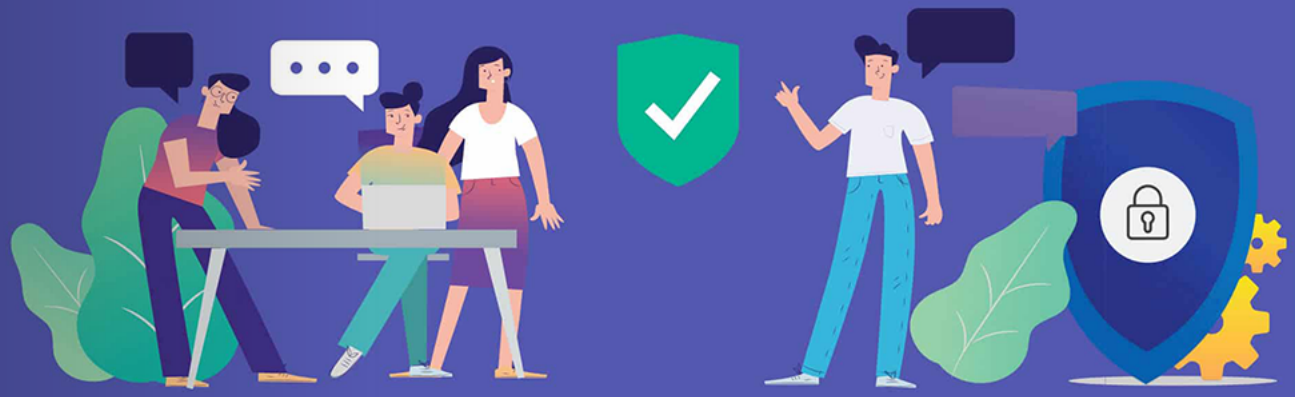
Microsoft 365 Tenant-Security

Verstehen. Anwenden. Absichern.



Über Marco

- Marco Schmittnägel
- SharePoint seit 2008
- Microsoft Cloud seit 2012
- Architektur, Beratung, Umsetzung
- Schwerpunkte aktuell
  - Tenant Architekturen
  - Teams, SharePoint, OneDrive
  - Machine Learning / AI

Über Bernd

- Bernd Jahn
- Seit 2018 in der IT
- Seit 2020 im Cloud-Umfeld
- Information Security Officer
- M365 Security Expert
- AvePoint Certified Specialist

LANSCO

Das (medienwirksame) Thema mit der Sicherheit

Resentful employee deletes 1,200 Microsoft Office 365 accounts, gets prison

https://www.bleepingcomputer.com/news/security/resentful-employee-deletes-1-200-microsoft-office-365-accounts-gets-prison/

AI Attacks Surge as Microsoft Process 100 Trillion Signals Daily

https://www.infosecurity-magazine.com/news/microsoft-process-100-trillion/

Deutschland mit am meisten von Cyberangriffen betroffen

Deutschland lag zuletzt laut einem Microsoft-Bericht weltweit an vierter Stelle der von Cyberangriffen betroffenen Staaten. Länder wie Russland weiteten diese aus.

https://www.zeit.de/digital/internet/2025-10/microsoft-bericht-cyber-sicherheit

Microsoft Patches Critical Entra ID Flaw Enabling Global Admin Impersonation Across Tenants

https://thehackernews.com/2025/09/microsoft-patches-critical-entra-id.html

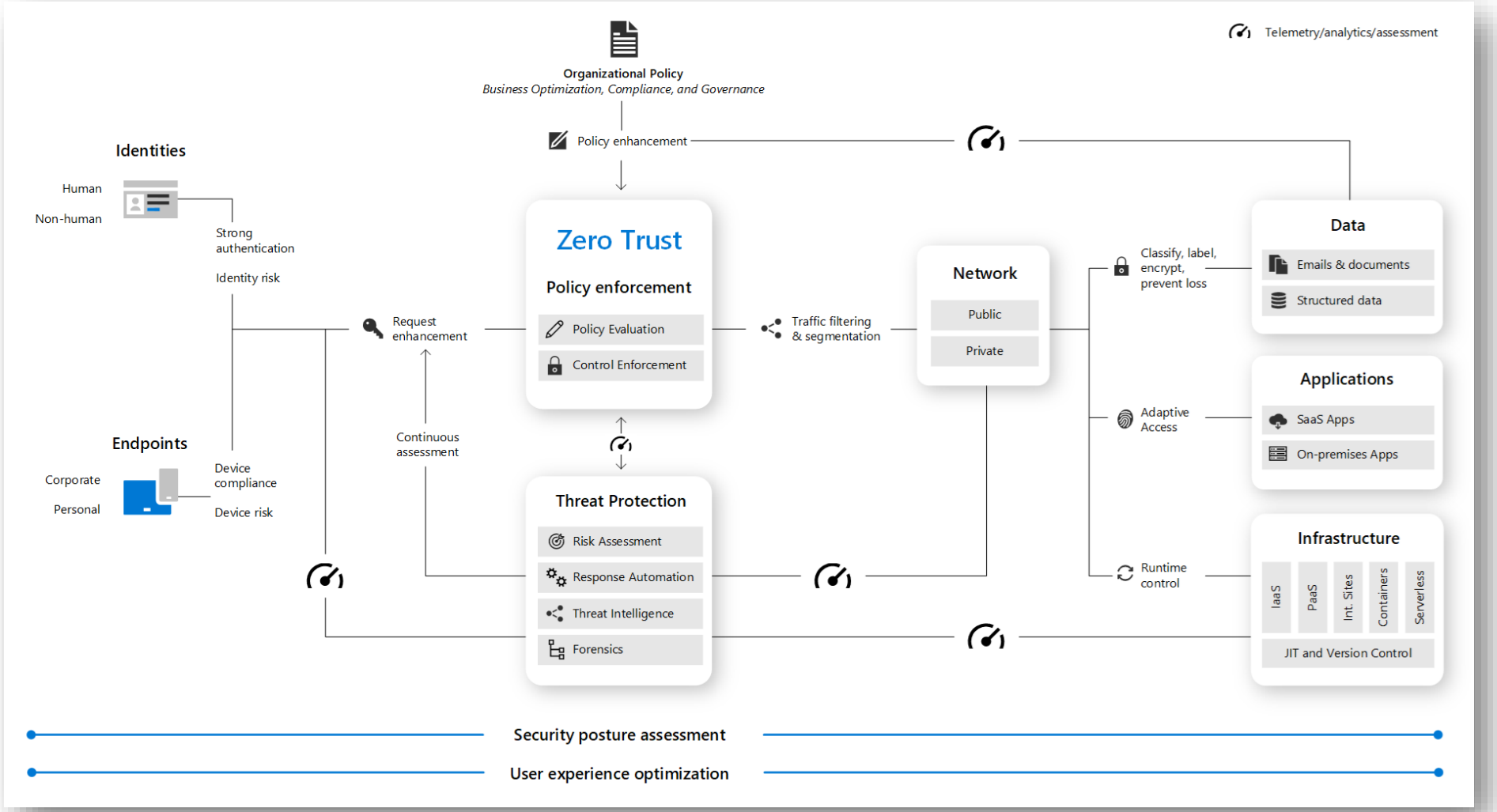
Was ist anders als früher?

Angriffe können durch Automatisierung und neuerdings durch KI nahezu grenzenlos skaliert werden.

Gleichzeitig steigt deren Komplexität so weit, dass sie oft nur noch durch hochspezialisierte Experten oder Systeme erkannt und abgewehrt werden können.

