Microsoft

Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs

Een inleidend presentatie over hoe Microsoft 365 A5 kan helpen met het voldoen aan het Normenkader Informatiebeveiliging en Privacy en nieuwe mogelijkheden bieden voor het onderwijs.

13 juni 2024

SLBDIENSTEN.NL

Software én onderwijs, goed geregeld

Martijn Frank

Security Specialist Nederland

https://www.linkedin.com/in/martijnfrank/

martijn.frank@slbdiensten.nl

Microsoft

Xander Kupers

Senior Specialist Modern Workplace - Education

Link met mij

Of stuur mij een Teams chat:
xander.kupers@microsoft.com

Normalieter hebben we 3 uur de tijd om dit te presenteren….

We gaan het kort houden!

Agenda (om verwachtingen te managen)

1. Waarom hebben we dit ook alweer nodig?
2. Introduction to Normenkader-IBP
3. What is Zero-Trust?
4. How does Microsoft technology map to the Normenkader-IBP’s requirements

NOS Nieuws • Donderdag 20 oktober 2022, 18:17

Gegevens duizenden pashouders van TU Eindhoven op straat na hack

Gelekt document Fontys bevatte geen gevoelige informatie

Lessen uit ransomware-aanval op British Library

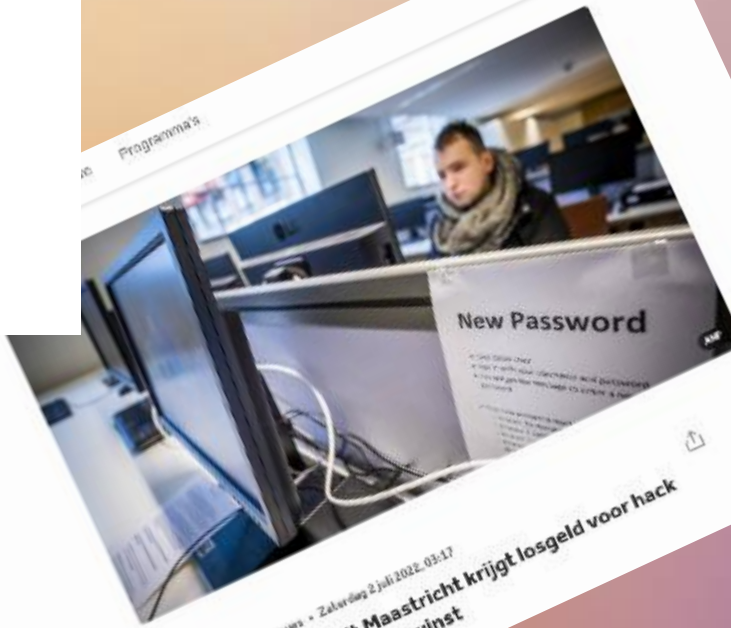
NOS Nieuws • Zaterdag 13 april, 13:44

Schoolboekenleverancier Iddink gehackt, mogelijk klantengegevens gelekt

Omroep West

NOS Nieuws • Maandag 23 augustus 2021, 18:51

ROC Mondriaan in Den Haag gehackt: 'Medewerkers staan werkloos bij de vestigingen'



NOS Nieuws • Zaterdag 2 juli 2022, 03:17

Universiteit Maastricht krijgt losgeld voor hack terug met flinke winst

Cijfers

60% van wereldwijde cyberaanvallen gericht op onderwijsinstellingen (bron: Microsoft Security Intelligence Divisie)

90% van de aanvallen is bedoeld om geld te verdienen

81% weet niet dat dit probleem speelt binnen onderwijs

(Bron: Breens Network)

De grootste risico's in onderwijs zijn DDOS 62%, Ransomware 50% en Malware 50%

De drie grootste zorgen zijn tijd en energieverlies 69%, kosten 65% en verminderde bereikbaarheid 48%

Slechts 5% of minder van het IT-budget wordt voor Security gereserveerd. Norm in bedrijfsleven is 25%

What is Normenkader-IBP?

Normenkader Informatiebeveiliging en Privancy voor het Funderend Onderwijs (IBP FO)

Een hulpmiddel: om toe te werken naar **sterkere informatiebeveiliging** en **betere bescherming van persoonsgegevens.**

Verdeeld over 2 delen: Informatiebeveiliging (15 domeinen) en Privacy (nog in ontwikkeling) en gebaseerd op het NBA Volwassenheidsmodel voor informatiebeveiliging.

Alle schoolorganisaties binnen het Funderend Onderwijs (PO/VO) te laten voldoen aan **minimale normen** met betrekking tot de digitale veiligheid.

Het **instrument voor het verbeteren van informatiebeveiliging en privacy:** Het programma ontwikkelt het “Information Security and Privacy Standards Framework for Fundamental Education”, dat schoolbesturen zal helpen een betere bescherming van persoonsgegevens te realiseren.

Normenkader-IBP FO

- Een antwoord op de stijging van maar liefst 88% in cyberincidenten de afgelopen jaren (Bron: Privacy op School)
- Scholen moeten in 2027 hieraan voldoen
- Benoemd door het Ministerie van Onderwijs
- Gemaakt in samenwerking met Kennisnet, SIVON, de PO Raad en de VO Raad.
- Het niet voldoen aan de eisen heeft juridische gevolgen

Gaat pas in per 2027….dus waarom nu al mee bezig?

Wie gaat het beoordelen, wat gebeurt er wanneer we er niet aan voldoen?

Wie is er verantwoordelijk voor het naleven van het Normenkader?

En implementatie?

En succes?

Maar waarom is dit eigenlijk belangrijk?

Hier gaan we doorheen…maar dan anders

15 domeinen voor informatiebeveliging

1. Bestuur
2. Organisatie
3. Risicomanagement
4. Personeelbeheer
5. Configuration Management
6. Incident-/Problem Management
7. Change Management
8. Systemonwikkeling
9. Datamanagement
10. Identity and Access Management
11. Security Management
12. Fysieke beveliging
13. IT-Operatie
14. Bedrijfcontinuïteitsmanagement
15. Ketenbeheer

Hoofdstuk	Inhoudsopgave	Norm	Microsoft Technologie
1.	**Bestuur**		
1.1	Strategie	Een strategie en visie op informatie- en cybersecurity is leidend voor activiteiten en maatrelegen met betrekking tot informatieebeveliging	Communicatie via Sharepoint (Intranet) en collaboratie via Viva Communications (Connections, Engage, Amplify)
1.2	Beleid	De organisatie heeft een (informatie)beveilingingbeleid vastgesteld, beschreven en gecommuniceerd met medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management	Communicatie via Sharepoint (Intranet) en collaboratie via Viva Communications (Connections, Engage, Amplify)
1.3	Planning/Roadmap	Bedrijfsdoelstelligen, risco's en compliance-eiden worden vertaald in een algemeen informatie-beveiligingsplan en/of cybersecurityplan, rekening houdend met de IT-infrastructuur en de veiligheidscultuur	Communicatie via Sharepoint (Intranet) en collaboratie via Viva Communications (Connections, Engage, Amplify) + als jaarplanning de nieuwe Microsoft Planner
2.	**Organisatie**		
2.2	Functiescheiding	Rollen en verantwoordelijlheden zijn gescheiden om de kans te verkleinen dat individuele personen kritieke processen in gevaar brengen. Het personeel voert alleen geautoriseerde taken uit die bij hun respectievelijke functies en rol horen.	Rechten Matrix +PIM (A5) voor beheerders
3.	**Risicomanagement**		
	Raamwerk voor	Er is een raamwerk voor informatierisicomanagement opgesteld en afgestemd op de doelstellingen van de organisatie en het raamwerk voor organisatierisicomanagement.	Threat & vulnerability management, Attack simulator (A5) PLUS training (Computrain?)

4.	**Personeelbeheer**		
4.2	Certificering, training en scholing	Opleding, training en/of ervaring worden regelmatig getoetst om te zien of het personeel over de benodige competenties beschikt om taken naar behoren te vervullen. Basis (IT-)competenties zijn vastgesteld en, indien nodig, worden kwalificatie-en certificeringsprogramma's gebruikt om te controleren of ze worden bijgehouden.	Viva Learning/MIIP Webinars of andere webinars
4.6	Veiligheidsbewustzijn	Er is een bewustwordingsprogramma om gebruikers bewust te maken van hun verantwoordelijkheid om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie (middelen) te beschermen.	Viva Learning/ Attack Simulator
6.	**Incident-/Problem Management**		
6.1	Incident Management	Een formeel incidentmanagementproces wordt gecommunicerd en geimplementeerd. Er zijn procedures ingesteld om ervoor te zorgen dat alle incidenten en storingen worden geregistreerd, geanalyseerd, gecategoriseerd, en geprioriteerd naar impact. Alle incidenten worden bijgehouden en periodiek beoordeeld om ervoor te zorgen dat ze tijdig worden verholpen.	Documentatie, Dynamics, Self-Service Portal, Viva Connections integration met ServiceNow/TopDesk
6.3	Incidentrespons op (cyber)beveiligingsincidenten	De organisatie beschikt over mogelijkheden voor incidentrespons om (cyber) beveilingingincidenten snel te detecteren, te isoleren en de impact te veperken en om diensten op een betrouwbare manier te herstellen en weer in de lucht te brengen.	Microsoft Defender Suite + Microsoft Sentinel: Sentinel en Threat Management (logging van Microsoft Defender oplossingen) A3 = discovery, A5 = automated response & remediation. Ook MDCA = A5)
8.	**Systemontwikkeling**		
8.2	Toegang tot de productieomgeving door ontwikkelaars	Medewerkers (ontwikkelaars) die betrokken zijn bij de ontwikkeling en implementatie van wijzingen in applicaties en ondersteunende besturingssystemen en databases, hebben geen schrijftoegang tot de productieomgeving. Medewerkers (ontwikkelaars) die verantwoordelijk zijn voor het vrijgeven van de broncode voor productie hebben geen schrijftoegang tot de test-of ontwikkelomgeving.	PIM documentation - Microsoft Entra ID Governance (A5)

