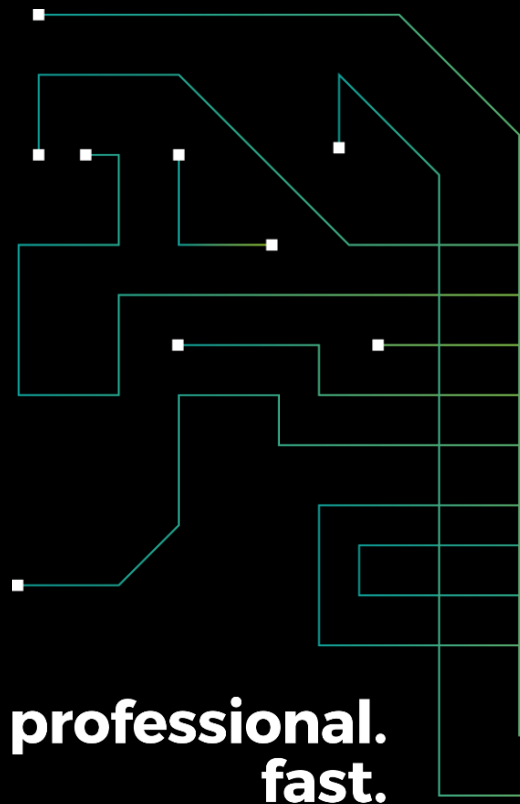
DATENSCHUTZ & COMPLIANCE NEU DEFINIERT MIT MICROSOFT 365 PURVIEW



professional.
fast.
secure.

11.4.2025/Purker Matthias

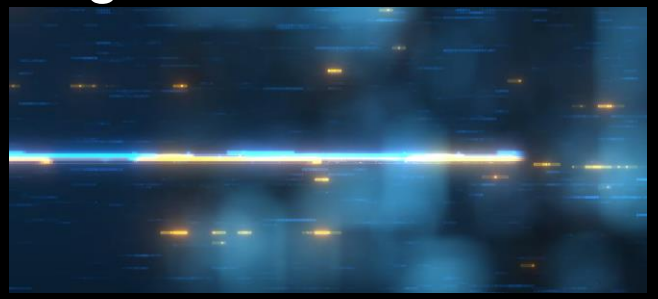
base it

EINFÜHRUNG

EINFÜHRUNG
ORGANISATORISCH

Daten

Jede Aktion generiert Datensätze. Gespeichert in Datenbanken, File Shares, E-Mails, Cloud-Diensten… innerhalb und außerhalb meiner Organisation.



Identifizierung

Welche sind meine sensiblen und schützenswerten Daten?

Aktion

Automatisierung für Markierung und Schutz von sensiblen Daten unabhängig vom Speicherort.

Maßnahmen gegen unabsichtliches Teilen, Exfiltrierung, Datendiebstahl uvm.

EINFÜHRUNG MS PURVIEW

DEFINITION VON DATEN – CLASSIFIER IN PURVIEW

- Sensitive Info Typ

Credit Card Number

Test Copy Edit Delete

Details

Description

Detects credit card numbers for

Source code

Overview Matched items

Recommendation

Classifier is ready f

This classifier can now be used in p

Use classifiers to auto-apply sensit

Use classifiers to auto-apply retent

Details

Description

This classfier predict whether a given document contains any programming code from any of the 23 programming languages: ActionScript, C, C#, C++, Clojure, CoffeeScript, Go, Haskell, Java, TLAB, Objective-, R, Ruby, Scala, n Script

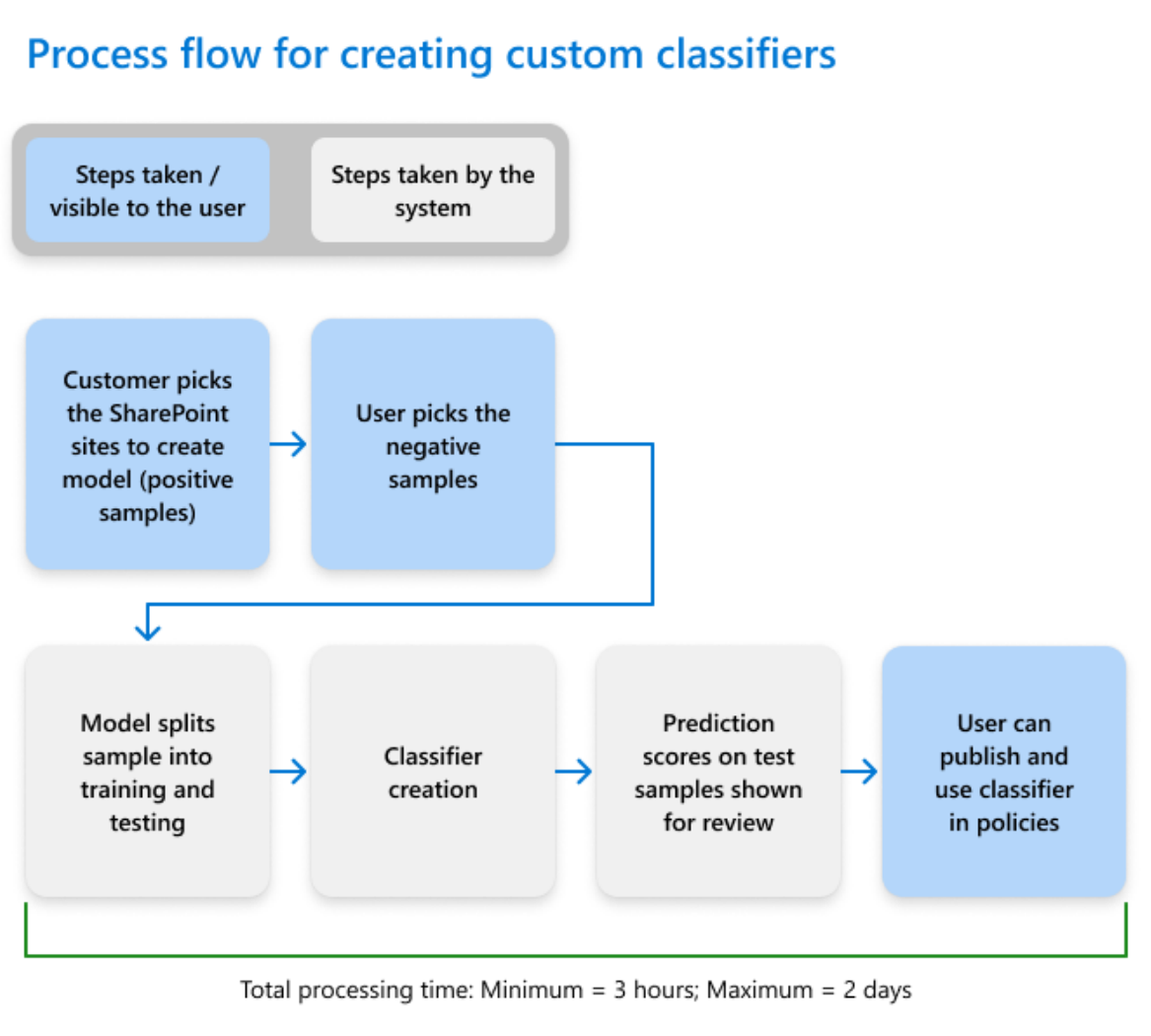
```
SSN,AccountID,FirstName,LastName,Email
270 34 7884,B12345678,Richard,Jackson,Richard@contoso.onmicrosoft.com
030 72 7381,B12345678,Sarah,Jefferson,sarah.jefferson@contoso.com
757-85-7495,B12345678,Bradly,McGordon,bradly.mcgordon@testcompany.com
781-70-8498,B12345678,Shiva,Agarwal,sargarwal@national.onmicrosoft.com
749 25 3016,B12345678,Flash,Gordon,flash.gordon@outlook.com
789-21-8631,12345678,Andrew,O'Donnal,andrew.odonnal@contoso.onmicrosoft.com
182-73-1694,12345678,Angelica,Jackson,angelica.jackson@msn.com
303-81-0470,12345678,Ruchi,Gupta,ruchig@office.com
758 13 4820,12345678,William,Richardson,william.richardson@contoso2.onmicrosoft.com
111-69-8921,12345678,Joseph,Smith,joseph.smith@outlook.com
```