LANSCO

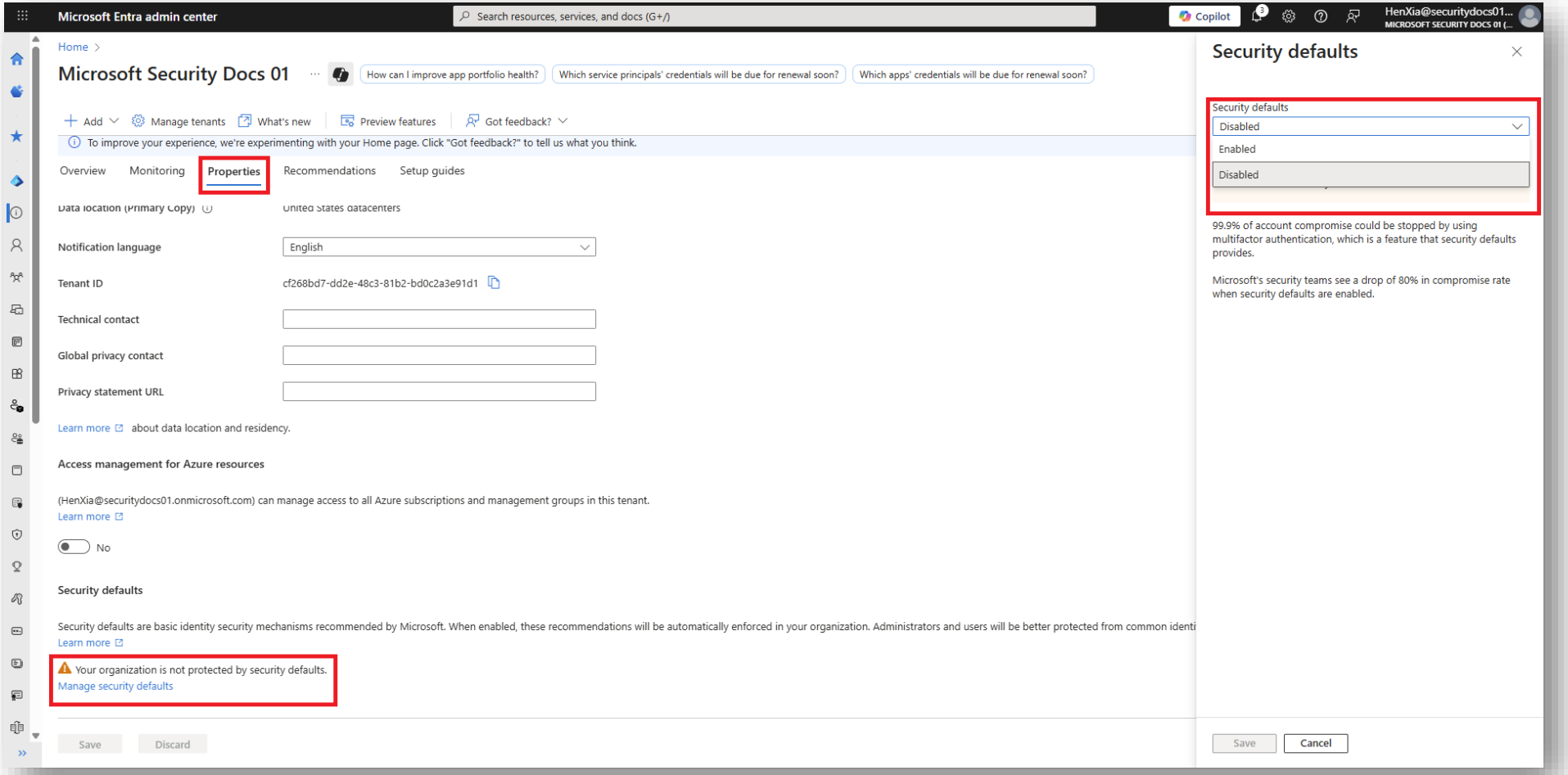
Sicherheitsarchitektur zu Zeiten von Cloud und KI



https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust

LANSCO

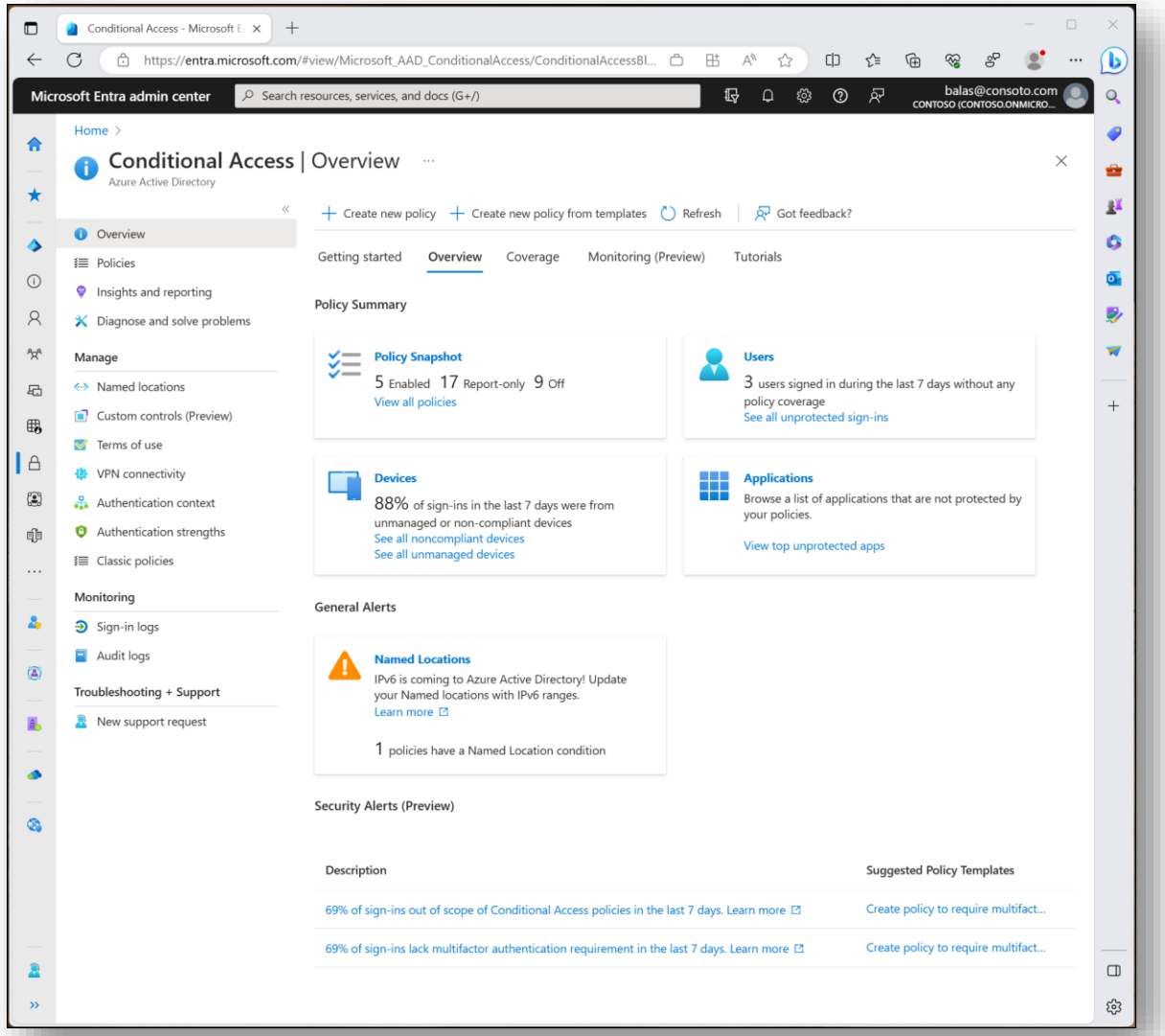
Security Defaults als Ausgangspunkt



➔ Multifaktor-Authentifizierung + Alte Protokolle ausschalten + Admin-Funktionen zusätzlich absichern

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

Conditional Access als die Grundlage, es richtig zu machen



Enthalten in:

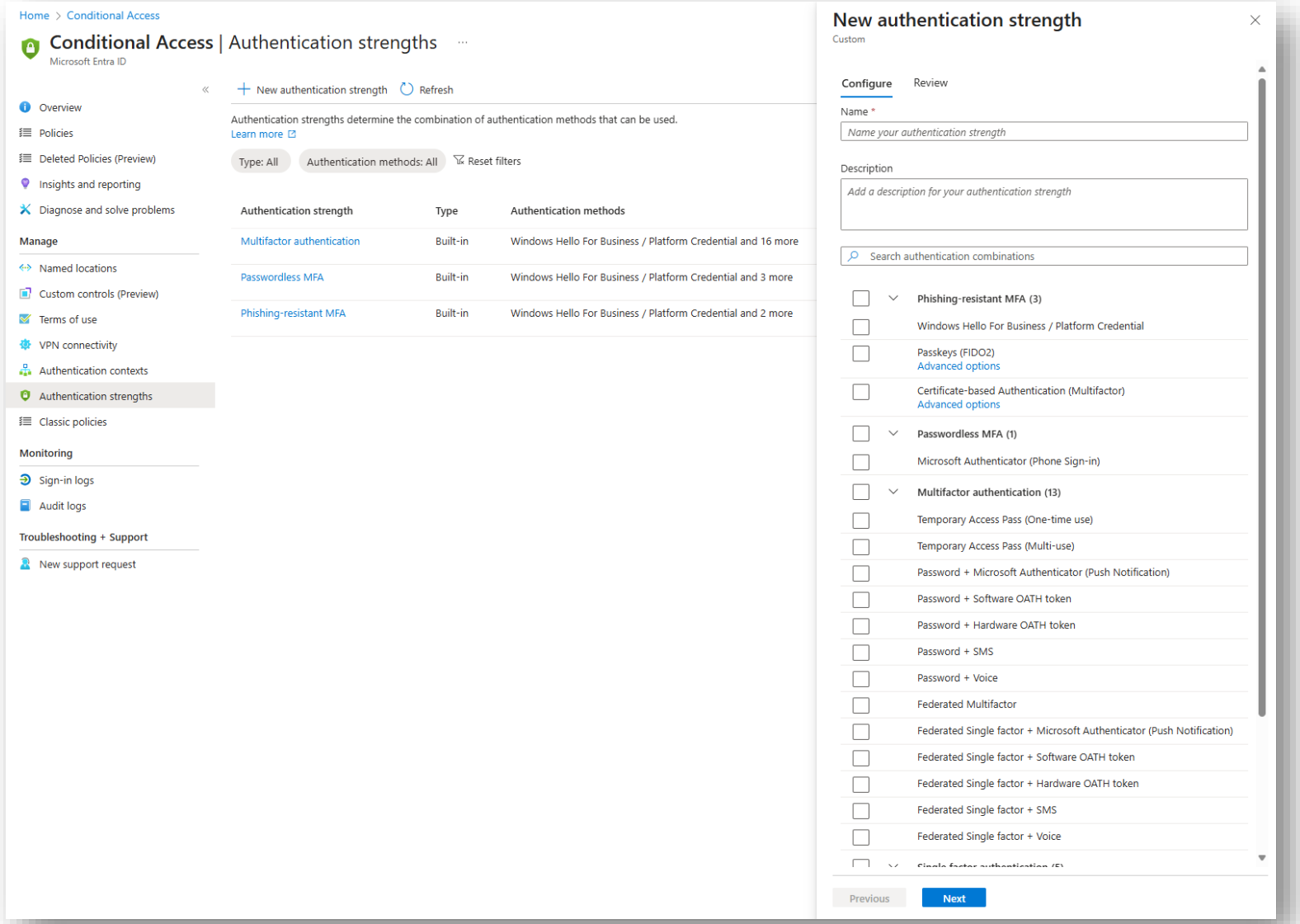
- Entra ID P1
- Microsoft 365 Business Premium
- Microsoft 365 F1 / F3
- Microsoft 365 E3 / E5
- Microsoft 365 A3 / A5

(NICHT enthalten in Office 365-Plänen)

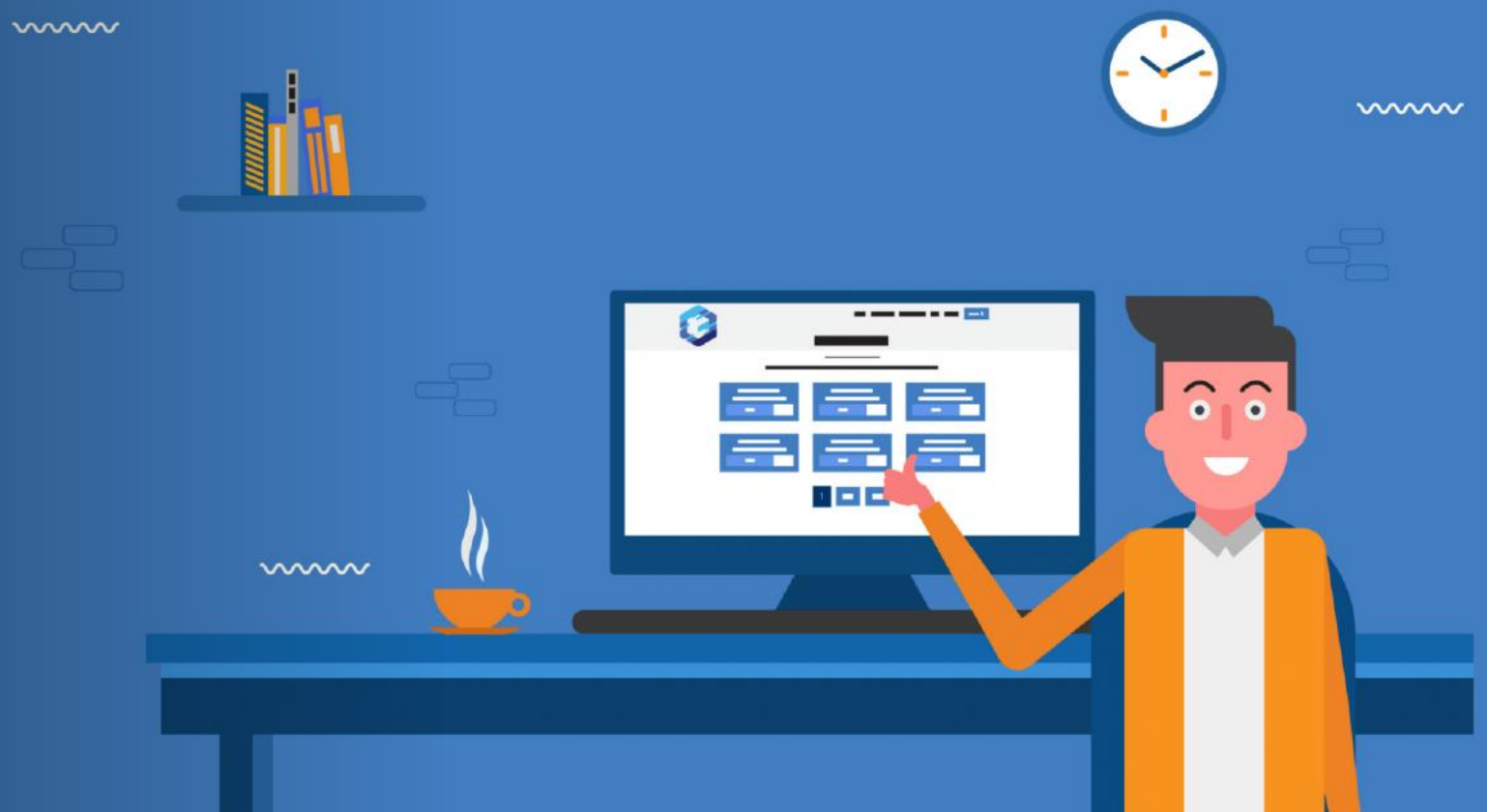
https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

LANSCO

Unterschiedliche Authentifizierungsstärken anwenden



Gäste & Conditional Access

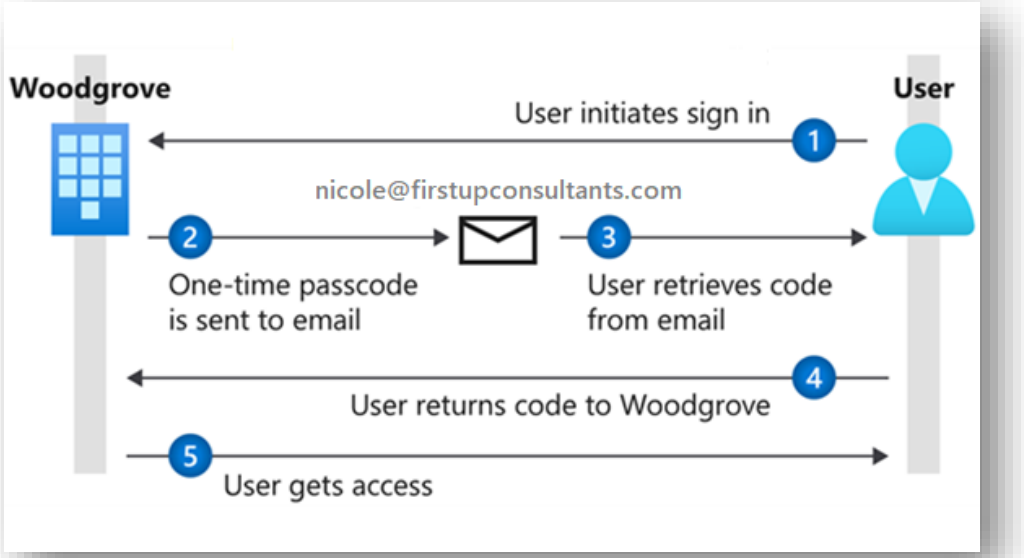


Demo

LANSCO

Hinweis zu der Teilen-Funktion & Gästen

Früher wurde die Absicherung beim Teilen von Dateien und Ordnern über SharePoint geregelt.