9.	**Datamanagement**		
9.2	Classificatie	Stel een classificatieschema op dat in de hele organisatie van toepassing is, op basis van de kriticiteit en gevoeligheid (bijvoorbeeld openbaar, vertrouwelijk, topgeheim) van organisatiegegevens. Dit schema bevat details over het eigenaarschap van gegevens; gedefinieerde passende (informatie)beveiligingsniveaus en beschermingsmaatregelen; en een korte beschrijving van eisen voor het bewaren en vernietigen van gegevens, en goeveligheid. Het wordt gebruikt als basis voor het toepassen van maatregelen zoals toegangcontrole, archivering en versleuteling.	Information Protection en Document labeling (met tagging) (A5)
9.3	Beveiligingseisen voor datamanagement	Beleid en procedures zijn vastgesteld en geïmplementeerd om (informatie)beveiligingseisen te identificeren en toe te passen op de ontvangst, verwerking, opslag en doorgifte van relevante gegevens in lijn met bedrijfsdoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en wettelijke vereisten (bijvoorbeeld privacy van bepaalde gegevens).	Information Protection en Document labeling (met tagging) + Defender for Cloud Apps (A5)
9.4	Inrichting van opslag en retentie	Er zijn procedures gedefinieerd en geïmplementeerd voor het effectief en efficiënt opslaan, bewaren en archiveren van gegevens, zodat wordt voldaan aan organisatiedoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en wettelijke vereisten.	Information Protection en Document labeling (met tagging) + Defender for Cloud Apps - Volgens FORA mag backup niet op dezelfde locatie/platform als de data zelf staan (ook al is het in de cloud).
9.5	Uitwisseling van (gevoelige) gegevens	(Cyber)beleid en procedures zijn vastgesteld en geïmplementeerd, zodat aan bedrijfseisen voor de bescherming van gegevens en software wordt voldaan waneer gegevens en software worden uitgewisseld binnen de organisatie of met een externe partij. Gevoelige transactiegegevens worden alleen uitgewisseld via een vetrouwd pad of medium waarbij (cyber)maatregelen zijn genomen om de authenticiteit van de inhoud, bewijs van versturen, bewijs van ontvangst en onweerlegbaarheid van de oorsprong aan te tonen.	Purview advanced message encryption, Defender for Cloud Apps - Encryption & Bitlocker (Microsoft Purview Advanced Message Encyption), MD for CloudApps. (A5)
9.6	Verwijdering van data	Er zijn (cyber)procedures vastgesteld en geïmplementeerd om ervoor te zorgen dat aan business requirements voor het beschermen van (gevoelige) gegevens en software wordt voldaan bij het verwijderen of overdragen van gegevens of hardware.	AIP P2 (Purview Lifecycle Management – Entra ID Governance) + A5
10.	**Identity and Access Management**		
10.1	Toegangsrechten	De organisatie heeft toegangsgroepen (of rollen) gedefinieerd op basis van vastgestelde bedrijfsregels, waaronder functiescheiding, in een Autorisatiematrix. Er zzijn procedures die tijdige initiatie en update in de autorisatiematricies voor alle toepassingen regelen. Het management keurt wijzigen in vastgestelde rechten voor toegangsgroupen (or rollen) goed. Alle gebruikersactiviteiten zijn traceerbaar tot op het individu (bijvoorbeeld gebaseerd op een combinatie van gebruikersnaam en wachtwoord of token of biometrische informatie).	IAM + PIM (A5) - Entra Verified ID (Tutorial - Advanced Microsoft Entra Verified ID setup - Microsoft Entra Verified ID | Microsoft Learn)

10.2	Administratie van toegangsrechten	Toegangsrechten voor werknemers worden toegewezen in overeenstemming met toegewezen taakverantwoordelijkheden (bijvoorbeeld via op rollen gebaseerde toegang). Beheerprocedures zijn beschikbaar om activiten vast te stellen voor het aanvragen, uitgeven of sluiten van een account en de bijbehorende toegangsrechten voor gebruikers. De procedure omvat tevens de methode die door het bevoegd gezag wordt gebruikt om deze activiteiten op de juiste wijze te autoriseren. Toegang wordt verschaft op basis van het neet-to-know/neet-to-have-principe.	IAM + PIM (A5) - Entra Verified ID (Tutorial - Advanced Microsoft Entra Verified ID setup - Microsoft Entra Verified ID | Microsoft Learn)
10.3	Superusers	Het management heeft maatregelen ingevoerd die ervoor zorgen dat superuesertoegang beperkt is tot de juiste (beperkte) groep indiiduem en dat activiteiten die worden uitgevoerd met superuseraccounts worden gemonitord. Superuseraccounts moeten worden goeggekeurd door het verantwoordelijk management.	PIM (A5)
11.	**Security Management**		
11.2	Authenticatiemechanismes.	Alle gebruikers (intern, extern en tijdelijk) en hun activiteiten op IT- systemen moeten uniek indentificeerbaar zijn. Het management is verantwoordelijk voor de periodieke controle van de lijst met actieve ID's in relevante applicaties om te bepalen of unieke user ID's zijn geïmplementeerd om traceerbaarheid te garanderen en ervoor te zorgen dat algemene en systeemaccounts geblokkerd of op andere wijze beschermd zijn. Alle onjuiste of inactieve user ID's die tijdens het controleproces worden opgemerkt, worden tijdig gedeactiveerd.	Entra ID (B2C, B2B) en/of FIDO2. PIM, PAM
11.7	Threat en Vulnerability Management	Er is een proces voor Threat en Vulnerability Management geïmplementeerd om bedreigingen te indentificeren en kwestbaarheden, die kunnen leiden tot een verslechtering van de presentaties van of een aanval op bedfrijfsmiddelen, tijdig te detecteren en te verhelpen. Het aantal aanvalsvectoren wordt ook beschouwd, waardoor de algehele blootstelling wordt verminderd.	Microsoft Threat & Vulnerability Management – part of MDE (A5)
11.8	Beschikbaarheid en bescherming van infrastructuur	Interne beheers-, beveiligings- en auditmaatregelen worden geïmpleneteerd tijdens configuratie, integratie en onderhoud van hardware en infrastructuursoftware om middelen te beschermen en beschikbaarheid en integreit te waarborgen. Verantwoordelijkheden voor het gebruik van gevoelige infrastructuurcomponenten zijn duidelijk gedefinieerd en bekend bij degen die infrastructuur componenten ontwikkelen en integreren. Het gebruik ervan wordt gecontroleerd en geëvalueerd.	Physical environment (Defender for Server, Endpoint)
11.11	Network security	Beveiligingstechnieken en bijbehorende beheerprocedures (zoals firewalls, beveiligingsapparatuur, netwerksgmentatie en inbraakdetectie) worden gebruikt voor het autoriseren van toegangs- en besturingsinformatiestromen van en naar netwerken. Er wordt gebruikgemaakt van best practicies op dit gebied (bijvoorbeeld NCSC, ISO/IEC. ITSec).	MDE (A5)
11.12	Beheersing van malware-aanvallen	Preventie-, detectie- en correctiemaatregelen zijn aanwezig (met name actuele beveiligingspatches en virusscanning) in de hele organisatie om informatiesystemen en technologie te beschermen tegen malware (bijvoorbeeld virussen, wormen, spyware, spam).	MDE / MDO P2 (A5)