list: Keyword_cc_verification

- Keyword
  list: Keyword_cc_name
- Function
  processors: Func_expiration_da

EINFÜHRUNG MS PURVIEW

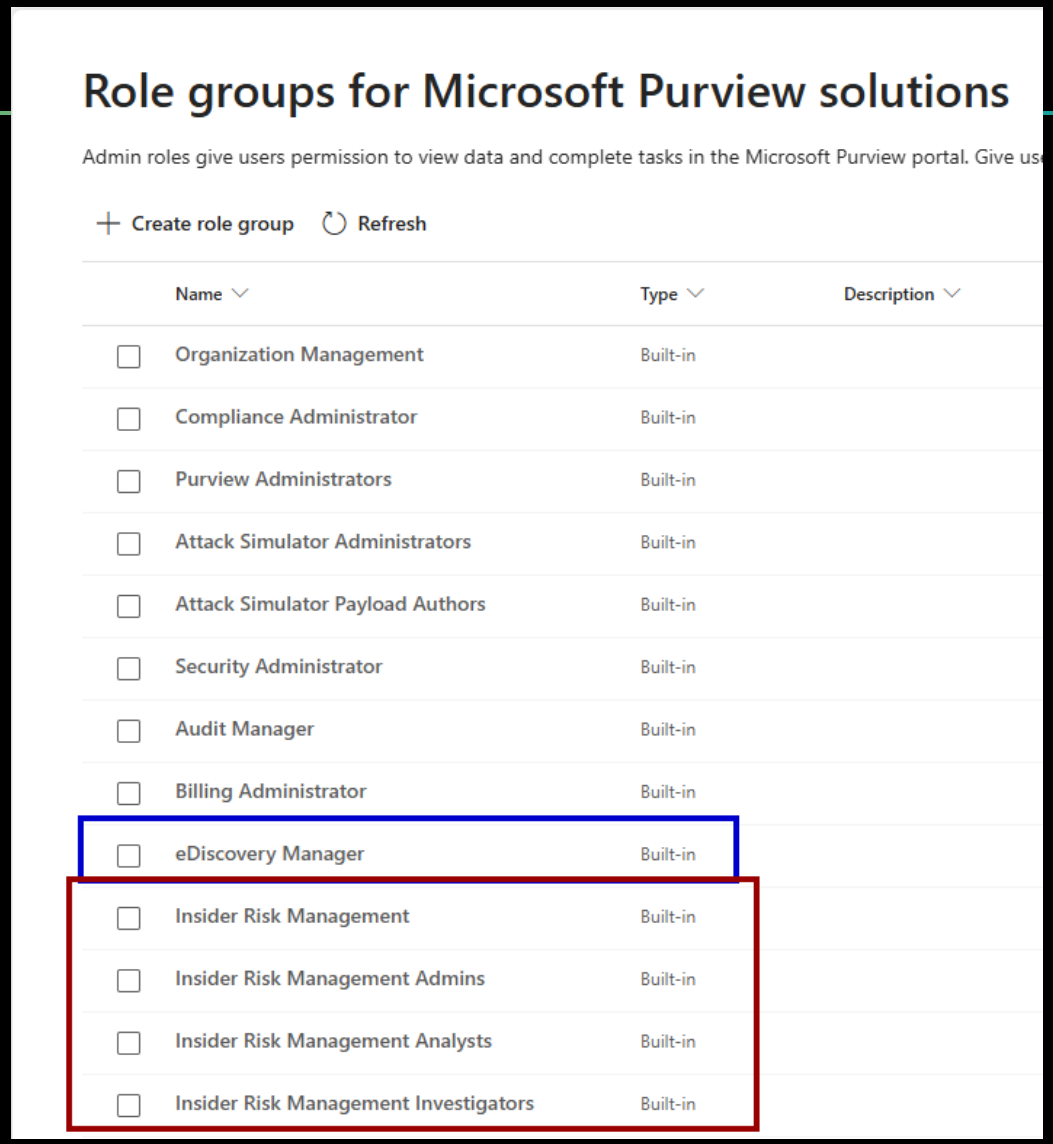
PROZESS ERSTELLUNG VON CLASSIFIER



EINFÜHRUNG MS PURVIEW

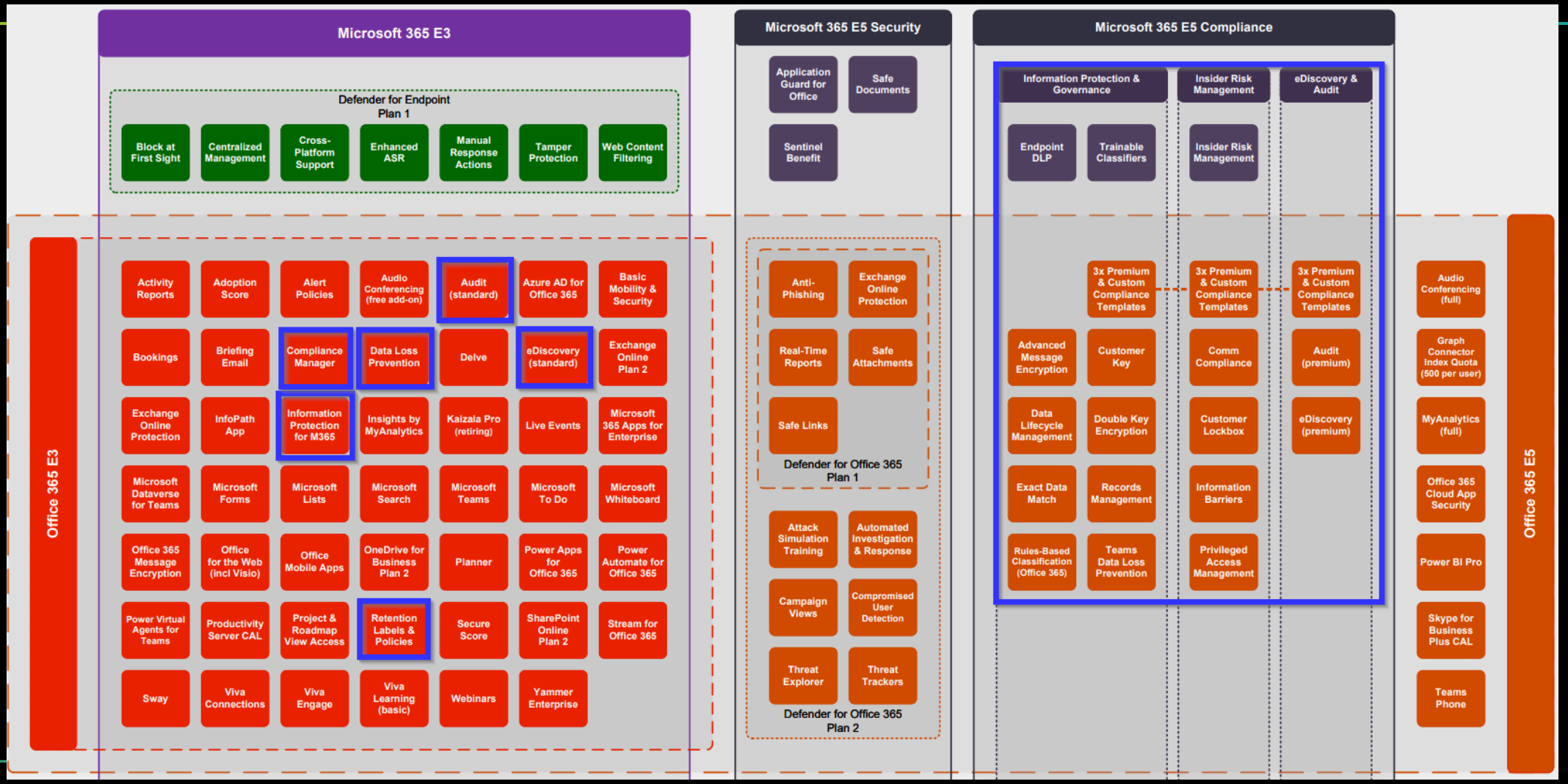
ROLLEN IN PURVIEW

- Administrative Rollen
  - Compliance Administrator
  - Insider Risk Management
- End-User relevante Rollen
  - Insider Risk Management Analyst
  - Information Protection Investigators