Empfehlung:
Aktivierung der auf Entra B2B Integration, wobei dadurch einmalig alle alten Links kaputt gehen.

https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration
https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode

Benutzertypen gezielt sichern

Wie viel Sicherheit darfs denn sein?

LANSCO

Umgang mit unterschiedlichen Benutzertypen

Endbenutzer

- Größter Schulungsbedarf
- Größte Angriffsfläche
- MFA verpflichtend
- Ziel: Passwordless

Externe Benutzer

- Zugriff begrenzt
- Regelmäßig aufräumen
- MFA verpflichtend

Servicebenutzer

- Stattdessen Workload Identities nutzbar?
- MFA und Nutzung begrenzen

Privilegierte Benutzer

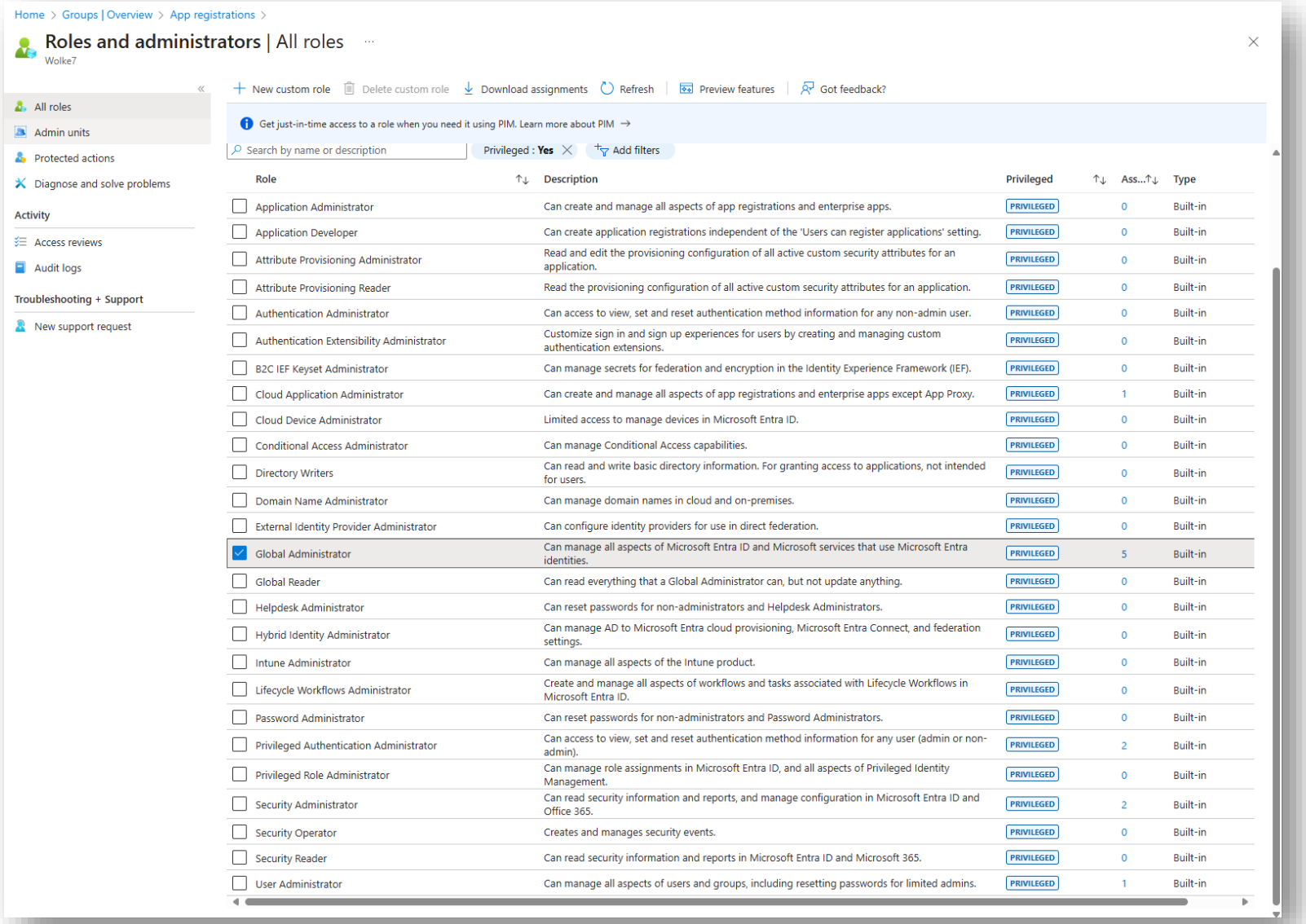
- PIM nutzen
- Maximal starke Authentifizierung
- Nutzung begrenzen

Sonstige

- z.B. Shared Mailboxes
- Individuell entscheiden
- Nach Möglichkeit deaktivieren

LANSCO

Die Gefahr durch privilegierte Benutzer



Getrennte Benutzerkonten für Administratoren

Administratoren leben in zwei Welten:

- Normale Tätigkeiten als Endbenutzer (z.B. Mails)
- Administrative Tätigkeiten

➔ Gleicher Benutzer = Größere Angriffsfläche

Getrennte Benutzerkonten für Administratoren

Endbenutzer-Konto:

- Standard-Lizenzierung
- MFA (idealerweise Passwordless)
- Endbenutzer-Berechtigungen auf Inhalte und Funktionen

Administrator-Konto:

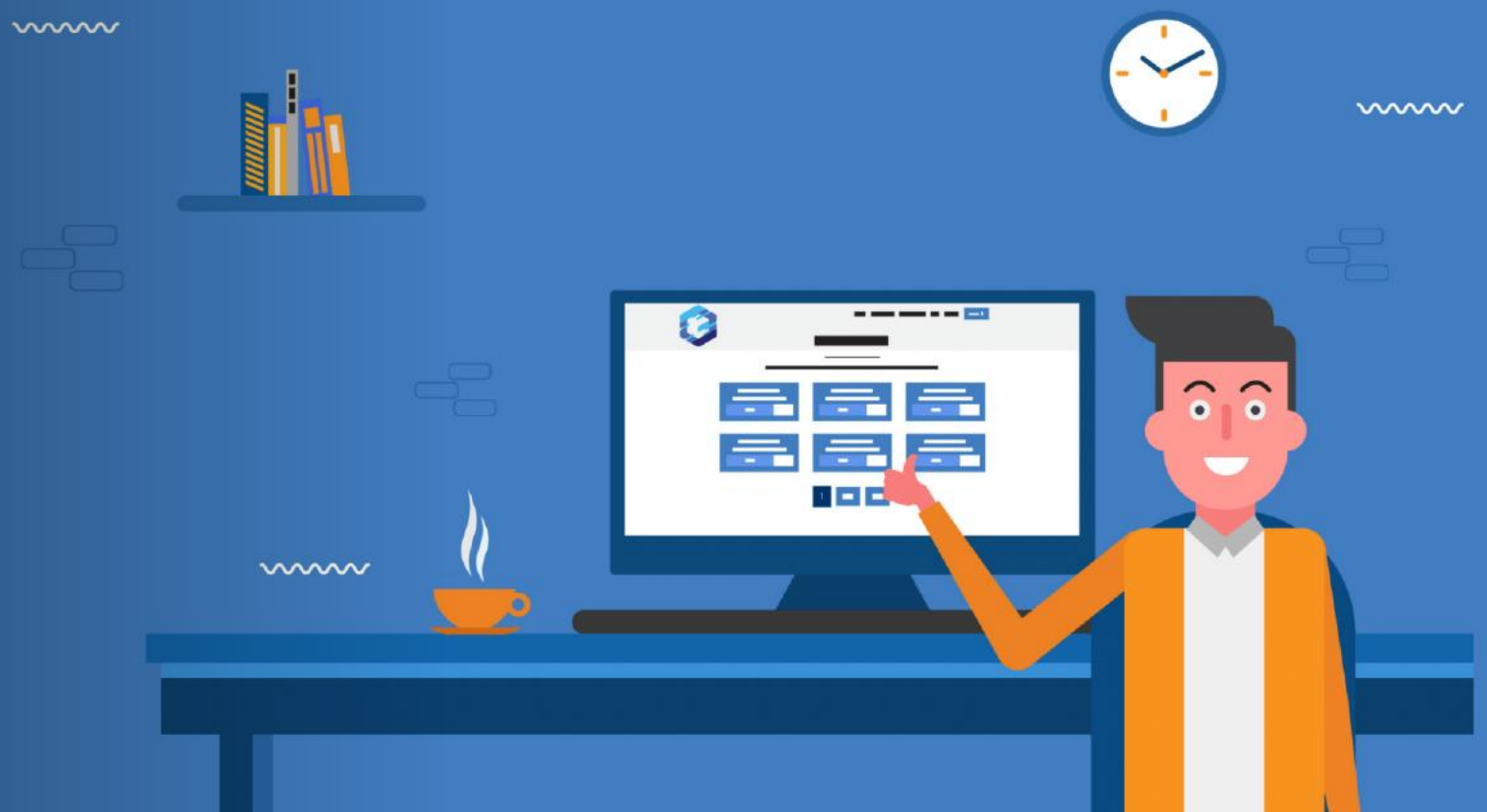
- Idealerweise Entra ID P2 oder E5
- Phishing-resistant MFA
- Keine dauerhaften Berechtigungen auf Inhalte
- Ausschließlich für administrative Tätigkeiten – aktiviert durch PIM