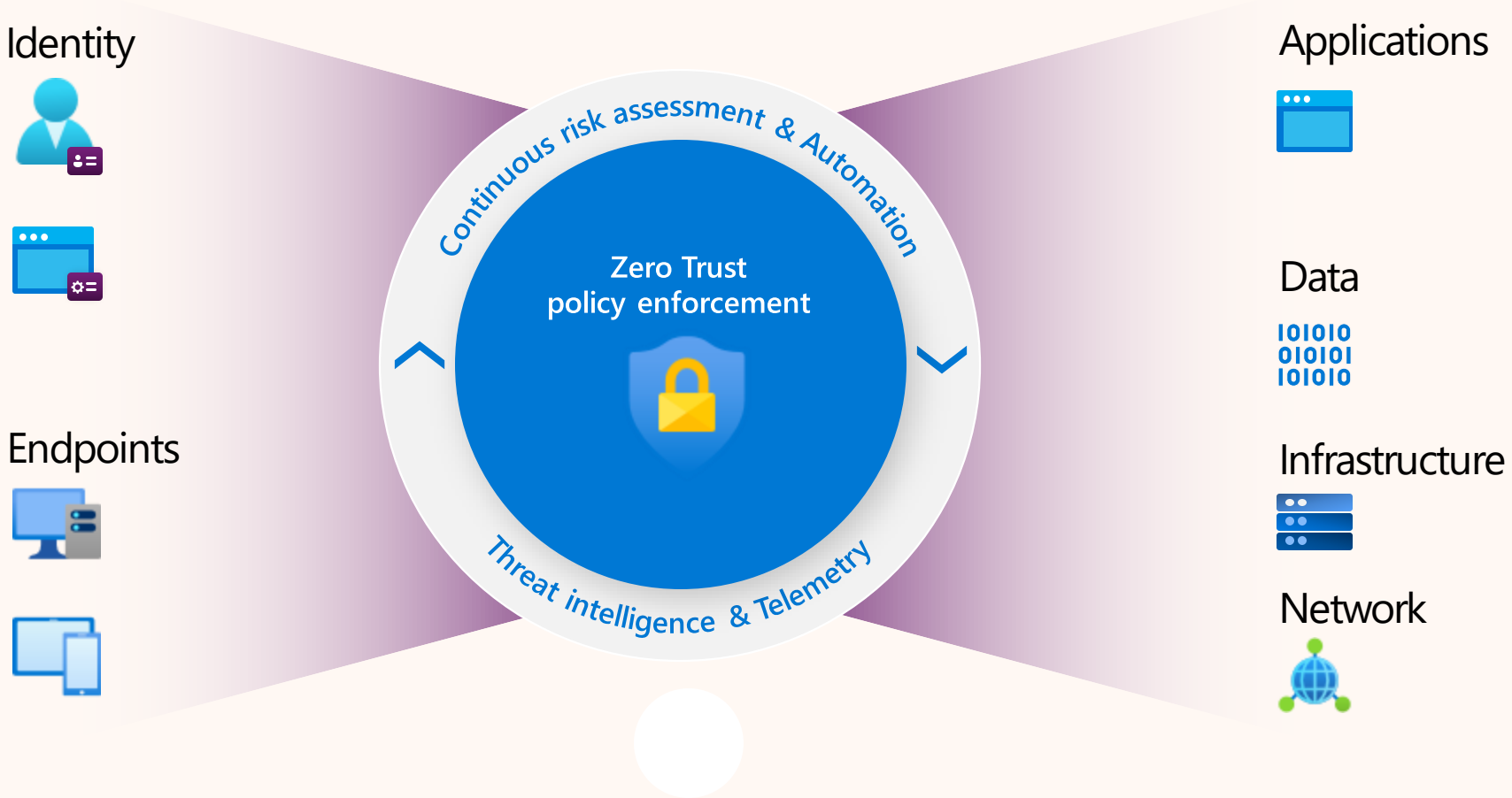
Microsoft

Zero Trust

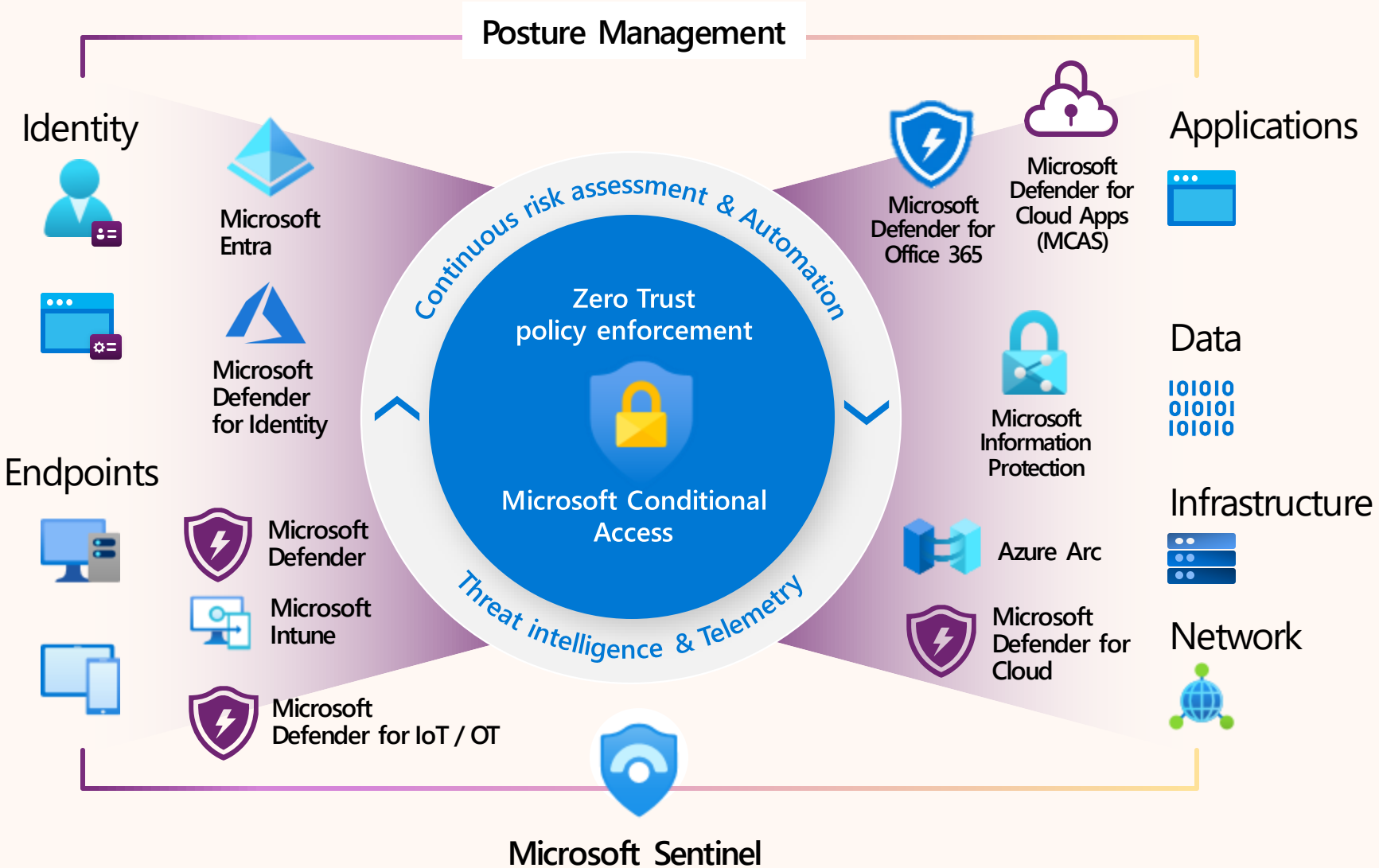
Zero Trust architecture recommends continuous risk assessment in the digital world where attacks happen at cloud speed. Each request shall be intercepted and verified explicitly by analyzing signals on user, location, device compliance, data sensitivity, and application type.