EINFÜHRUNG MS PURVIEW

LIZENZÜBERBLICK



base it

EDISCOVERY & CONTENT SEARCH

EDISCOVERY & CONTEN
SUCHE IM O365 TENANT

- Content Search

Speicherorte

Bestimmte Orte

Status	Ort	Enthalten
Ein	Exchange-Postfächer Microsoft 365-Gruppen, Teams, Yammer-Benutzernachrichten	Alle Benutzer, (
Ein	SharePoint-Sites OneDrive-Sites, Microsoft 365-Gruppenwebsites, Teamwebsites, Yammer-Netzwerke	Alle Websites a
Ein	Öffentliche Exchange-Ordner	Alle

+ Bedingung hinzufügen

Ergebnisse exportieren

Grundgesamtheit

Durchsuchbare Dateien: Export [redacted]

Ausgabeoptionen

- (•) Alle Elemente, außer denen mit einem unbekannten Format, sind verschlüsselt oder wurden aus anderen Gründen nicht indiziert.
- ( ) Alle Elemente, einschließlich derer mit einem unbekannten Format, sind verschlüsselt oder wurden aus anderen Gründen nicht indiziert.
- ( ) Nur Elemente, die ein unbekanntes Format haben, verschlüsselt sind oder aus anderen Gründen nicht indiziert wurden

Exchange-Inhalt exportieren als

- (•) Eine PST-Datei pro Postfach
- ( ) Eine PST-Datei, die alle Nachrichten enthält
- ( ) Eine PST-Datei mit allen Nachrichten in einem einzigen Ordner
- ( ) Einzelne Nachrichten

[ ] Deduplizierung für Exchange-Inhalt aktivieren

Schätzung

	Zahl	Größe	Aktualisiert auf
Durchsuchbare Eleme...	2 446 Ergebnisse	647.15 MB	29.4 [redacted] 10:06:...
Nicht durchsuchbare ...	389 Ergebnisse	117.52 MB	29.4 [redacted] 10:06:...
Elemente gesamt	2 835 Ergebnisse	764.67 MB	29.4 [redacted] 10:06:...

EDISCOVERY & CONTENT-SEARCH

UNTERSCHIEDE CONTENT-SEARCH & EDISCOVERY

Inhaltssuche	eDiscovery (Standard)	eDiscovery (Premium)
– Suchen nach Inhalten – Schlüsselwortabfragen und Suchbedingungen – Exportieren von Suchergebnissen – rollenbasierte Berechtigungen	- Suche und Export - Case Management - Rechtliche Aufbewahrung	- Verwaltung von Verwahrer - Benachrichtigungen zur Aufbewahrung gesetzlicher Aufbewahrung - Erweiterte Indizierung - Überprüfungssatzfilterung - Tagging - Analysen - Vorhersagecodierungsmodelle und mehr...

base it

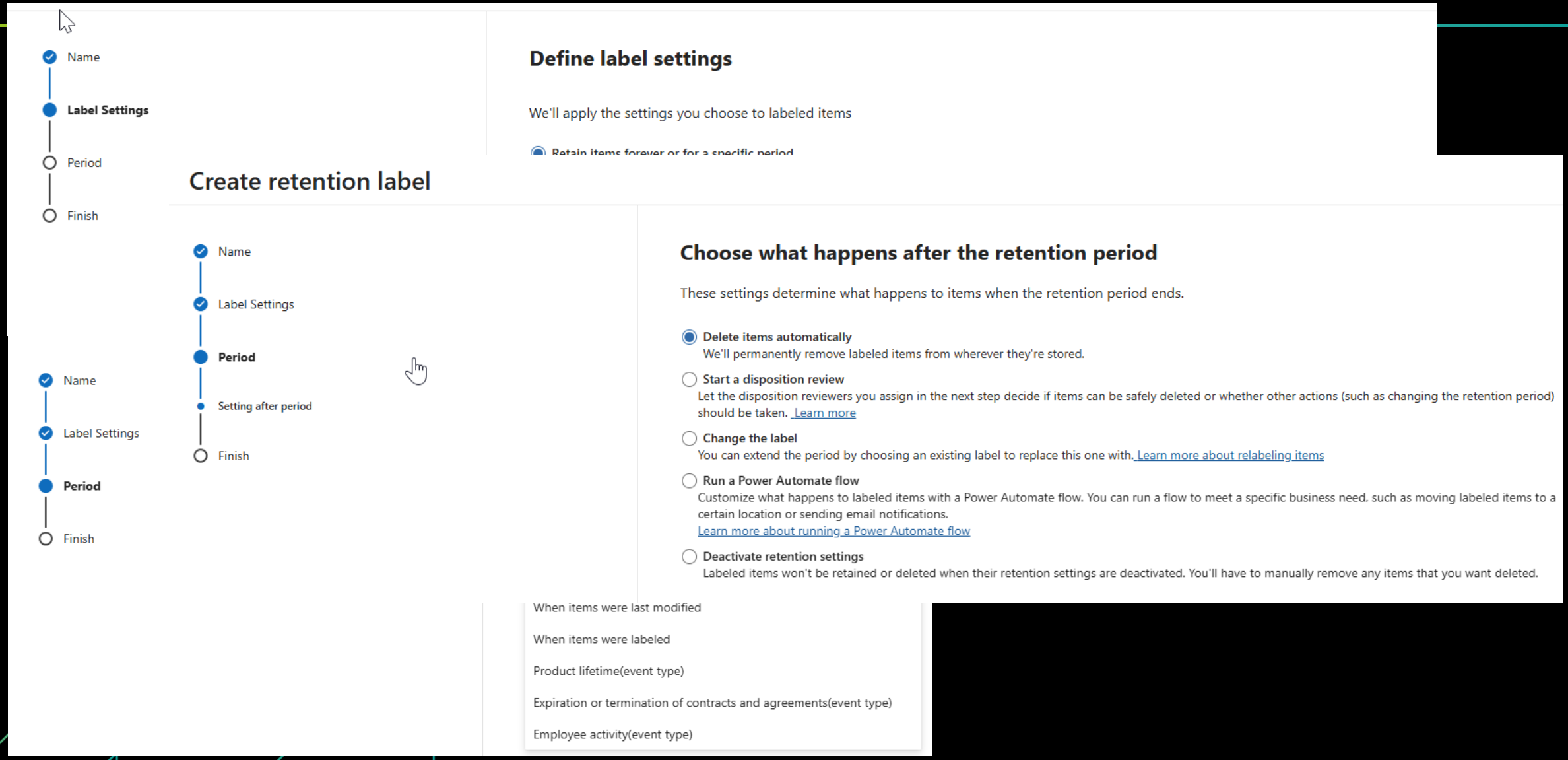
DATA LIFECYCLE MANAGEMENT

DATA LICECYCLE MANAGEMENT
EINFÜHRUNG

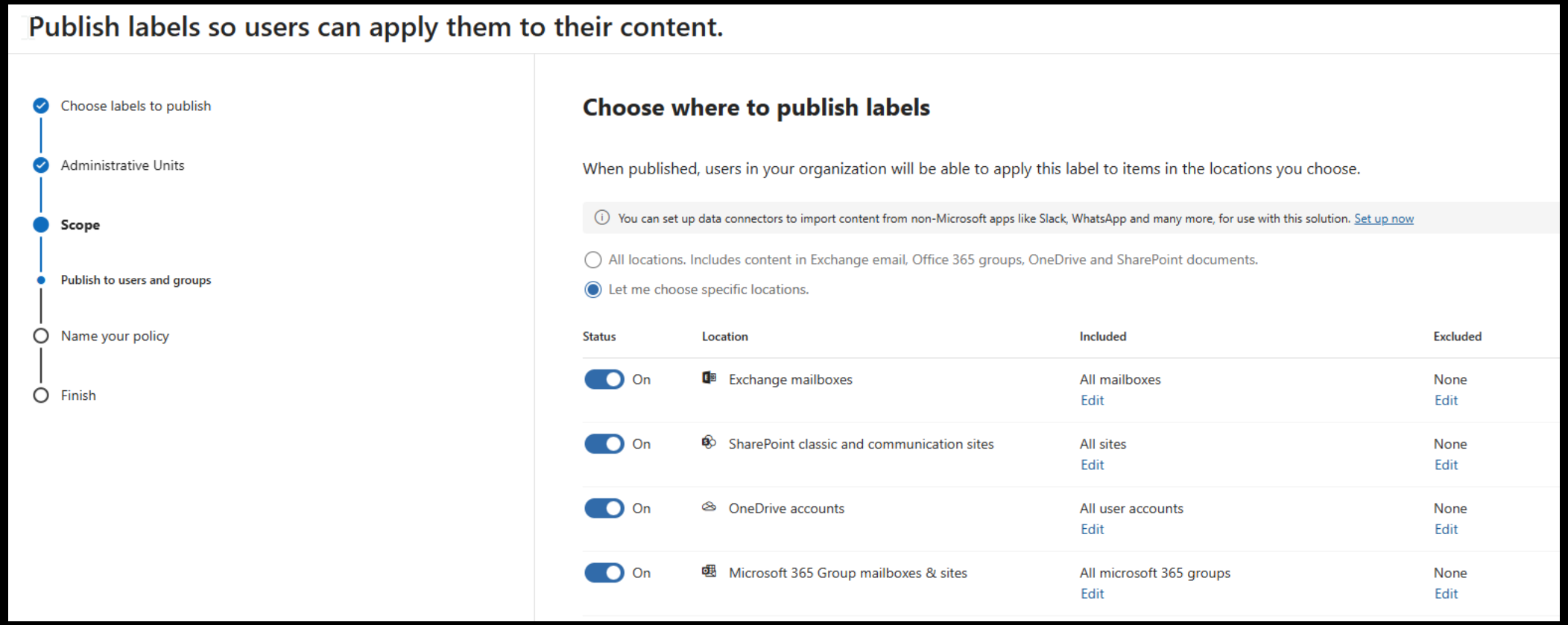
- Wie lange müssen Daten aufbehalten werden?
- Definition von Retention-Labels
  - Aufbewahrungszeitraum
  - Aktion nach Ablauf der Zeit
- Veröffentlichung durch Label-Policies
  - Static vs Adaptive Scopes
- MRM Retention Policies
  - Exchange Archivierung