PIMst du schon?

Privileged Identity Management ermöglich es, dass administrative Berechtigungen nur bei Bedarf aktiviert und ggf. genehmigt werden müssen.

➔ Selbst wenn das Admin-Konto kompromittiert wird, darf es zunächst nichts

Privileged Identity Management



Demo

Break Glass Accounts für den Notfallzugriff

Gesonderte Benutzerkonten mit Global Admin Rolle, die nur im Notfall verwendet werden und deren Authentifizierungsinformationen nur wenigen vertrauenswürdigen Personen zugänglich sind (z.B. Safe oder Bankschließfach)

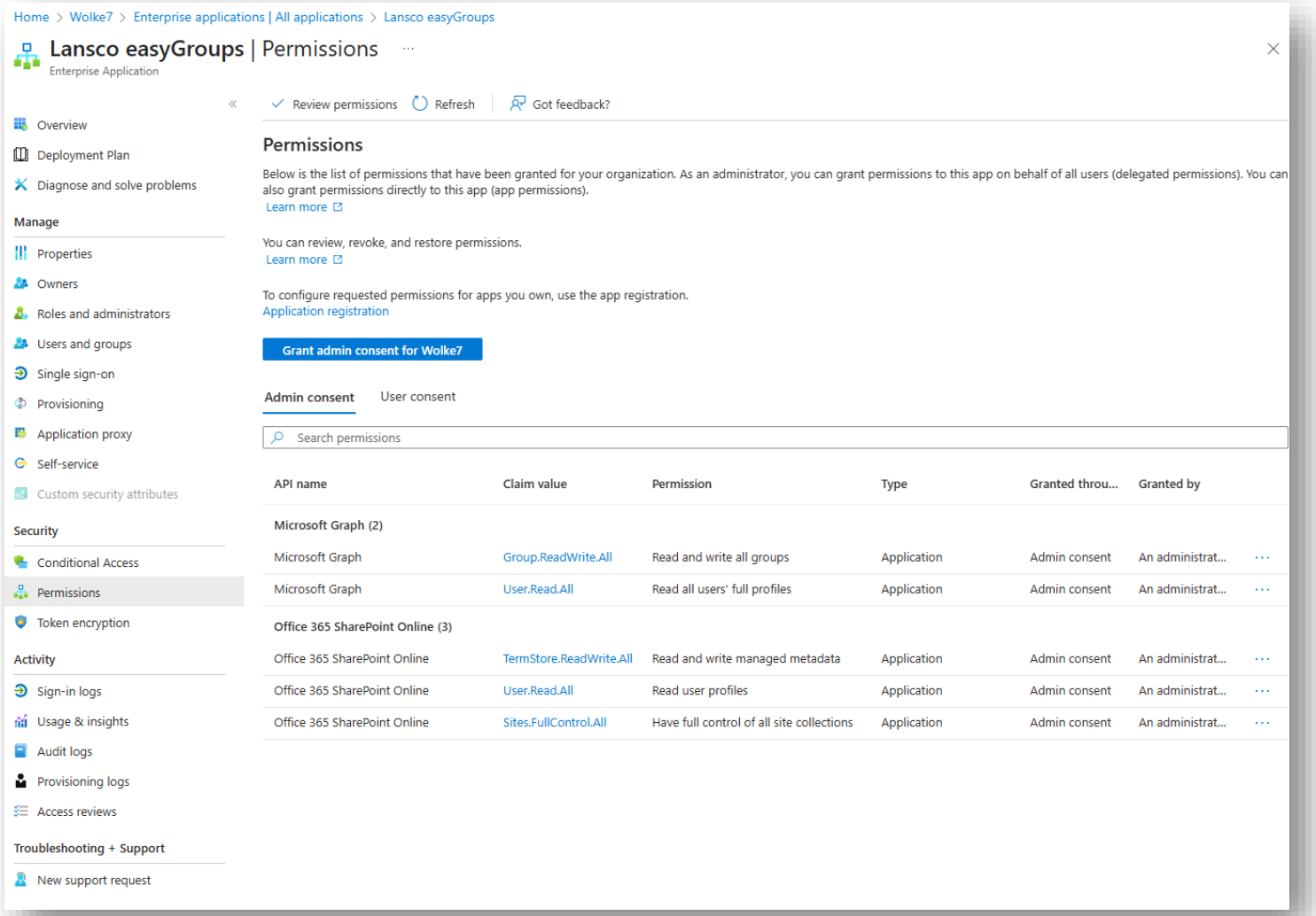
Gute Anleitung von Microsoft dazu: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access