More information on Zero Trust

Zero Trust Approach from Microsoft

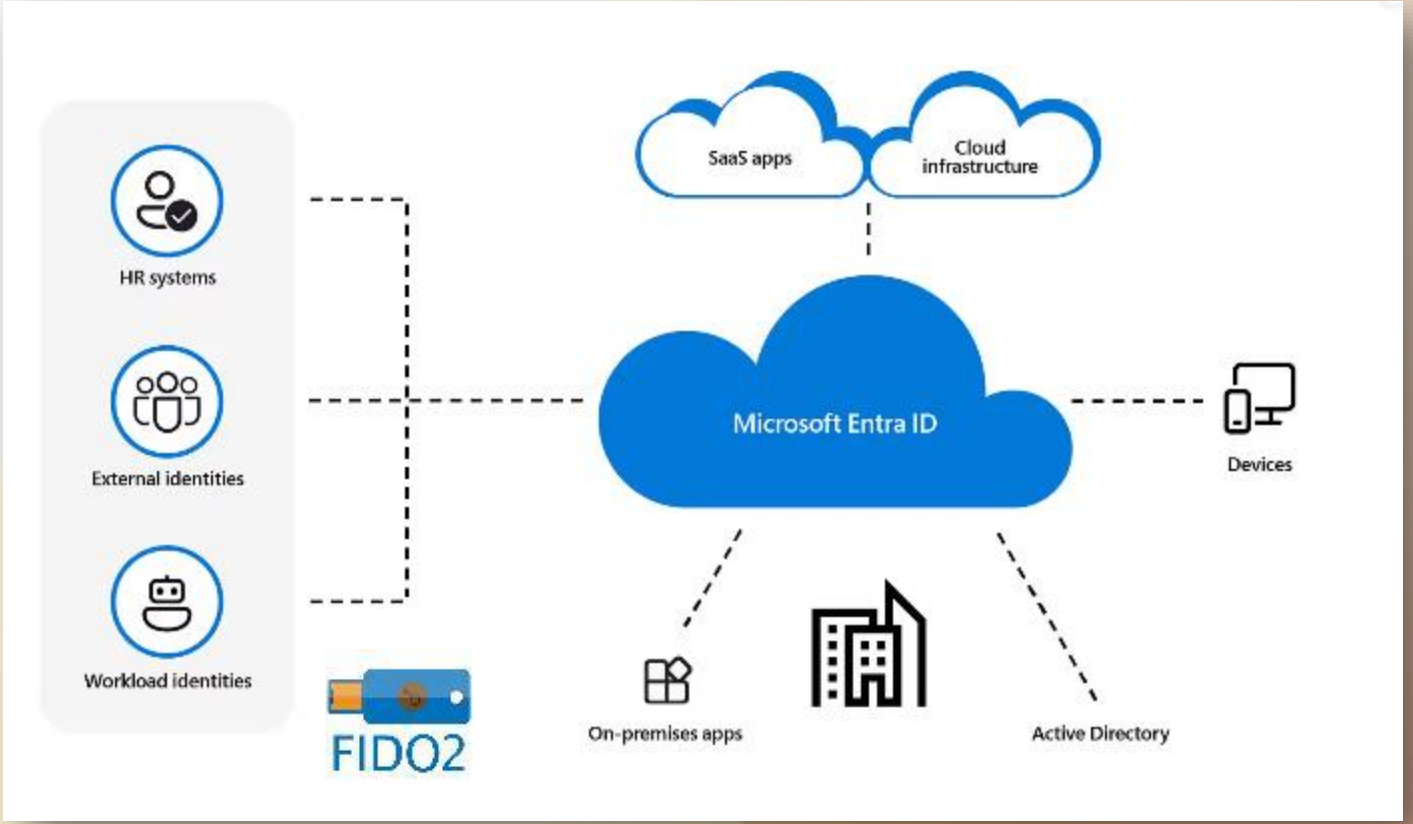


Microsoft Zero Trust Capabilities



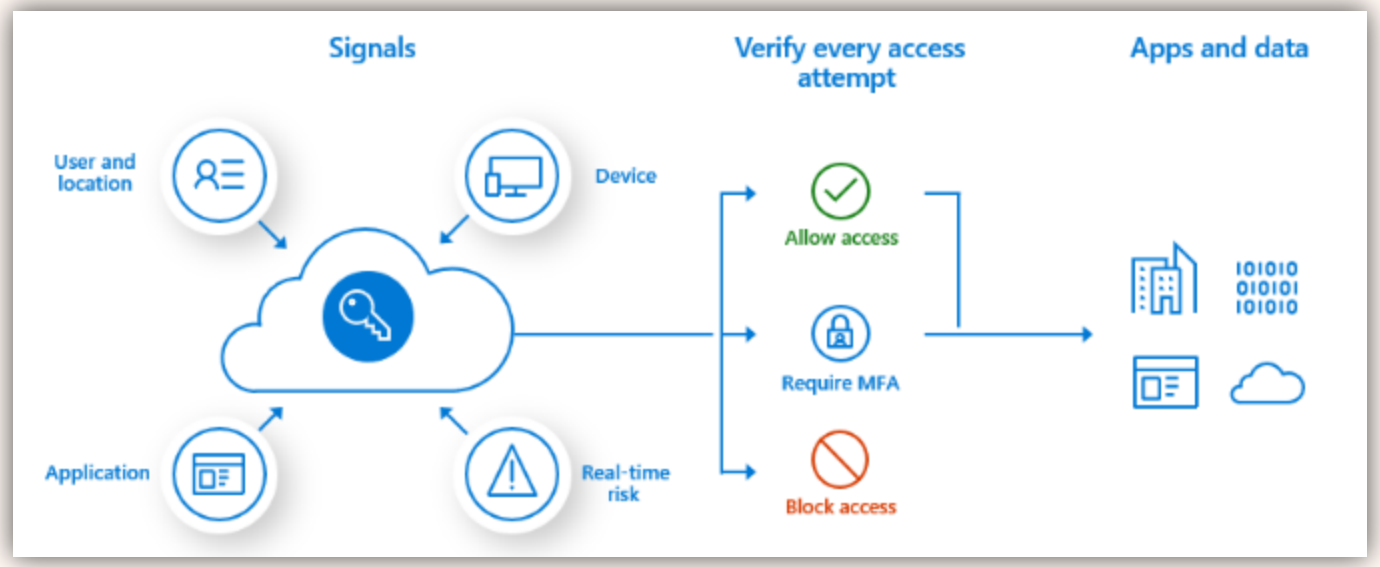
Microsoft

Identity



Multi-Factor Authentication (MFA) – part of M365 A3

- 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.
- Multifactor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan.
- Microsoft Entra ID Protection helps you manage the roll-out of Microsoft Entra multifactor authentication registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

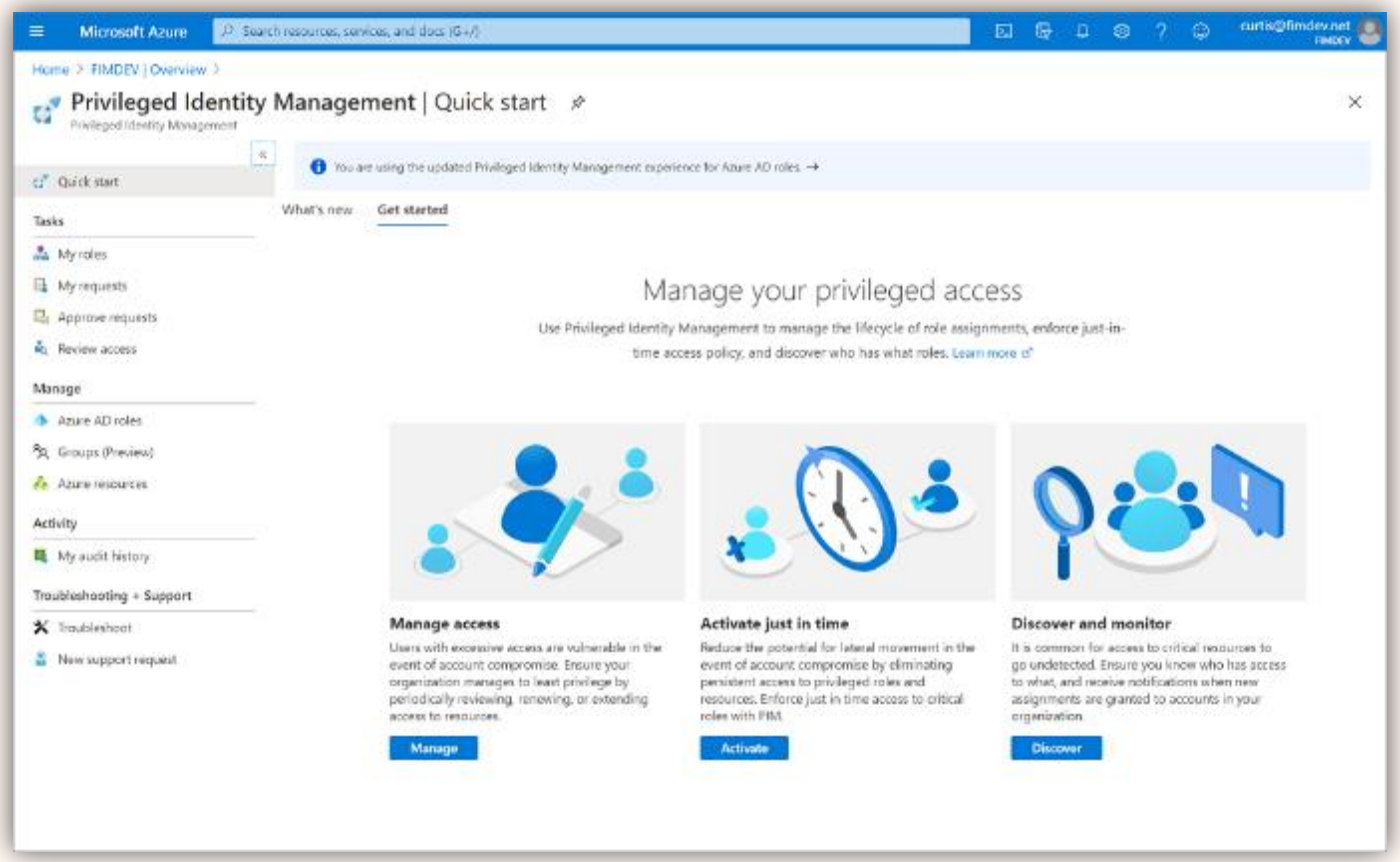


More information on MFA

Privileged Identity Management - Microsoft Entra

Linking to points 2.2, 8.2, 10.1, 10.2, 10.3, 11.2, of Normenkader-IBP

- 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. These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.
- 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.

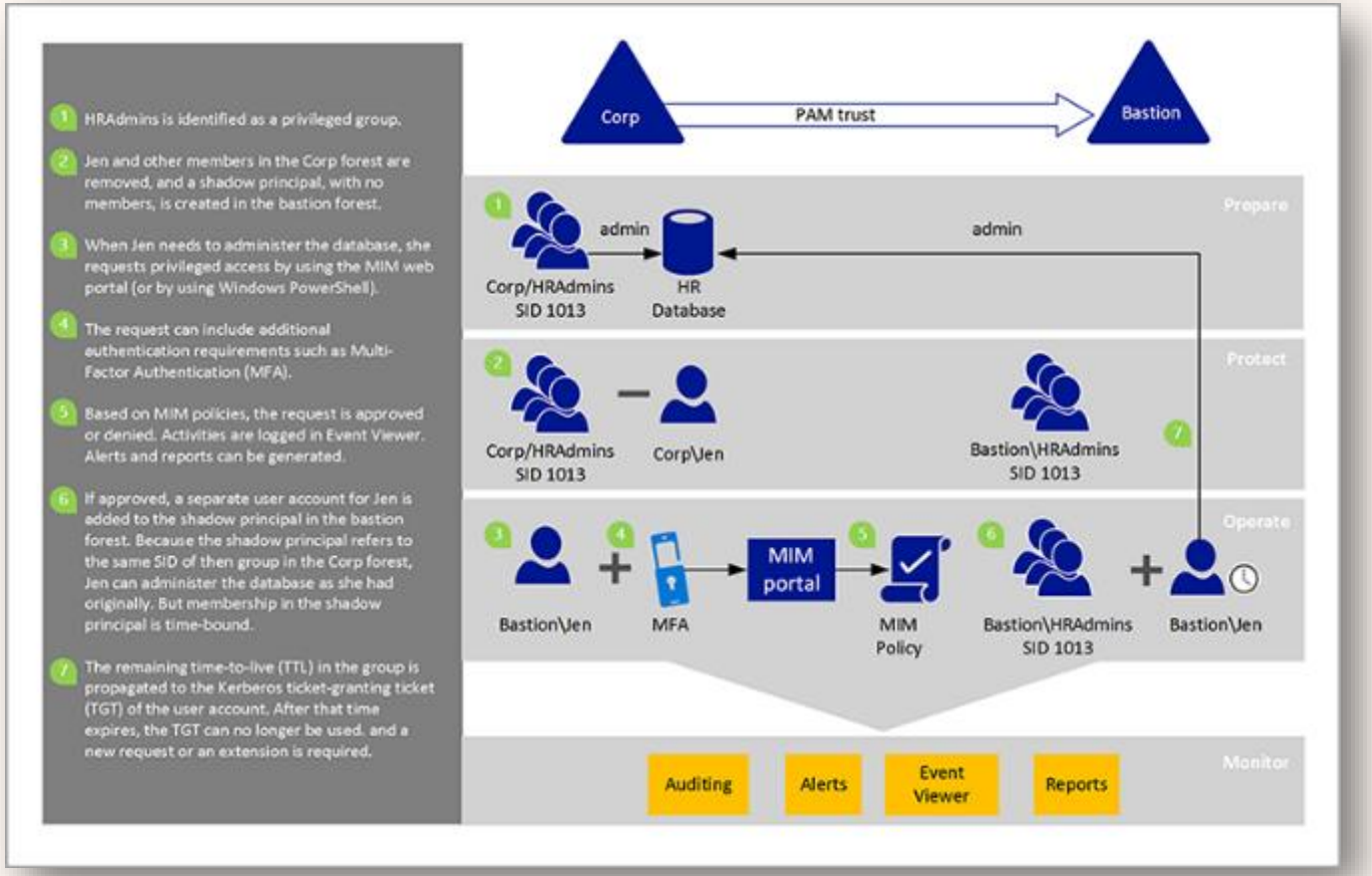


More information on [PIM]

Privileged Access Management

Linking to point 11.2 of Normenkader-IBP

- MIM Privileged Access Management (PAM) is a solution that helps organizations restrict privileged access within an existing and isolated Active Directory environment.
- MIM PAM is distinct from Microsoft Entra Privileged Identity Management (PIM).
- The PAM approach provided by MIM PAM is not recommended for new deployments in Internet-connected environments. MIM PAM is intended to be used in a custom architecture for isolated AD environments where Internet access is not available, where this configuration is required by regulation, or in high impact isolated environments like offline research laboratories and disconnected operational technology or supervisory control and data acquisition environments.