DATA LICECYCLE MANAGEMENT

ERSTELLUNG RETENTION-LABEL



DATA LICECYCLE MANAGEMENT
VERÖFFENTLICHUNG EINES LABELS

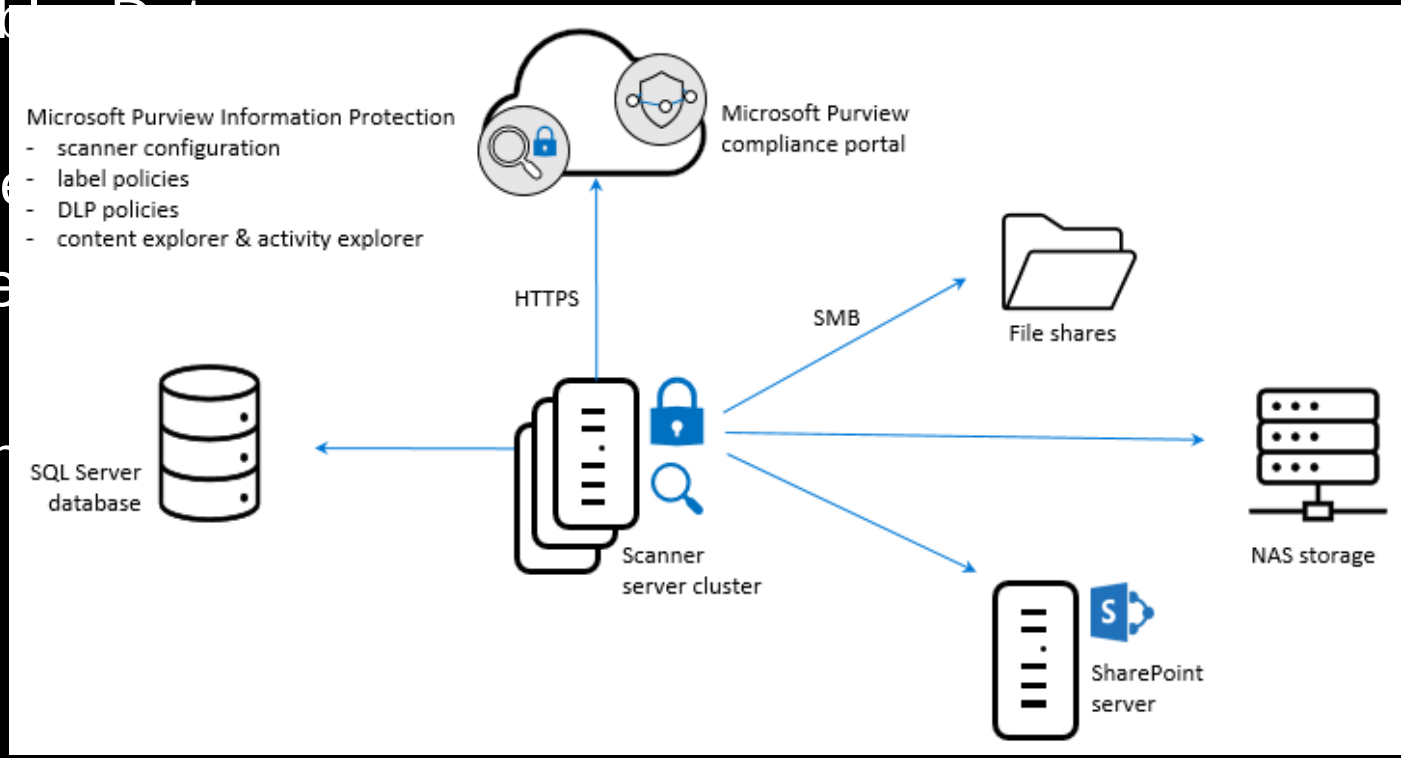


base it

DATA LOSS PREVENTION (DLP)