Workload Identities

Zugriffe durch Dienste und Anwendungen

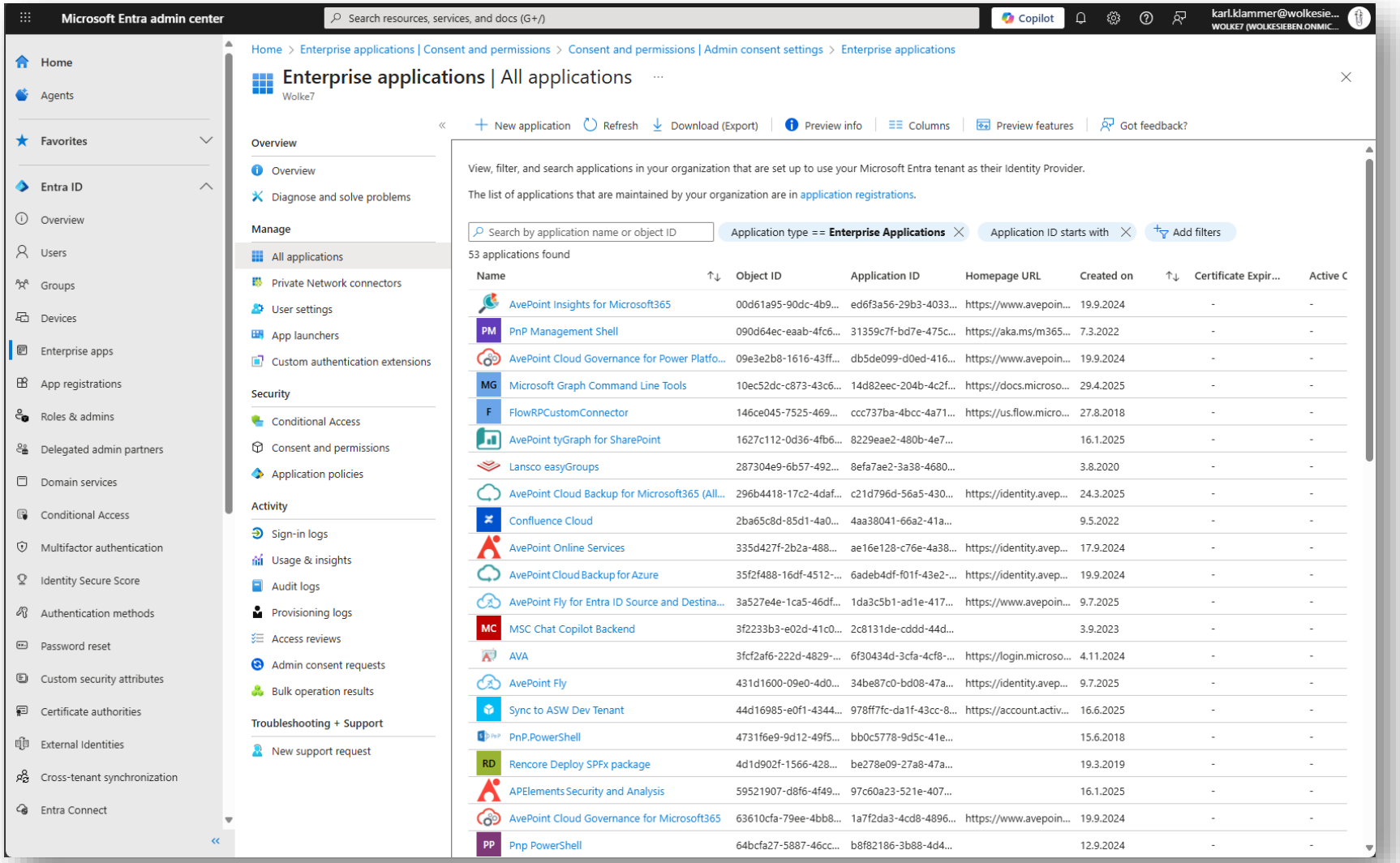
LANSCO

Workload Identity = Zugriff durch eine Anwendung auf unseren Tenant



LANSCO

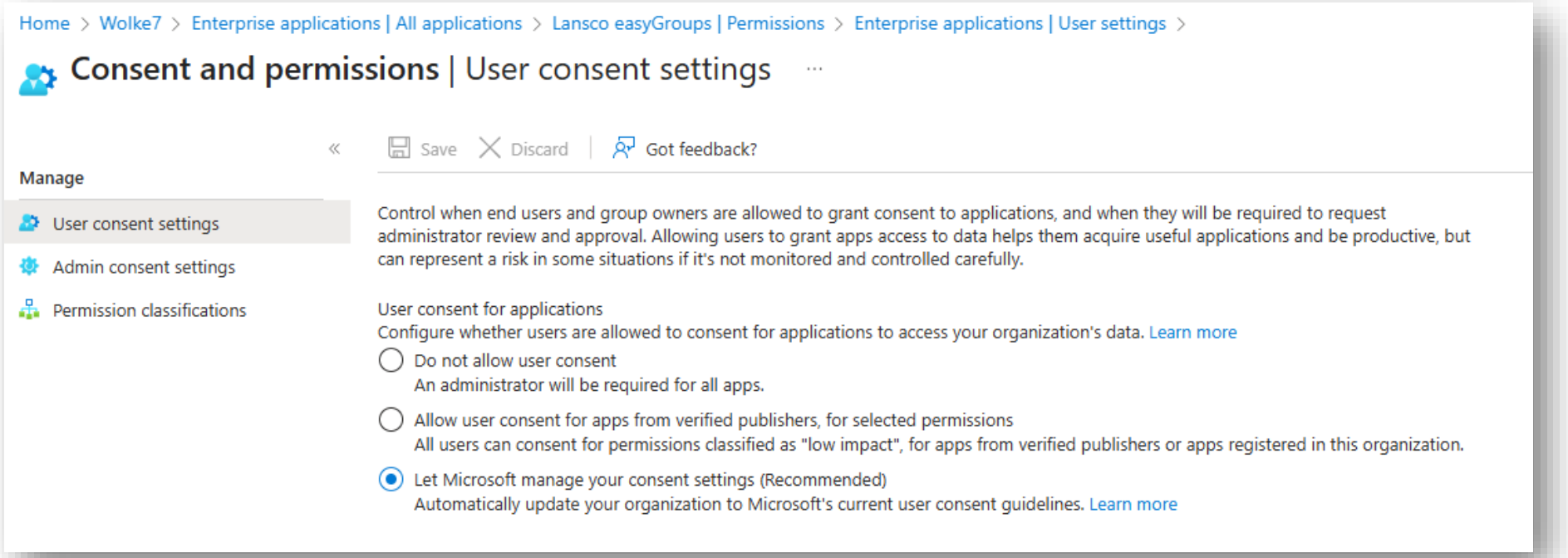
Workload Identities gezielt steuern und überwachen



https://learn.microsoft.com/en-us/entra/workload-id/workload-identities-overview

LANSCO

Consent für Workload Identities klar regeln



https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings

Was ist mit Device Management?

Device Management ist wie Identity & Access Management ein zentraler Bestandteil des Zero Trust-Modells.

Intune bietet eine sehr gute Integration in die restlichen Security-Funktionen der Microsoft Cloud.

Um nicht den Rahmen zu sprengen: Bei Interesse gerne melden ☺

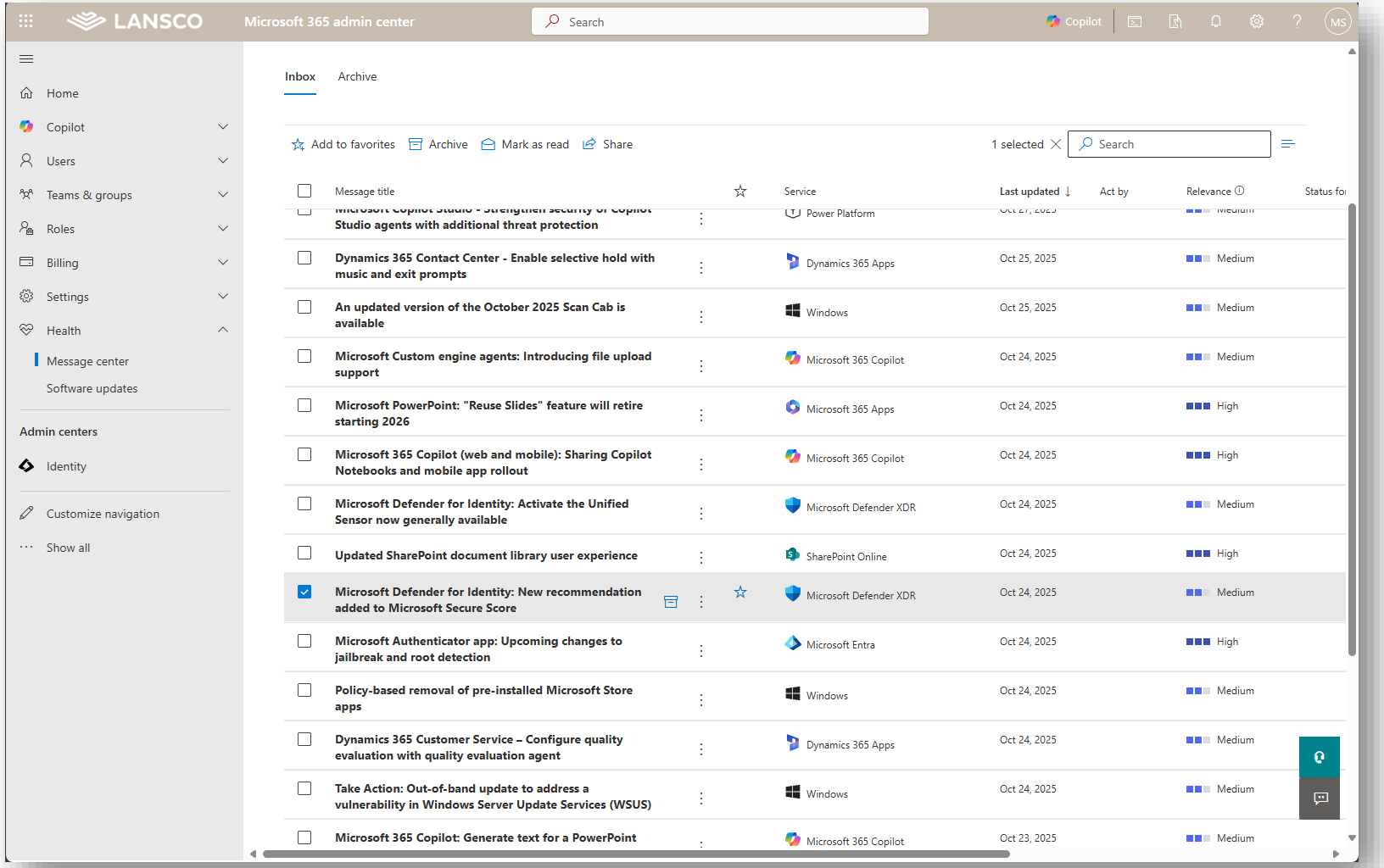
Evergreen Security

Prozesse für den laufenden Betrieb

Welche Prozesse sollten mindestens etabliert sein?