More information on **PAM**

Microsoft

Microsoft Defender

Microsoft Defender for Office Plan 2

Linking to point 11.2 of Normenkader-IBP

- Defender for Office 365 Plan 2 expands on the investigation and response capabilities of Plan 1 and EOP, including the addition of automation.

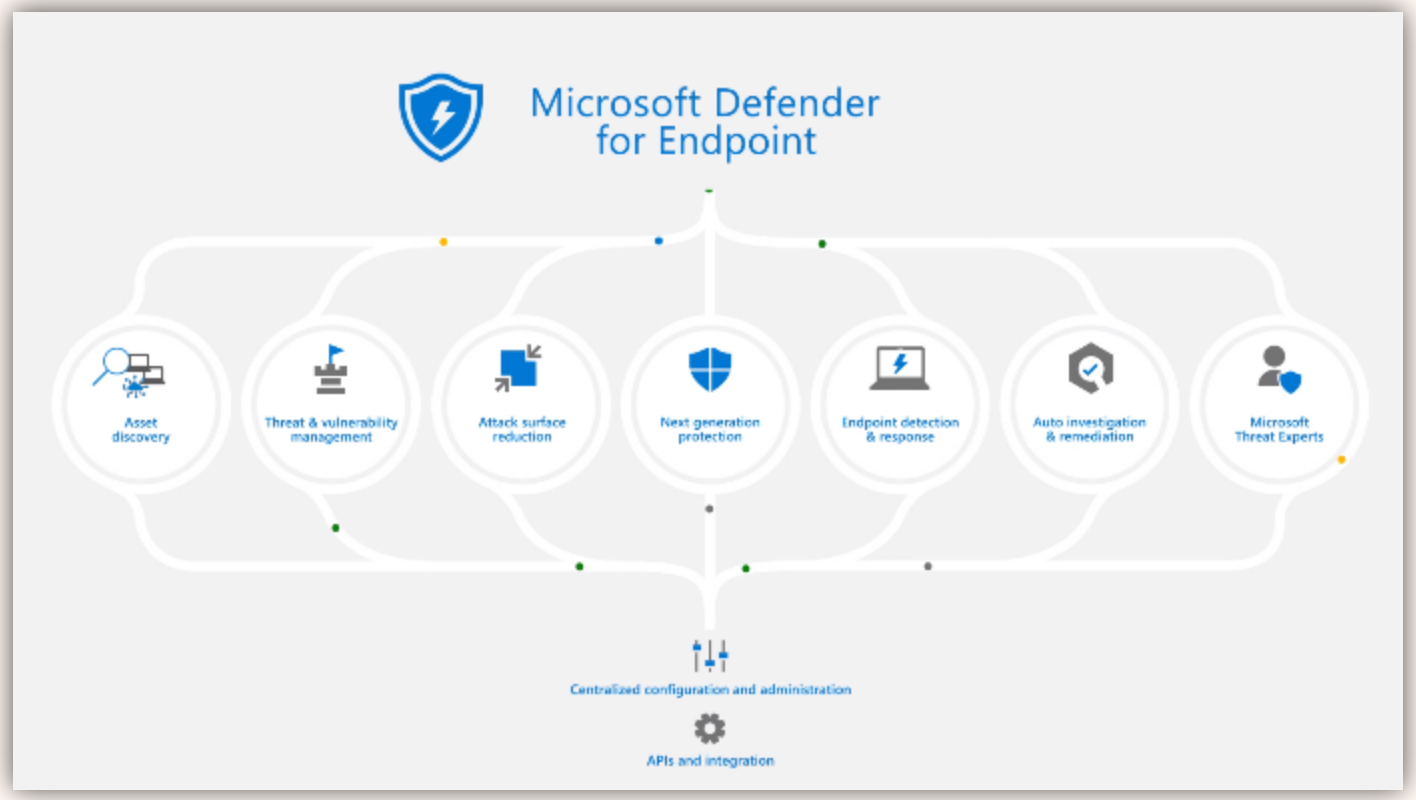
- Additionally to Plan1:
  - Threat Explorer (Explorer) instead of Real-time detections.
  - Threat Trackers
  - Campaigns (Attack Simulation)
  - Automated Investigation and Response (AIR):
  - AIR from Threat Explorer
  - AIR for compromised users
  - SIEM Integration API for Automated Investigations

More information on Defender for Office Plan 2

Microsoft Defender for Endpoint Plan 2

Linking to points 3.1, 11.8, 11.11, 11.12, of Normenkader-IBP

- Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Additionally to Plan 1:
  - Endpoint detection and response
  - Deception techniques
  - Automated investigation and remediation
  - Cyberthreat and vulnerability management
  - Threat intelligence (cyberthreat analytics)
  - Sandbox (deep analysis)
  - Endpoint attack notifications

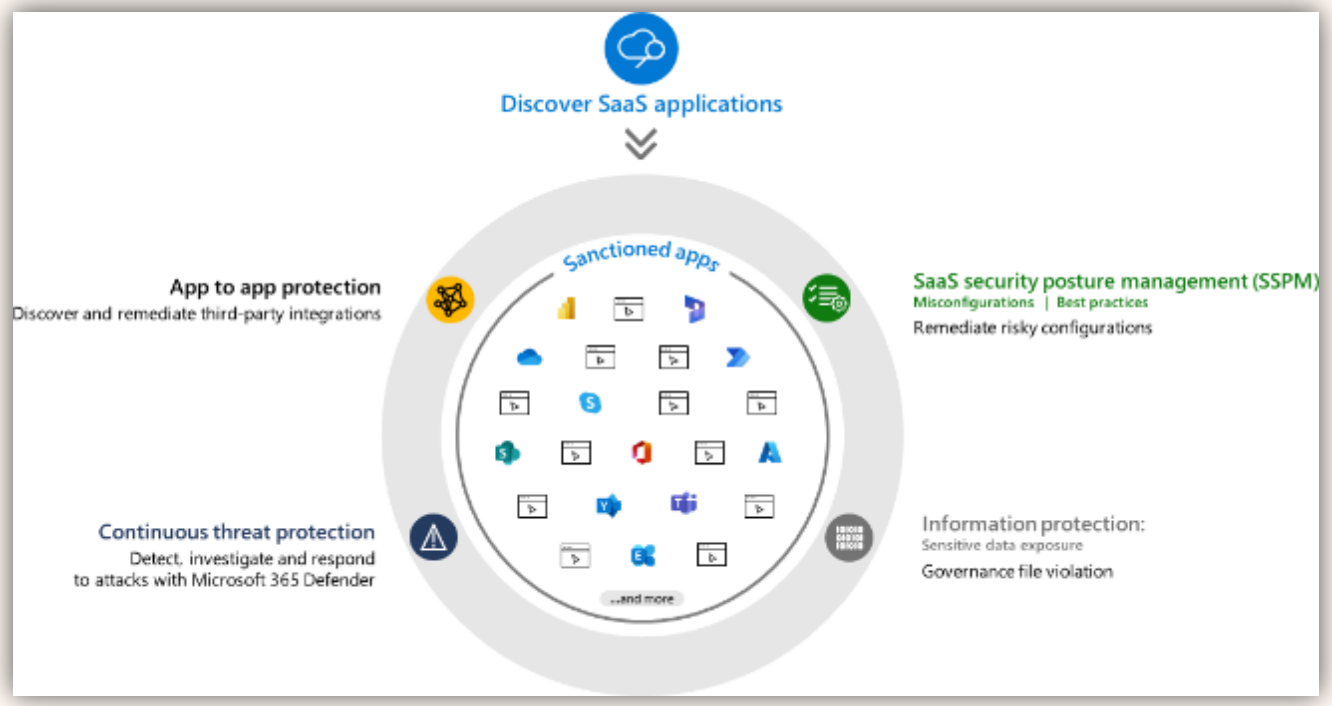


More information on [Defender for Endpoint Plan 2]

Microsoft Defender for Cloud Apps Plan 2

Linking to points of 9.3, 9.4, 9.5, 11.13 Normenkader-IBP

- Microsoft Defender for Cloud Apps is a critical component of the Microsoft Cloud Security stack. It's a comprehensive solution that helps your organization take full advantage of the promise of cloud applications. Defender for Cloud Apps keeps you in control through comprehensive visibility, auditing, and granular controls over your sensitive data.
- Defender for Cloud Apps has tools that help uncover shadow IT and assess risk while enabling you to enforce policies and investigate activities. It helps you control access in real time and stop threats so your organization can more safely move to the cloud.