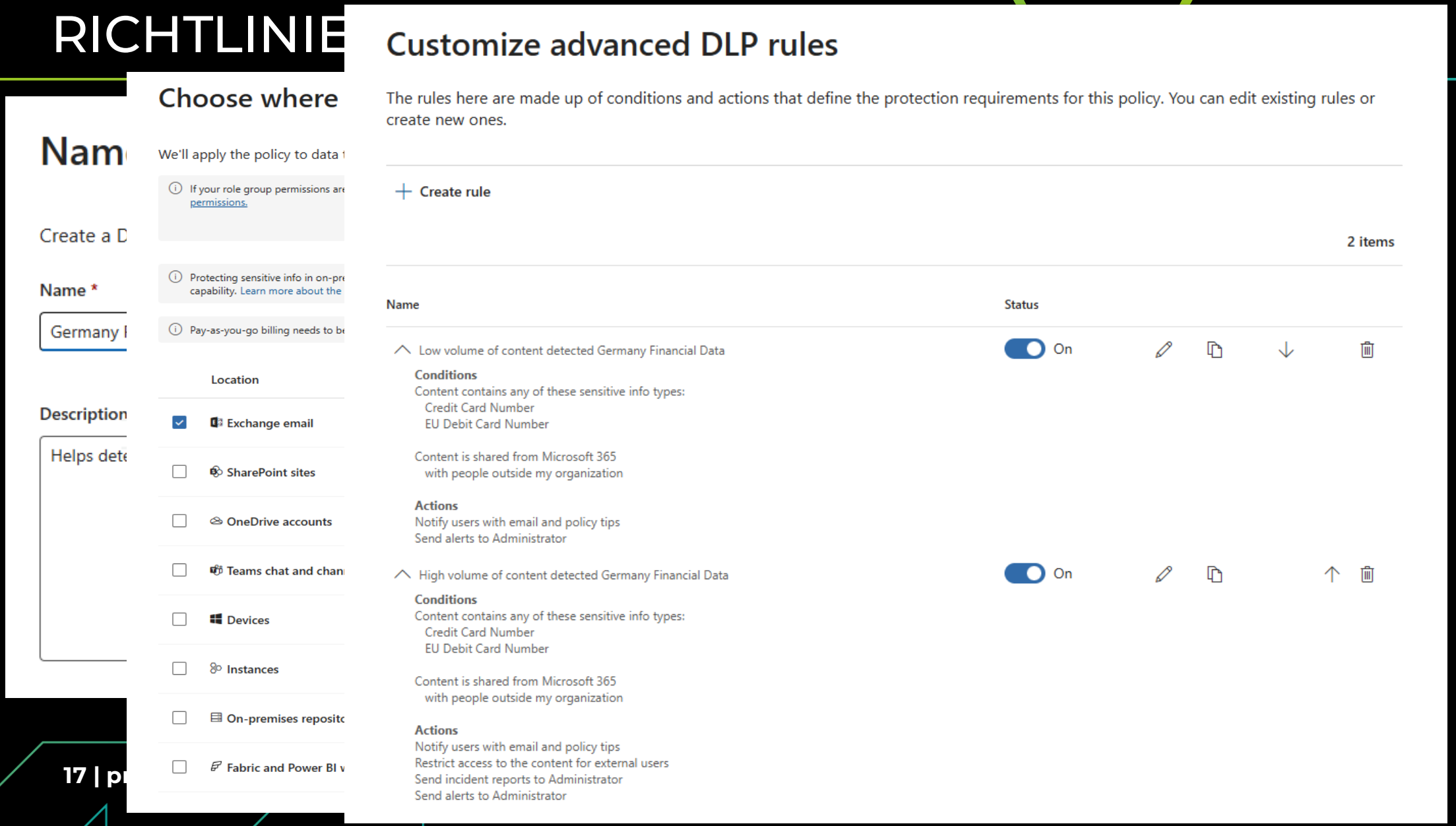
DATA LOSS PREVENTION (DLP)
EINFÜHRUNG

- Ziel von DLP :
  - Erkennung des Datenflusses sensib
  - Schutz vor unsicherer Freigabe
  - Verhinderung unangemessene Dat
- OnPremise & Endpoint Integratione
  - Defender for Endpoint
  - Überwachung von Client-Aktivitäten

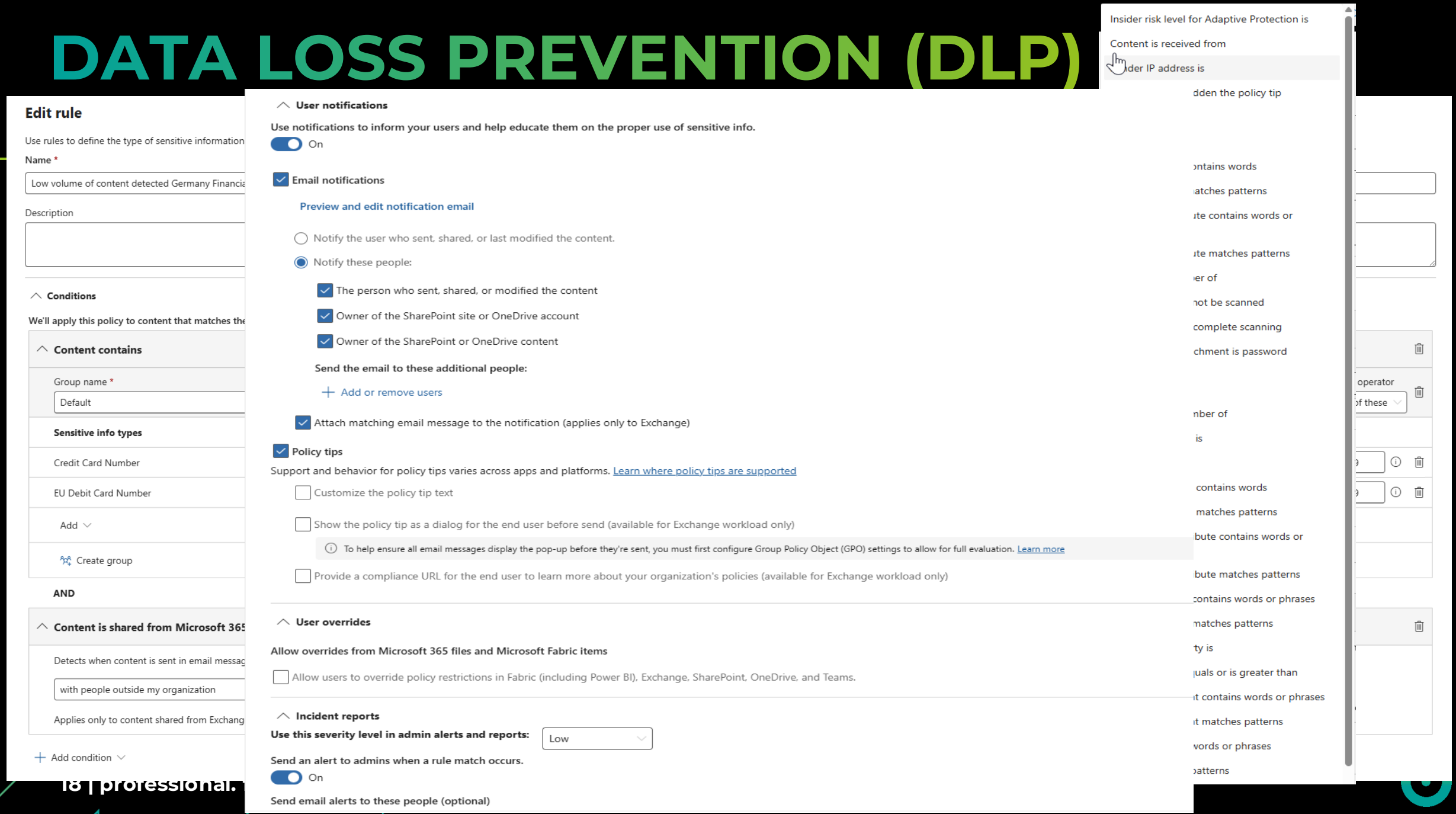


DATA LOSS PREVENTION (DLP)

RICHTLINIE



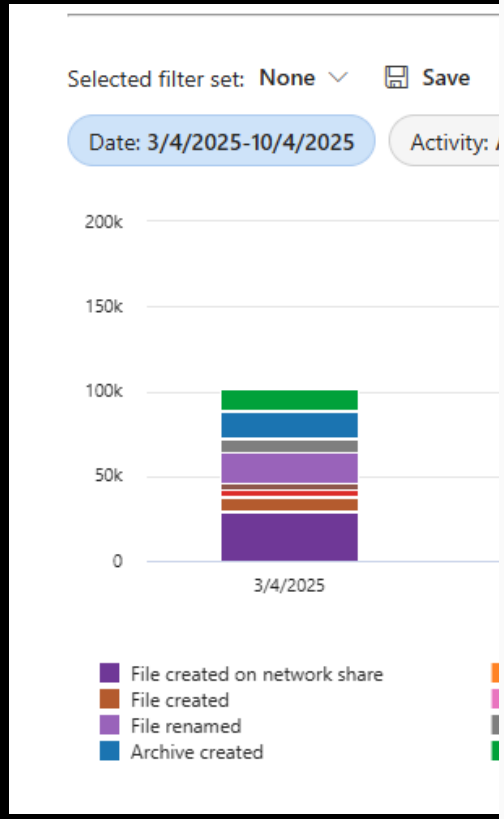
DATA LOSS PREVENTION (DLP)