1. Lebenszyklus für Benutzerkonten
2. Lebenszyklus für Workload Identities
3. Verarbeitung des Message Centers
4. Überwachung des Secure Scores
5. Reaktion auf Security Alerts
6. Vorgehen für Forensik und Logsichtung
7. Vorgehen für Notfallzugriff

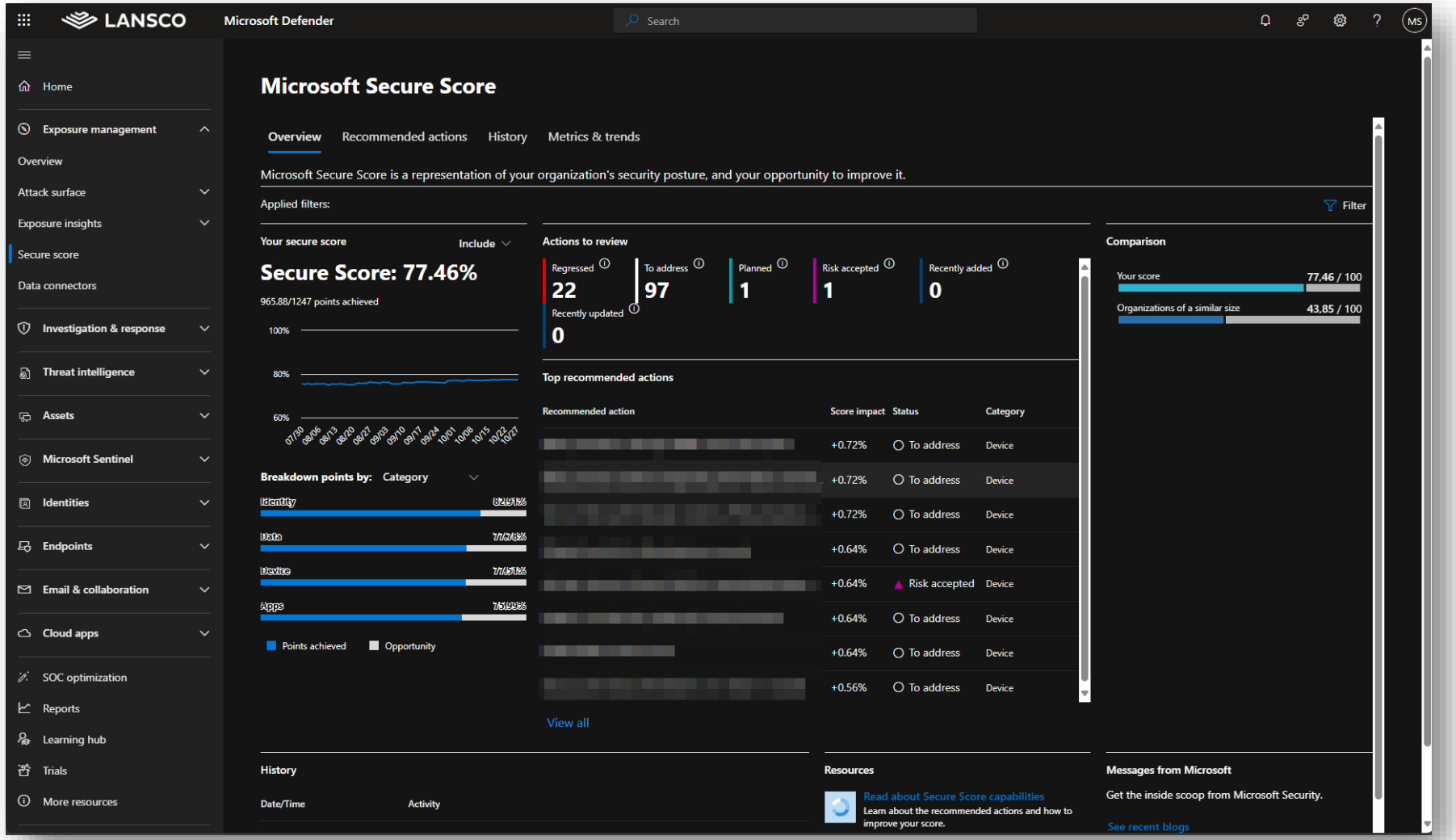
Message Center als Quelle für (sicherheitsrelevante) Neuerungen