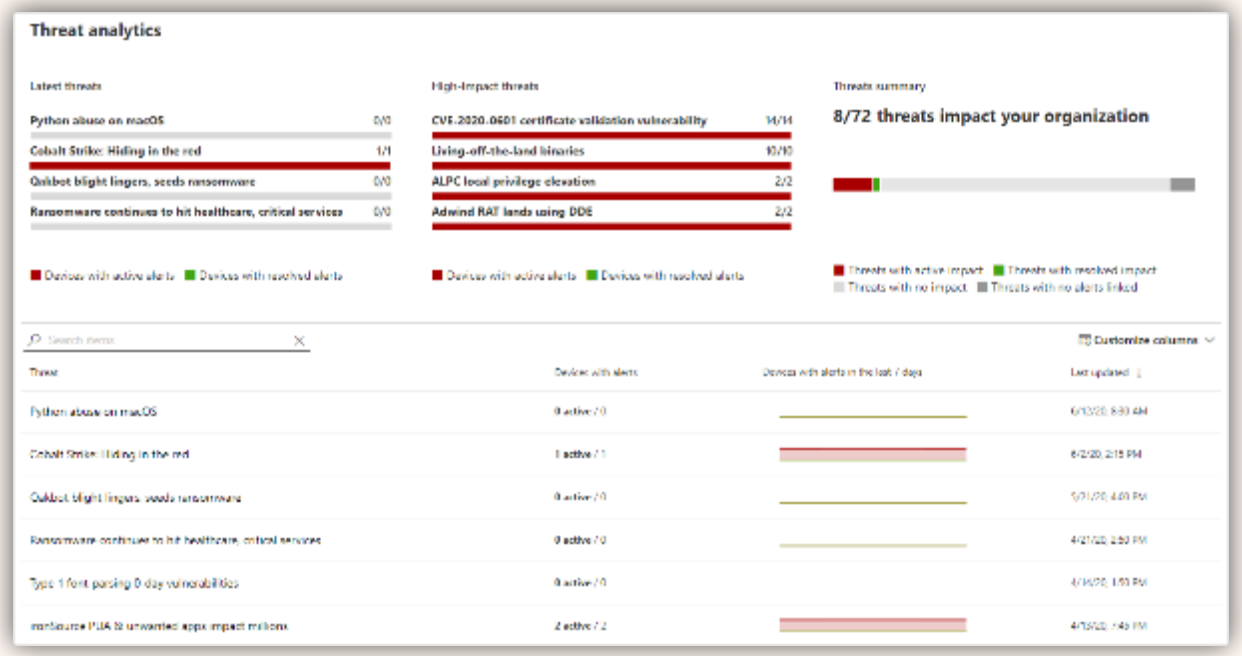


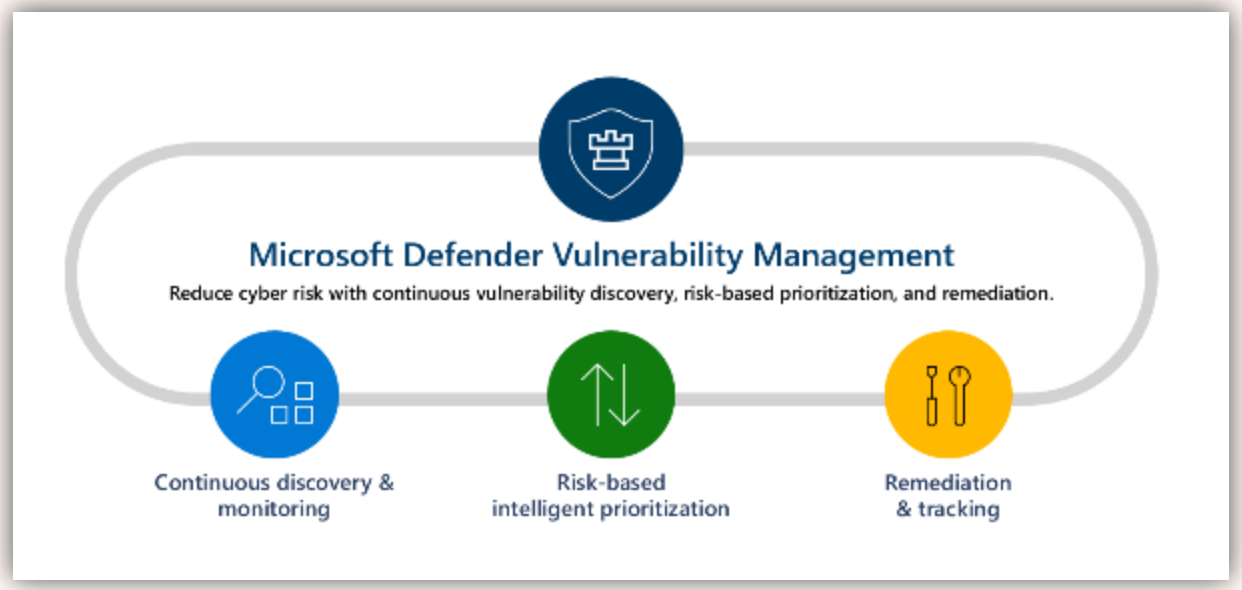
More information on [Defender for Cloud Plan 2]

Threat & Vulnerability Management

Linking to points 3.1, 11.7 of Normenkader-IBP

- With more sophisticated adversaries and new threats emerging frequently and prevalently, it's critical to be able to quickly:
  - Assess the impact of new threats
  - Review your resilience against or exposure to the threats
  - Identify the actions you can take to stop or contain the threats
- Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools. Using 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.



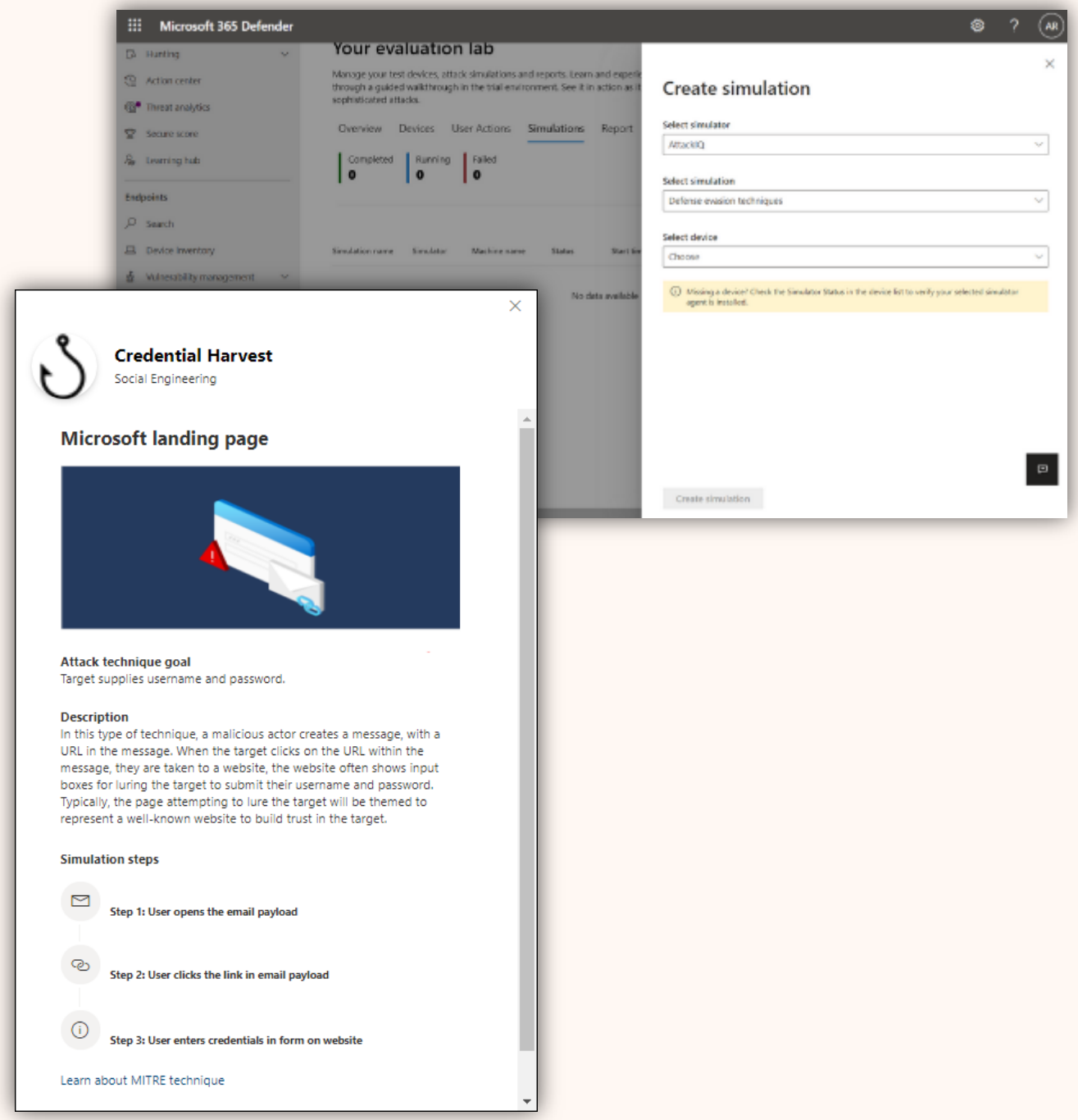


More information on [Microsoft Defender]

Attack simulation

Linking to points 3.1, 4.6 of Normenkader-IBP

- 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.
- These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

