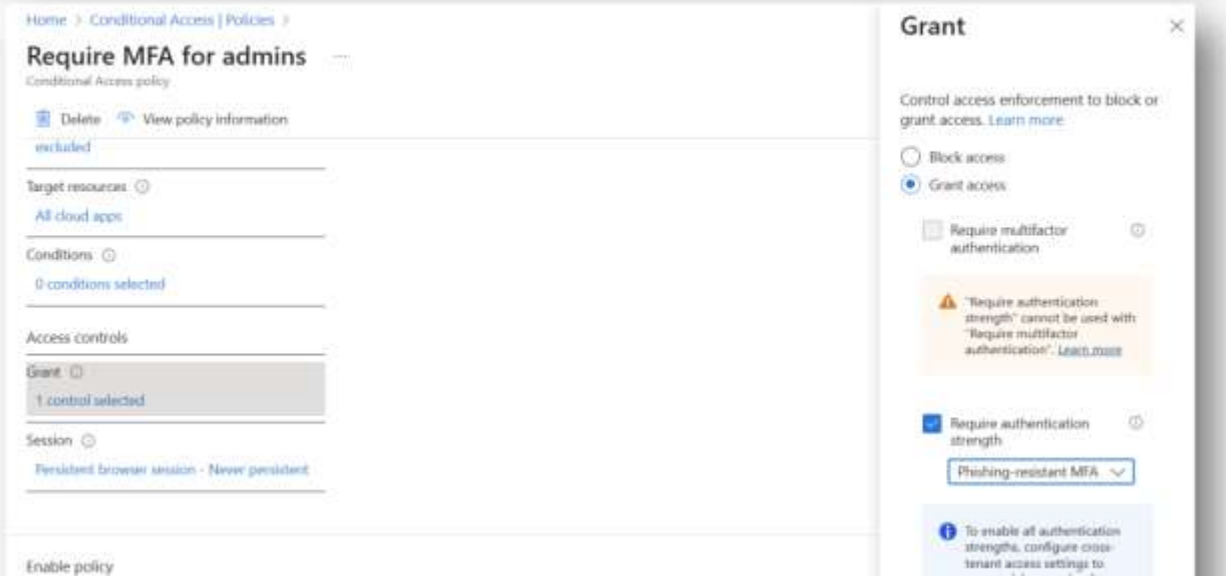
The use of multi-factor authentication or continuous authentication solutions

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

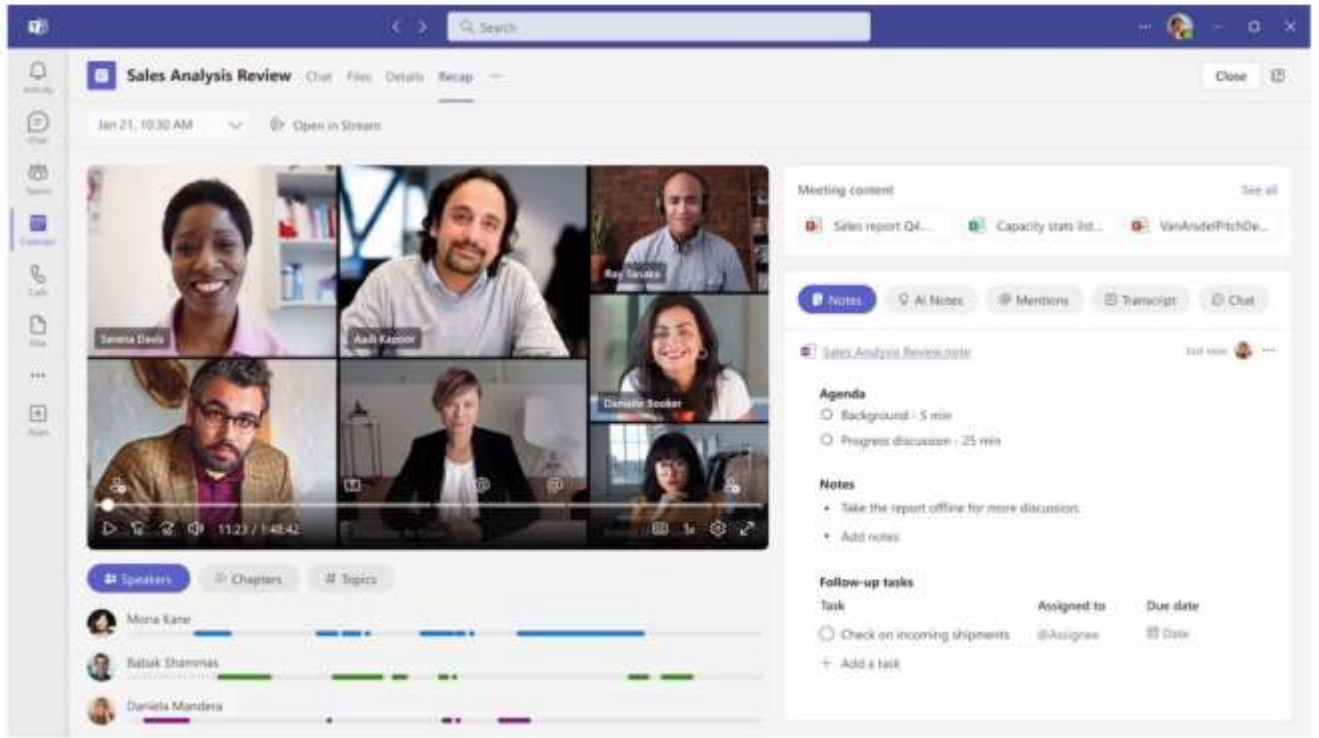
J

NIS 2 COMPLIANCE IS A ZERO TRUST JOURNEY

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.



Diskuse

Petr Vlk
Microsoft MVP
Enterprise Architect
KPCS CZ
vlk@kpcs.cz


KPCS