https://admin.cloud.microsoft/?#/MessageCenter

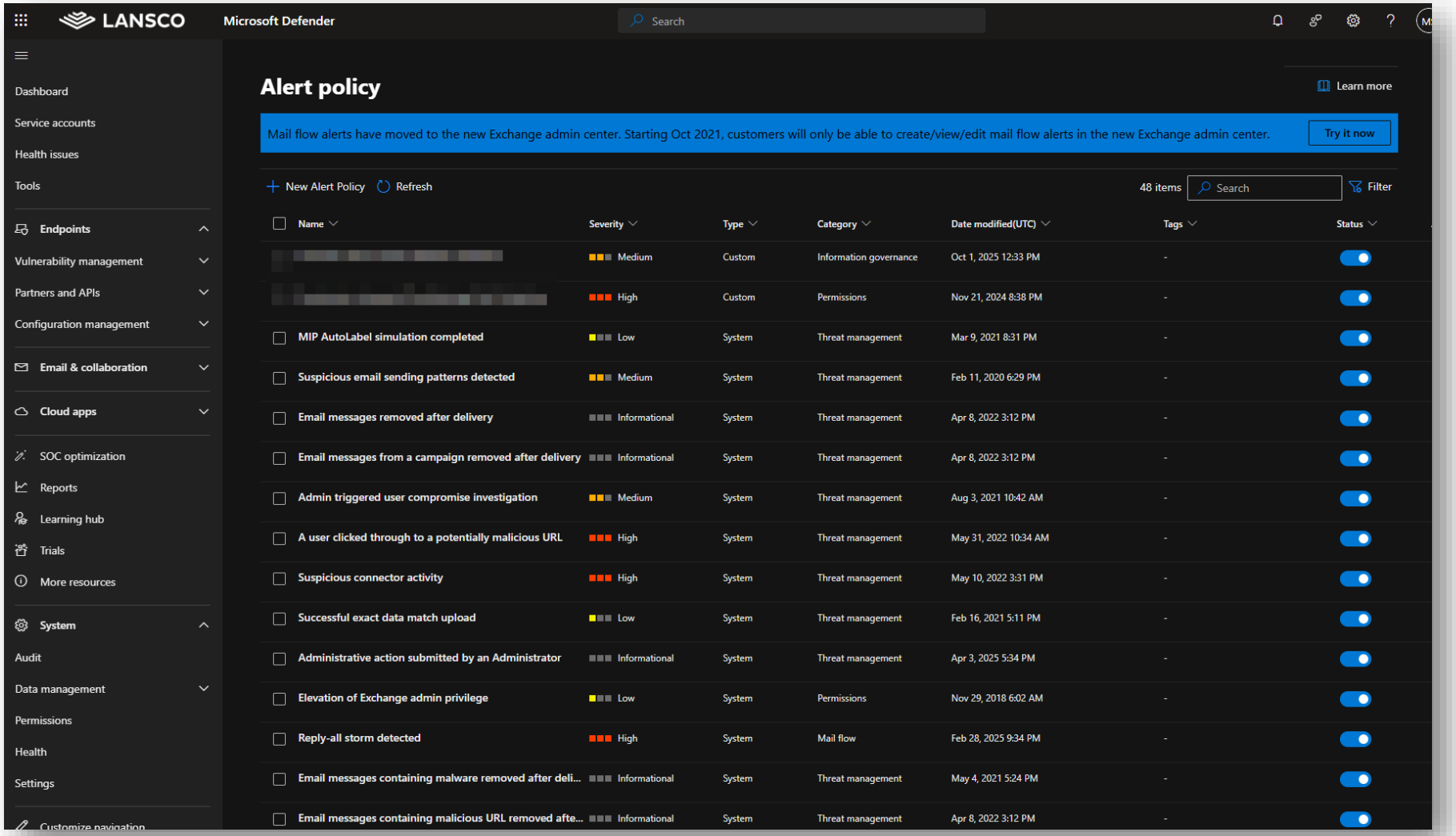
LANSCO

Secure Score als Metrik und Leitfaden für einen sicheren Tenant



https://security.microsoft.com/exposure-secure-score

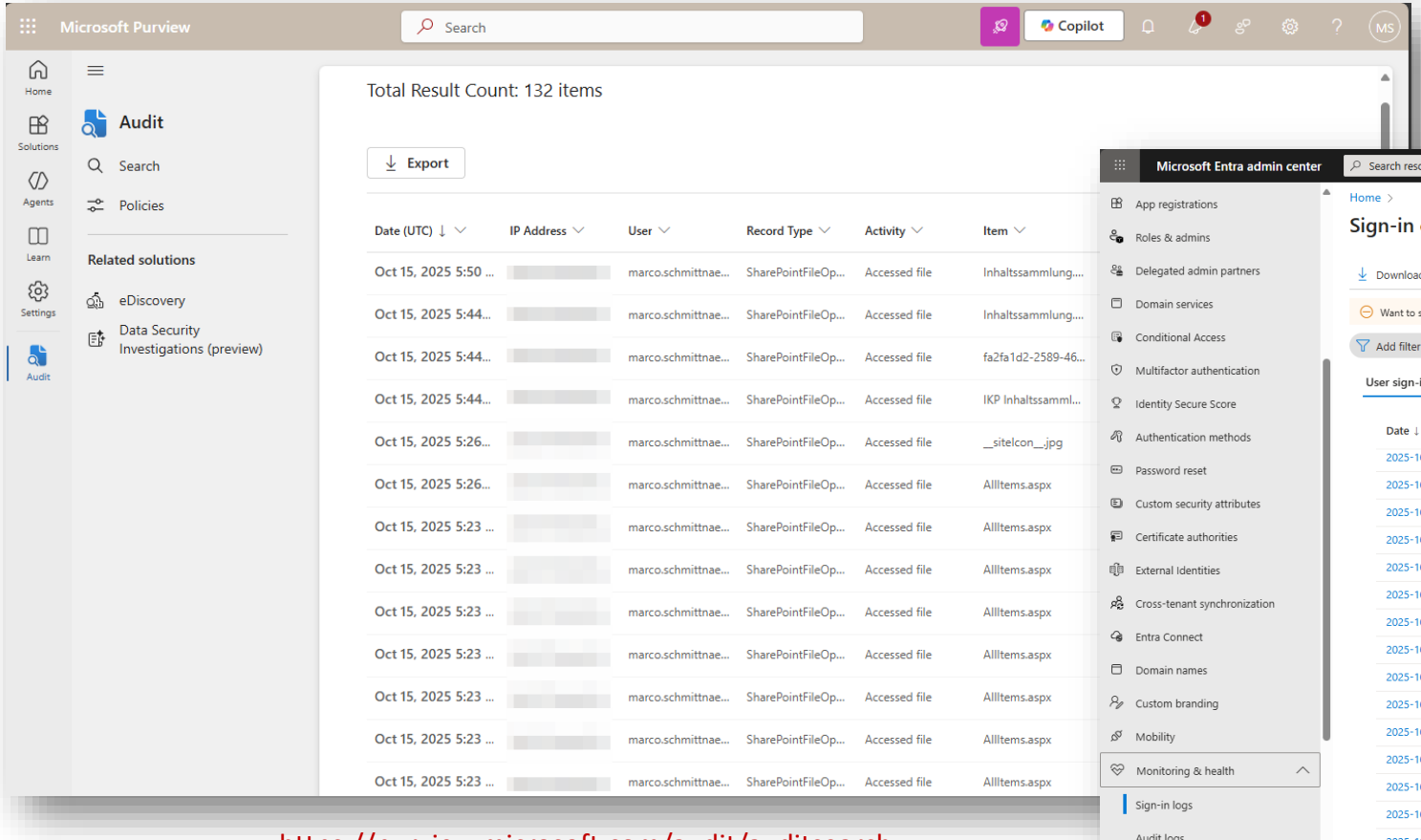
Alerts Policies nutzen



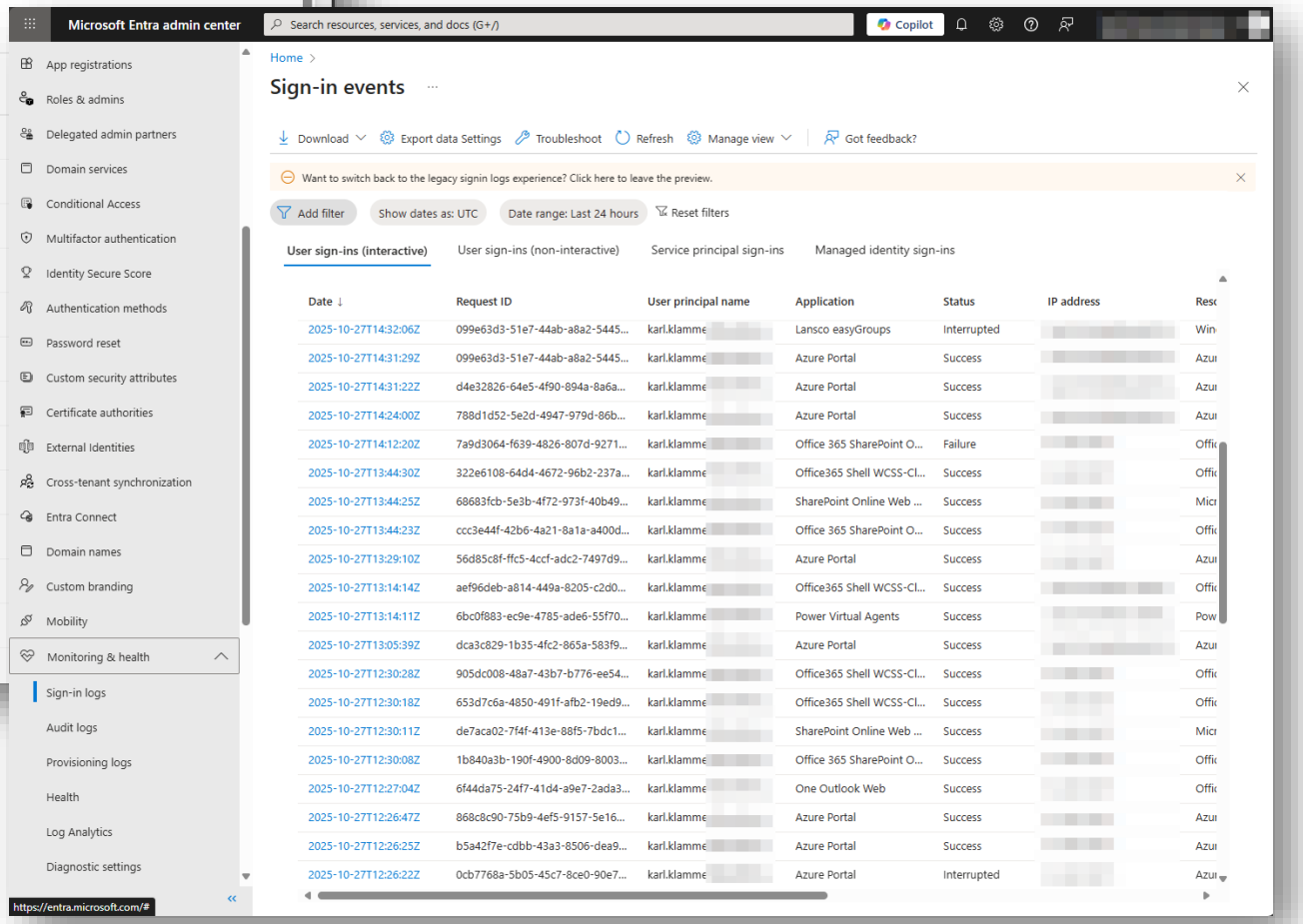
https://security.microsoft.com/alertpoliciesv2

https://learn.microsoft.com/en-us/defender-xdr/alert-policies

Audit- und Signin-Logs um Ereignisse nachzuvollziehen



https://purview.microsoft.com/audit/auditsearch



https://entra.microsoft.com/#view/Microsoft_AAD_IAM/SignInLogsList.ReactView

Wie könnt ihr konkret als nächstes tun?

1. Lizenzierung klären: Conditional Access für Endbenutzer & PIM für Admins
   (siehe https://m365maps.com/matrix.htm)
2. Getrennte Konten & PIM für Admins einführen
3. Break Glass Accounts einrichten
4. MFA über Conditional Access gezielt erzwingen
5. Secure Score und dessen Empfehlungen sichten

Fragen & Diskussion