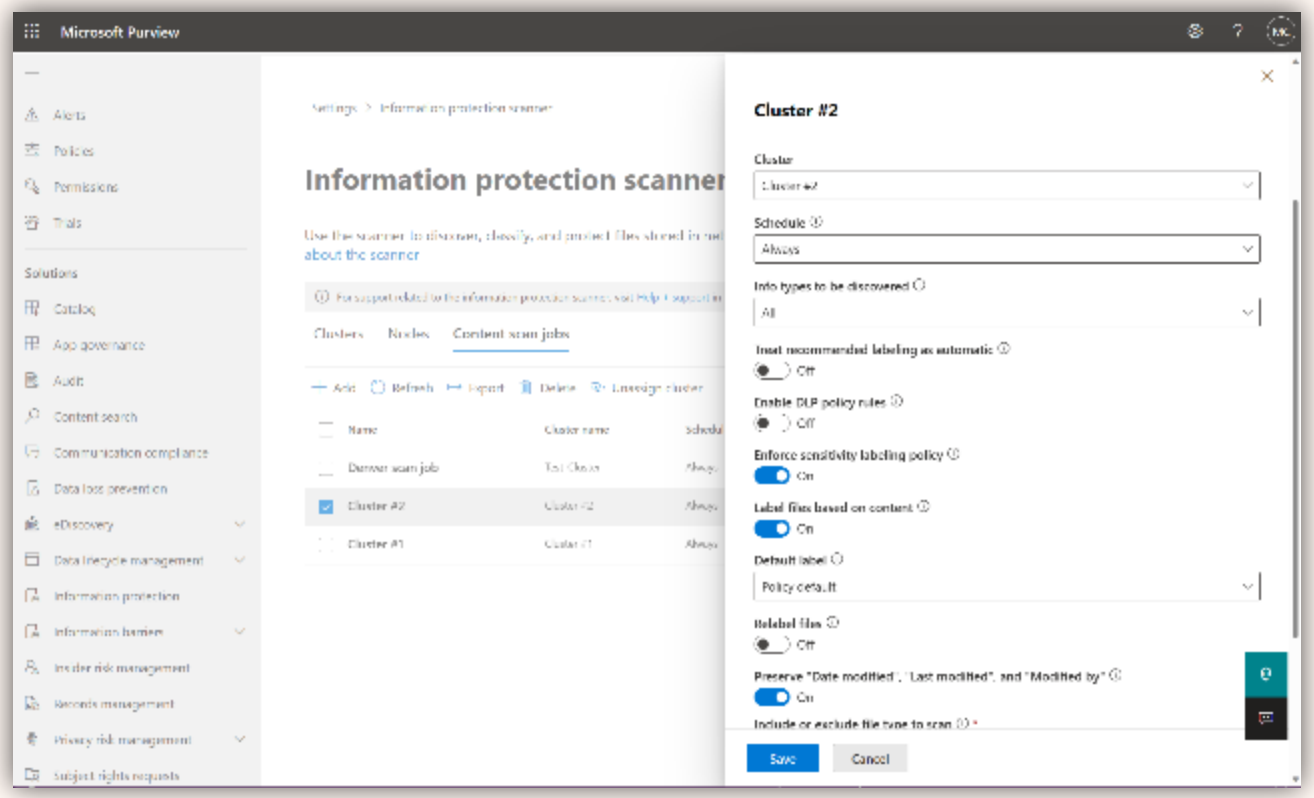


More information on [Attack simulator]

Azure Information Protection (AIP)

Linking to point 9.6 of Normenkader-IBP

- Azure Information Protection (AIP) is part of Microsoft Purview Information Protection (formerly Microsoft Information Protection or MIP). Microsoft Purview Information Protection helps you discover, classify, protect, and govern sensitive information wherever it lives or travels.
- AIP extends the labeling and classification functionality provided by Microsoft Purview with the following capabilities:
  - The unified labeling client
  - An on-premises scanner
  - The SDK

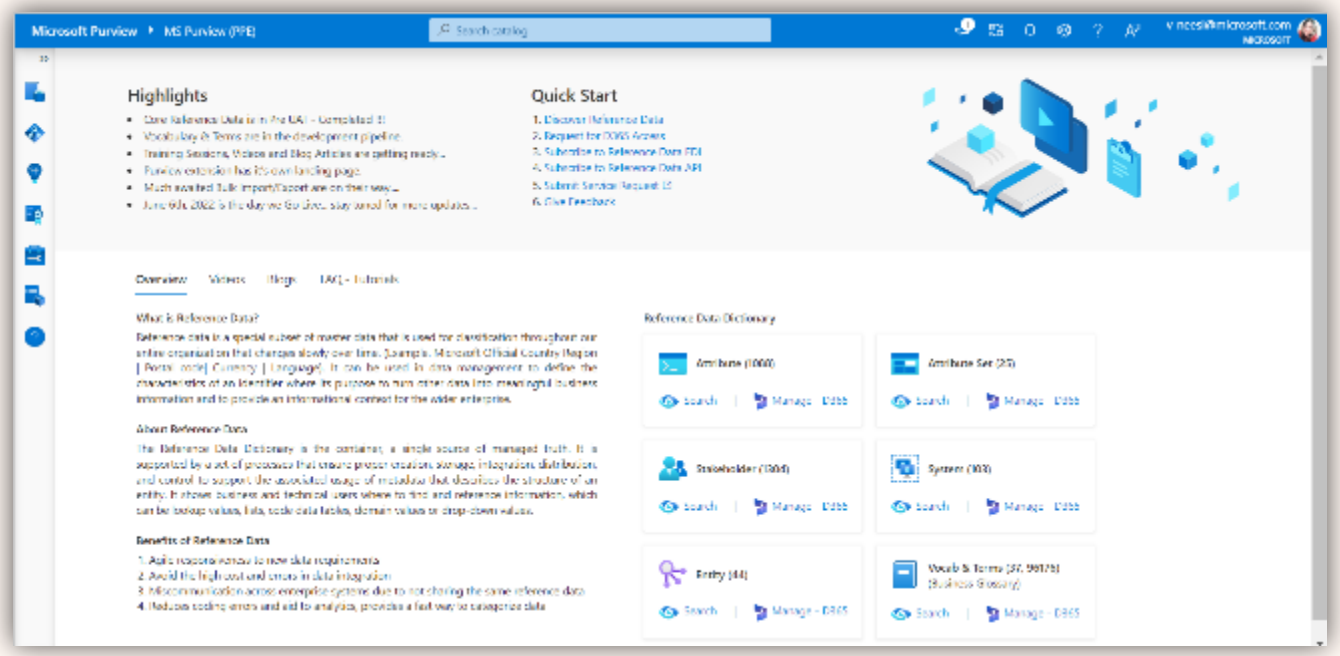


More information on AIP

Microsoft Purview

Linking to points 4.2, 6.3 9.2, 9.3, 9.4, 9.5, 9.6 of Normenkader-IBP

- Microsoft Purview solutions provide integrated coverage and help address the fragmentation of data across organizations, the lack of visibility that hampers data protection and governance, and the blurring of traditional IT management roles.
- Microsoft Purview combines the former Azure Purview and Microsoft 365 compliance solutions and services together into a unified platform to help your organization:
  - Gain visibility into data across your organization
  - Safeguard and manage sensitive data across its lifecycle, wherever it lives
  - Govern data seamlessly in new, comprehensive ways requirements

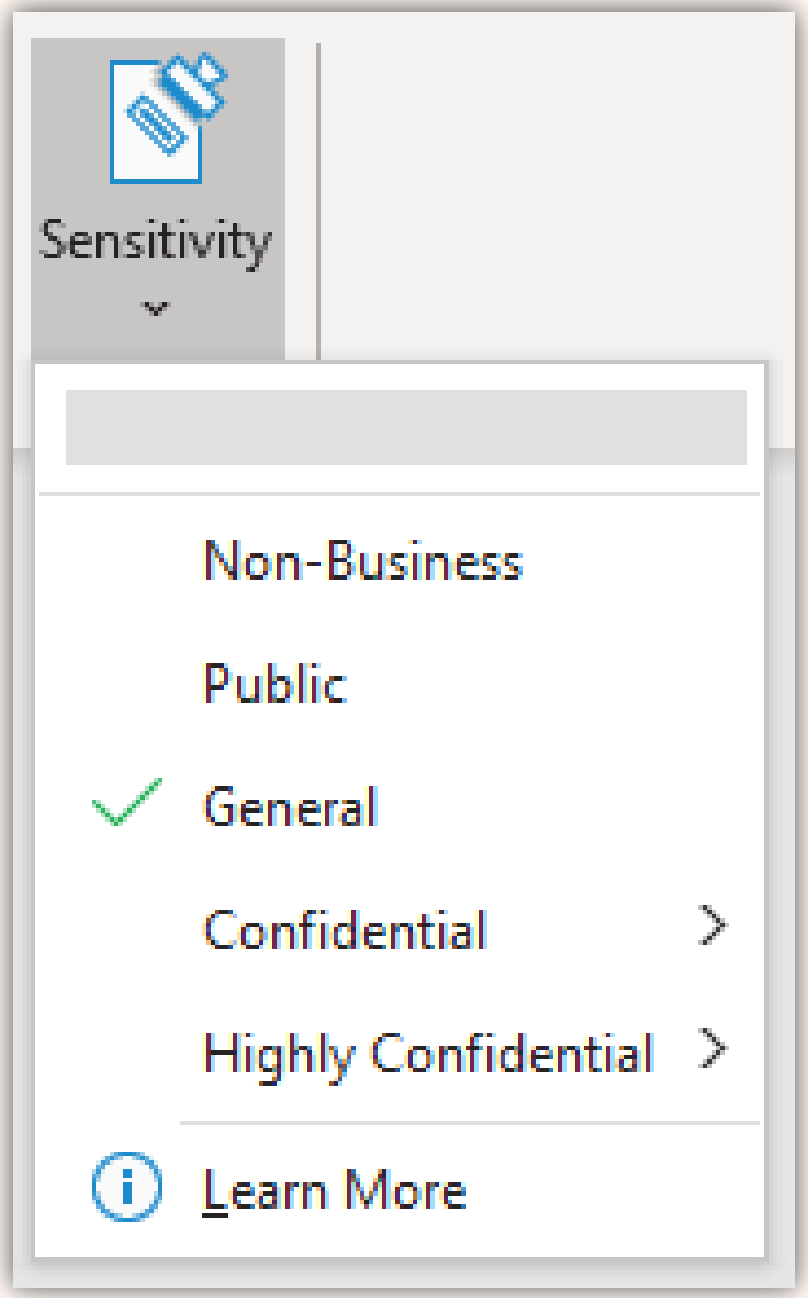


More information on [Microsoft Purview]

Information protection and labeling

Linking to points 9.2, 9.3, 9.4 of Normenkader-IBP

- 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.
- Microsoft Purview Information Protection helps 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.