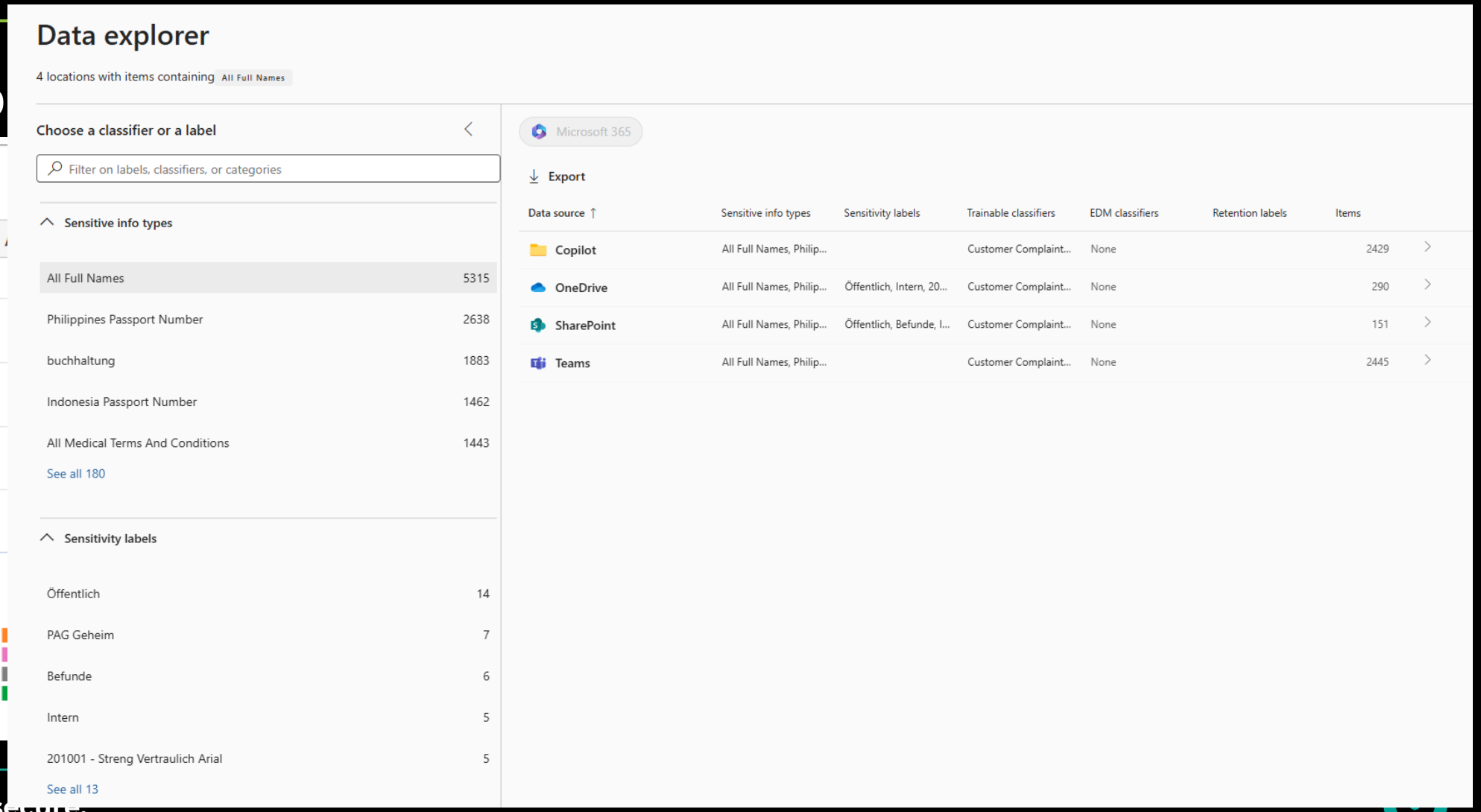


DATA LOSS PREVENTION (DLP)