More information on Sensitivity labels

Microsoft

Microsoft 365 Modern Workplace licensing

Microsoft 365 A5 adds incremental value to Microsoft 365 A3 across these solution areas

Security

Extends identity and threat protection to help stop damaging attacks with integrated and automated security

Compliance

Brings together information protection & advanced compliance capabilities to protect and govern data while reducing risk

Meetings & Calling

Adds audio conferencing and calling capabilities in the cloud to enable your teams

Analytics

Adds Power BI capabilities that help you realize significant business value from your data

Overzicht: [Microsoft 365 Education - Service Descriptions | Microsoft Learn]

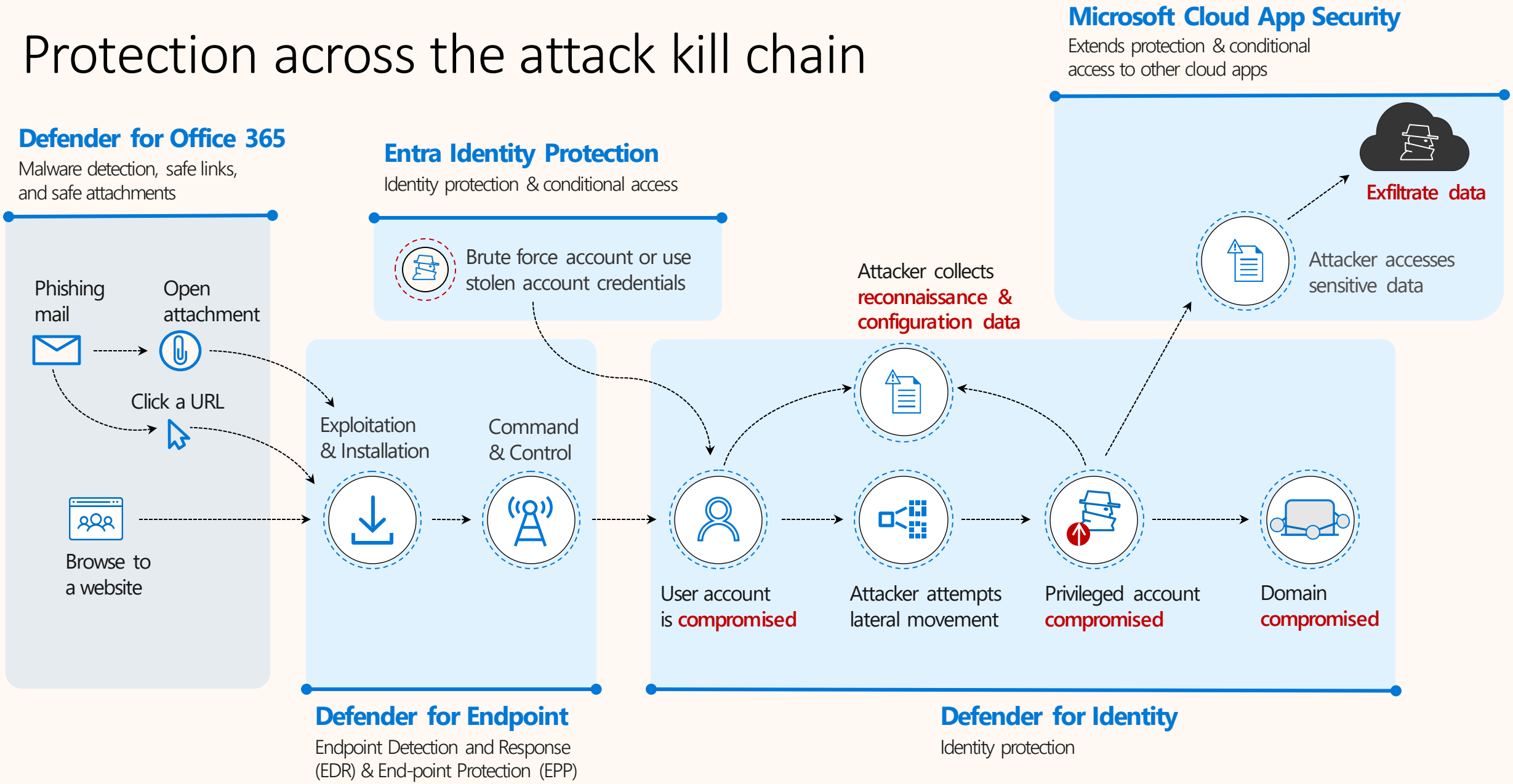
M365 A5 Security

Bestaat uit:

- MDO Plan 1 (is onderhandeld in SURF contract)
- MDO Plan 2 (Attack Simulation and Automated Investigation and Response)
- Entra ID Plan 2 (Conditional Access, PIM, Identity Protection, MFA registration)
- Defender for Identity & Defender for Cloud Apps
- MDE P2 en voor alle duidelijkheid: Automated investigation & remediation, EDR, MS Threat Experts, Sandbox Deep analysis, Threat Analytics, Threat & Vulnerability Management

Management and security	Microsoft 365 A1 for devices	Microsoft 365 Education A3 Student Use Benefit	Microsoft 365 Education A5 Student Use Benefit	Microsoft 365 Education A3	Microsoft 365 Education A5
Microsoft Defender for Office 365[10] Plan 2	No	No	Yes	No	Yes
School Data Sync	Yes	Yes	Yes	Yes	Yes
Intune for Education[6]	Yes	Yes	Yes	Yes	Yes
Advanced Threat Analytics	No	Yes	Yes	Yes	Yes
Microsoft Defender Antivirus	No	No	No	Yes	Yes
Microsoft Defender Device Guard	No	No	No	Yes	Yes
Microsoft Defender for Identity[11]	No	No	Yes	No	Yes
Office 365 Cloud App Security	No	Yes	Yes	Yes	Yes
Microsoft Defender XDR for Cloud Apps	No	No	Yes	No	Yes
Microsoft Defender for Endpoint[12] Plan 1	No	No	No	Yes	No
Microsoft Defender for Endpoint[12] Plan 2	No	No	No	No	Yes
Remote Help	Yes	Yes	Yes	Yes	Yes

Protection across the attack kill chain



M365 A5 Compliance

Bestaat uit:

- Information Protection & Governance
  - O.a: Endpoint DLP, Trainable classifiers, Advanced Message Encryption, Teams DLP, Automatic Sensitivity labels
- Insider Risk Management
  - O.a: Customer Lockbox, PAM
- eDiscovery & Audit

Compliance	Microsoft 365 A1 for devices	Microsoft 365 Education A3 Student Use Benefit	Microsoft 365 Education A5 Student Use Benefit	Microsoft 365 Education A3	Microsoft 365 Education A5
Microsoft Purview Audit (Standard)	Yes	Yes	Yes	Yes	Yes
Microsoft Purview Audit (Premium)	No	No	No	No	Yes
Microsoft Purview Message Encryption (Basic)	Yes[9]	Yes[9]	Yes[9]	Yes	Yes
Microsoft Purview Advanced Message Encryption	No	No	No	No	Yes
Microsoft Purview Customer Lockbox	No	No	No	No	Yes
Microsoft Purview Insider Risk Management	No	No	No	No	Yes
Microsoft Purview Privileged Access Management	No	No	No	No	Yes

Compliance	Microsoft 365 A1 for devices	Microsoft 365 Education A3 Student Use Benefit	Microsoft 365 Education A5 Student Use Benefit	Microsoft 365 Education A3	Microsoft 365 Education A5
Office 365 Rights Management	Yes	Yes	Yes	Yes	Yes
Azure Information Protection Plan 1	No	No	No	Yes	No
Azure Information Protection Plan 2	No	No	No	No	Yes
Litigation Hold	No	Yes	Yes	Yes	Yes
Content search	Yes	Yes	Yes	Yes	Yes
Microsoft Purview eDiscovery (Standard) (including Hold and Export)	No	Yes	Yes	Yes	Yes
Microsoft Purview eDiscovery (Premium)	No	No	No	No	Yes
Microsoft Purview Data Loss Prevention for email and files	Yes	Yes	Yes	Yes	Yes
Endpoint data loss prevention or DLP	No	No	No	No	Yes
Communications DLP (Teams chat)	No	No	No	No	Yes
Microsoft Purview Communication Compliance	No	No	No	No	Yes
Microsoft Purview Customer Key	No	No	No	No	Yes

Zelf aan de slag met het Normenkader

Er zijn verschillende stappen te doorlopen:

- Waar sta je nu?
- Wat heb ik precies nodig om te voldoen aan het Normenkader?
- Welke resources heb ik daarvoor nodig?

Cybersecurity Assessments with CSAT

Provide a **holistic view of the cybersecurity position** together with fact-based recommendations based on an internationally recognized **cybersecurity framework**.

CSAT collects and analyzes data from the **hybrid IT environment** in a short period of time to provides **data-driven recommendations**.

CloudLab **identifies cost saving** elements to help organizations finance their security improvements and cloud migrations.

Data areas from hybrid environment:

- Identities
- Workstations and Servers
- Infrastructure
- (Cloud) Applications
- Data
- Threat protection
- Policies and Processes

Deliverables:

- Company score based on CIS controls v8
- Mapping to NIS 2.0 European guidelines
- Migration plans to improve cybersecurity based on the Zero Trust Architecture
- Urgent Action Items and Quick Wins
- Risk-based action plan with improvement actions
- Total Cost of Ownership for Security and other relevant topics; e.g., Azure Migrate

Outcomes drive:

- Microsoft 365
  - All A5 SKUs
- Azure Migrations
- Azure Security
  - All Azure Security SKUs
- AVD & W365
- 3rd party security products
- Dynamics 365

Normenkader Deepdives SLB Diensten ism Microsoft

Dank jullie wel