PRAXISBEISPIELE

- Monitoring vo



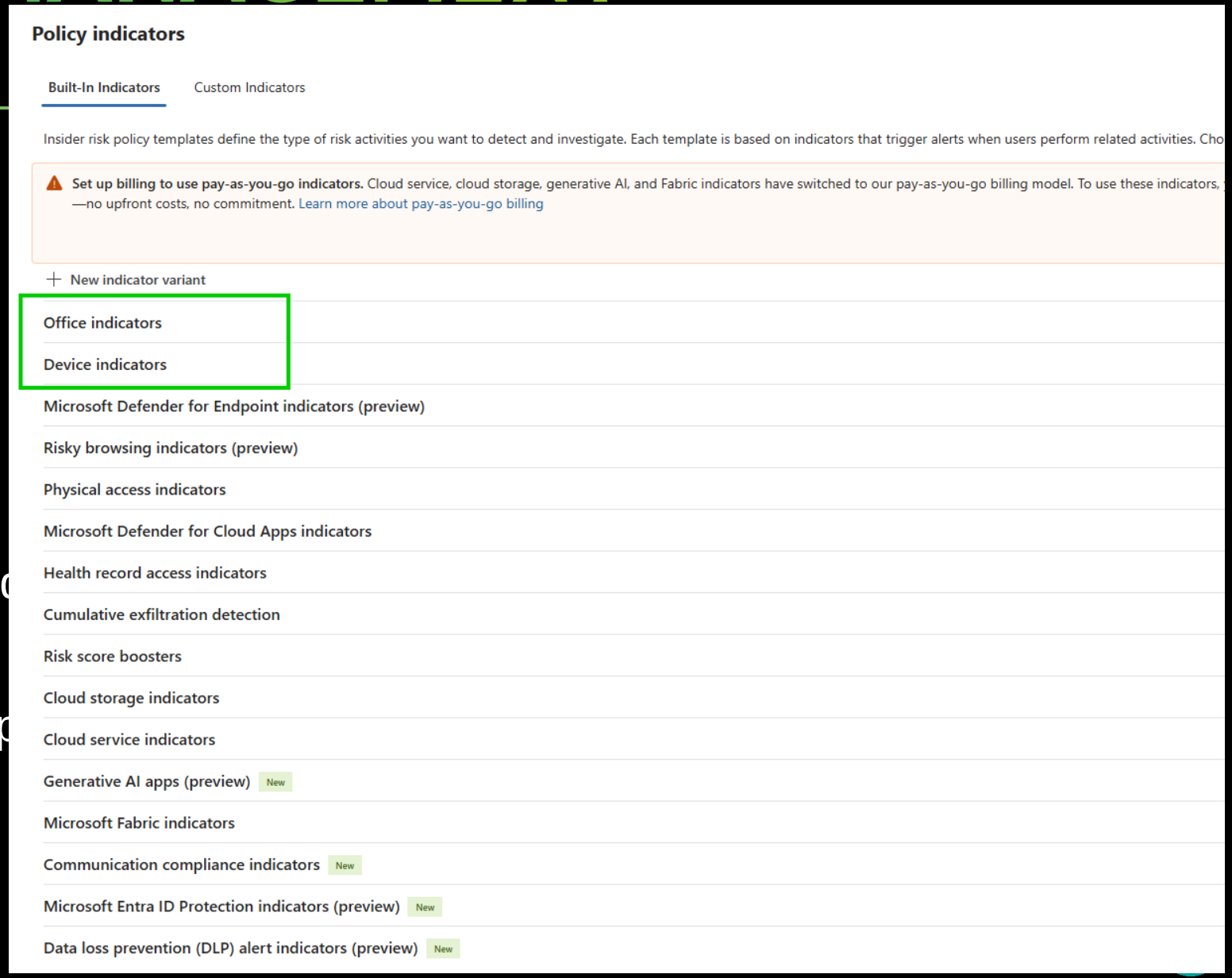


base it

INSIDER RISK MANAGEMENT

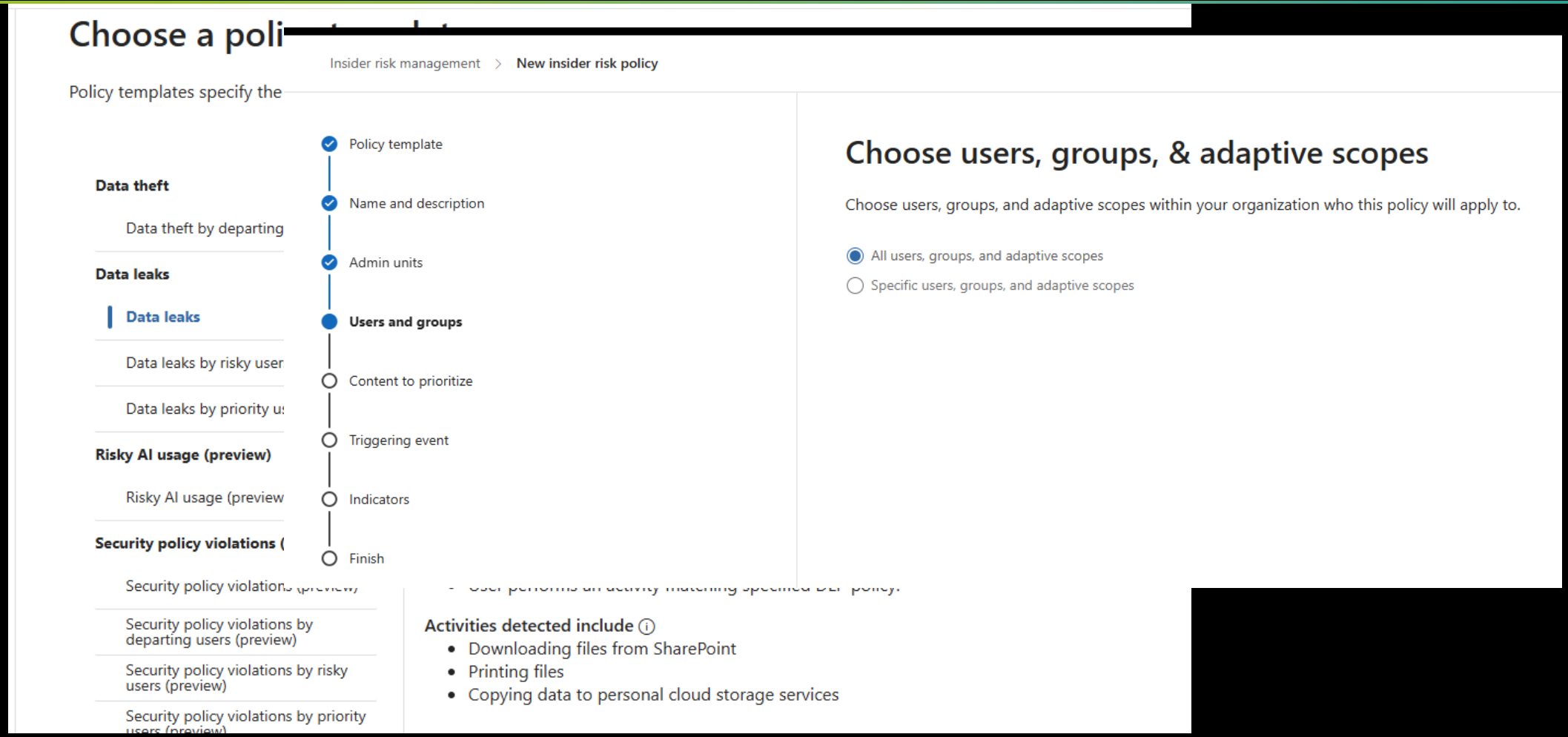
INSIDER RISK MANAGEMENT
EINFÜHRUNG

- Ziel von IRM :
  - Erkennung interner Risiken
- Trigger Events
- Data Connectors
- Bewertung des Risikos anhand
- Richtlinien basierend auf Temp
  - Datendiebstahl
  - Datenexfiltration



INSIDER RISK MANAGEMENT

RICHTLINIEN-BEISPIEL



INSIDER RISK MANAGEMENT
RICHTLINIEN-BEISPIEL

Choose triggering event for this policy

Choose one or more triggering events to determine when a policy will begin assigning risk scores to a user's activity.Learn more

- **User matches a data loss prevention (DLP) policy**
  Policy will start assigning risk scores when a user performs an activity matching the DLP policy you select. The DLP policy must be configured to generate 'High' severity incident reports. Learn more about DLP policy requirements.
  Select a DLP policy
- **User performs an exfiltration activity**
  Policy will start assigning risk scores when specific thresholds are detected for activity relating to the following indicators:
  Select which activities will trigger this policy

Unable to select some indicators? This is because they're currently turned off in your organization. To make them available to select, you can turn them on now.

Turn on indicators

- [x] Downloading content from SharePoint
- [x] Sending email with attachments to recipients outside the organization
- [x] Printing files
- [x] Creating or copying files to USB
- [x] Using a browser to upload files to the web
- [x] Sharing SharePoint files with people outside the organization

Choose thresholds for triggering events

The policy will start assigning risk scores to activity only when specific thresholds are met for the exfiltration activities you selected as the triggering event. Thresholds are based on the number of events recorded for an activity per day. You can use recommended thresholds or specify your own.

- (•) Apply built-in thresholds RECOMMENDED
- ( ) Choose your own thresholds

Indicators

The following indicators are used to generate alerts for the activity detected by the policy template you selected. Learn more

Total indicators selected: 54/91

Unable to select some indicators? This is because they're currently turned off in your organization. To make them available to select, you can turn them on now.

Choose indicators

- Office indicators (28/30 selected)
- Device indicators (8/15 selected)
- Physical access indicators (0/1 selected)

INSIDER RISK MANAGEMENT
RICHTLINIEN-BEISPIEL

Detection options

These advanced detection options are used to generate alerts for the activity detected.

Sequence detection

A sequence is a group of two or more activities performed one after the other over a period of 7 days that might suggest an elevated risk. Specific indicators are used to detect each step in a sequence, which are organized into four main types of activity: download, exfiltrate, obfuscate, and delete. Learn more about sequences

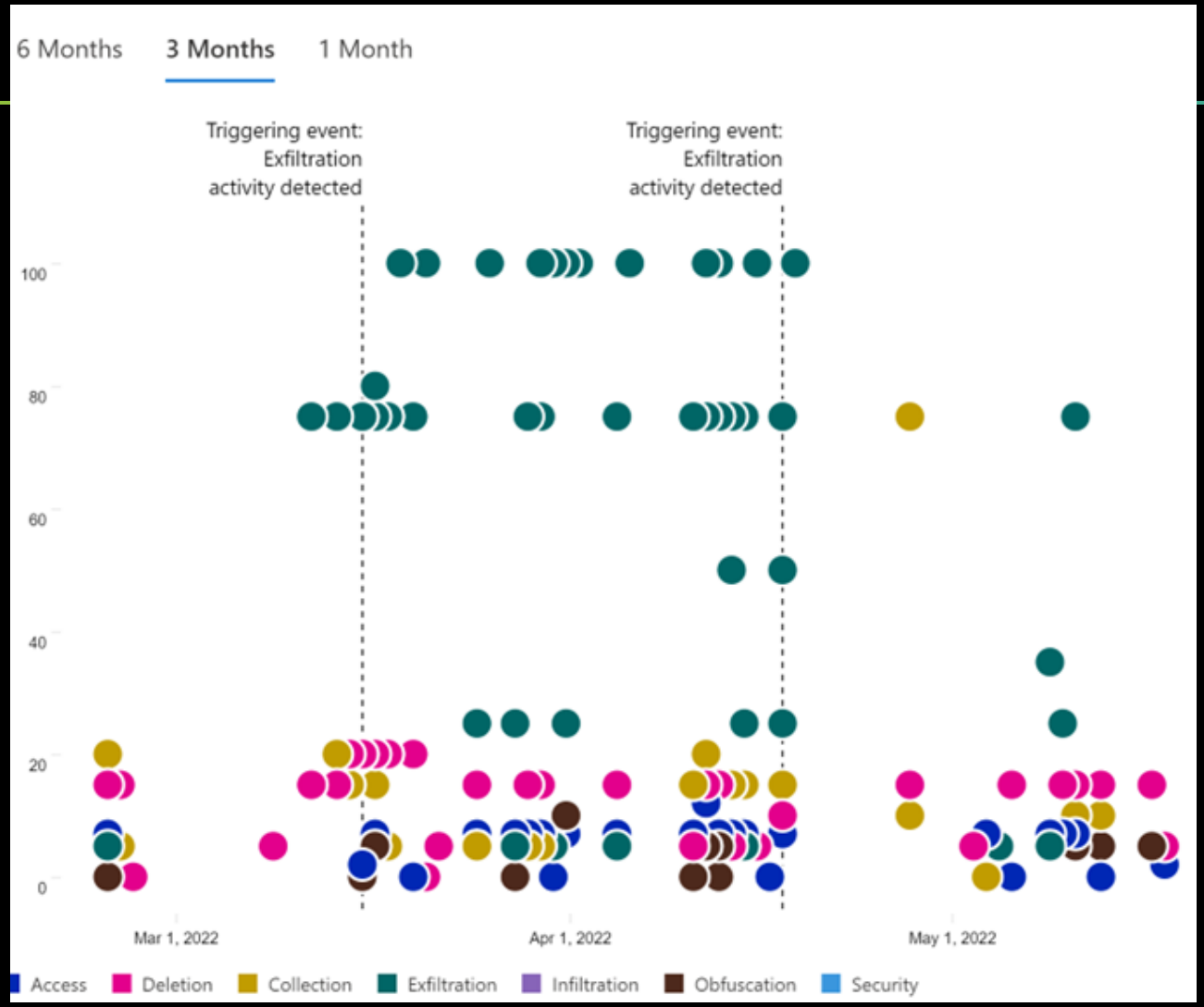
- [x] Select all
- [x] Download from Microsoft 365 location then exfiltrate
- [x] Download from Microsoft 365 location, obfuscate, then exfiltrate
- [x] Download from Microsoft 365 location, exfiltrate, then delete
- [x] Download from Microsoft 365 location, obfuscate, exfiltrate, then delete
- [x] Archive then exfiltrate
- [x] Archive, obfuscate, then exfiltrate
- [x] Archive, exfiltrate, then delete
- [x] Archive, obfuscate, exfiltrate, then delete
- [x] Downgrade or remove label then exfiltrate

Choose threshold type for indicators

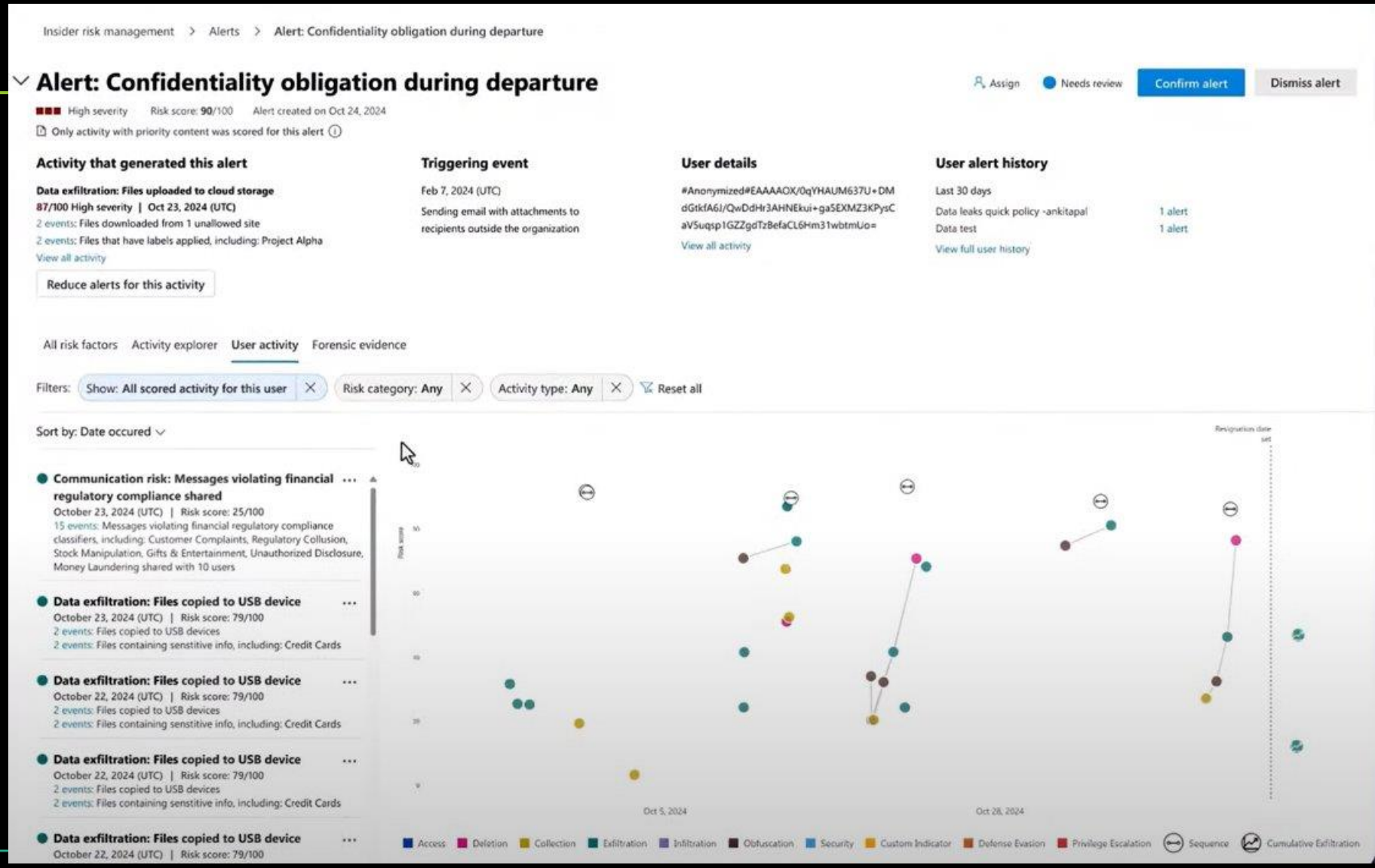
Each indicator you selected uses thresholds to influence the activity's risk score, which in turn determines whether an alert's severity is low, medium, or high. Each threshold is based on the number of events recorded for an activity per day.

- (•) **Apply thresholds provided by Microsoft**
  Built-in thresholds will be applied to all indicators you selected.
- ( ) **Apply thresholds specific to your users' activity** RECOMMENDED
  Thresholds based on your users' recent activity patterns will be applied to all built-in indicators you selected.
- ( ) **Choose your own thresholds**
  Customize thresholds that are prepopulated with values based on your users' recent activity patterns.

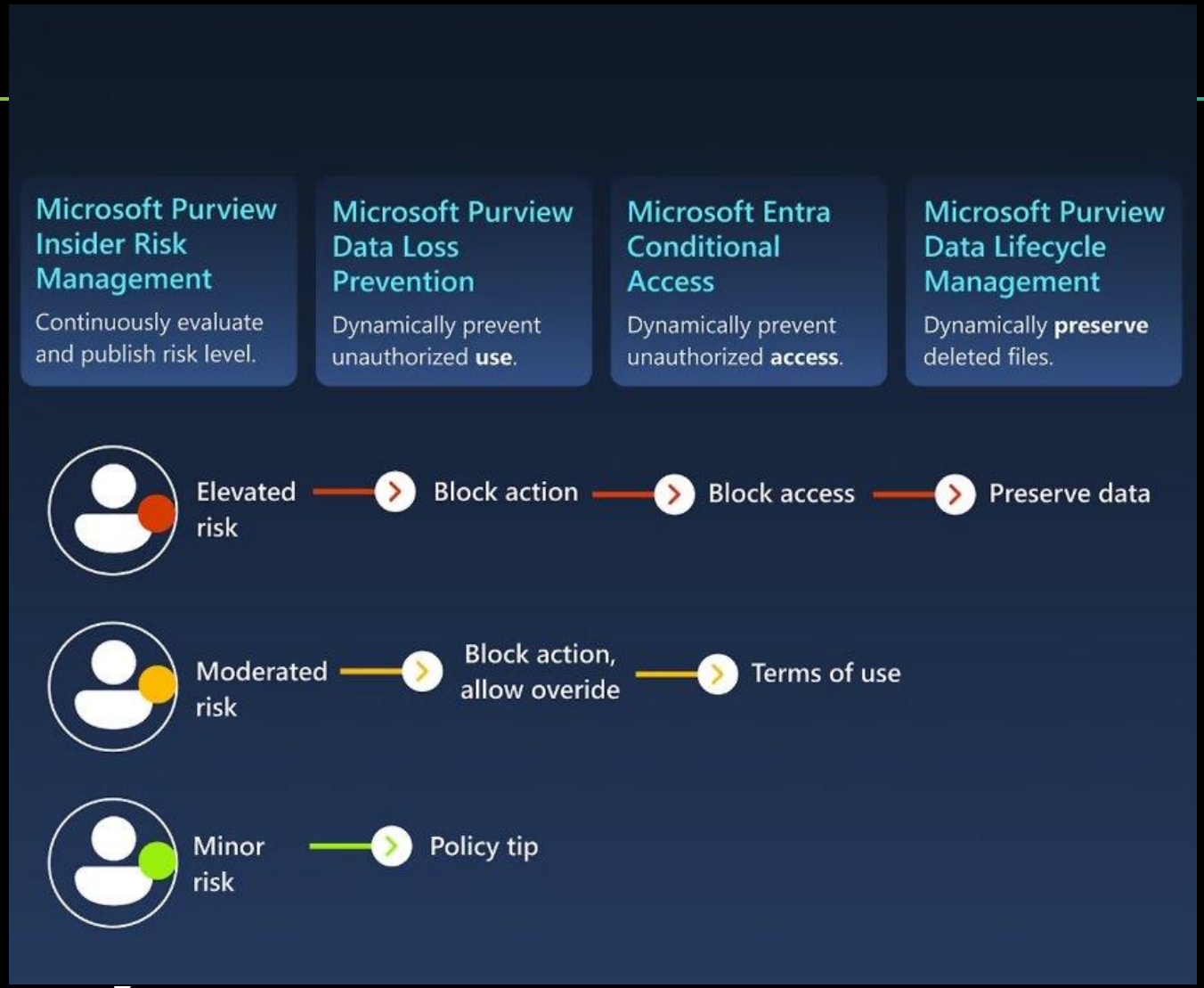
INSIDER RISK MANAGEMENT



INSIDER RISK MANAGEMENT



INSIDER RISK MANAGEMENT



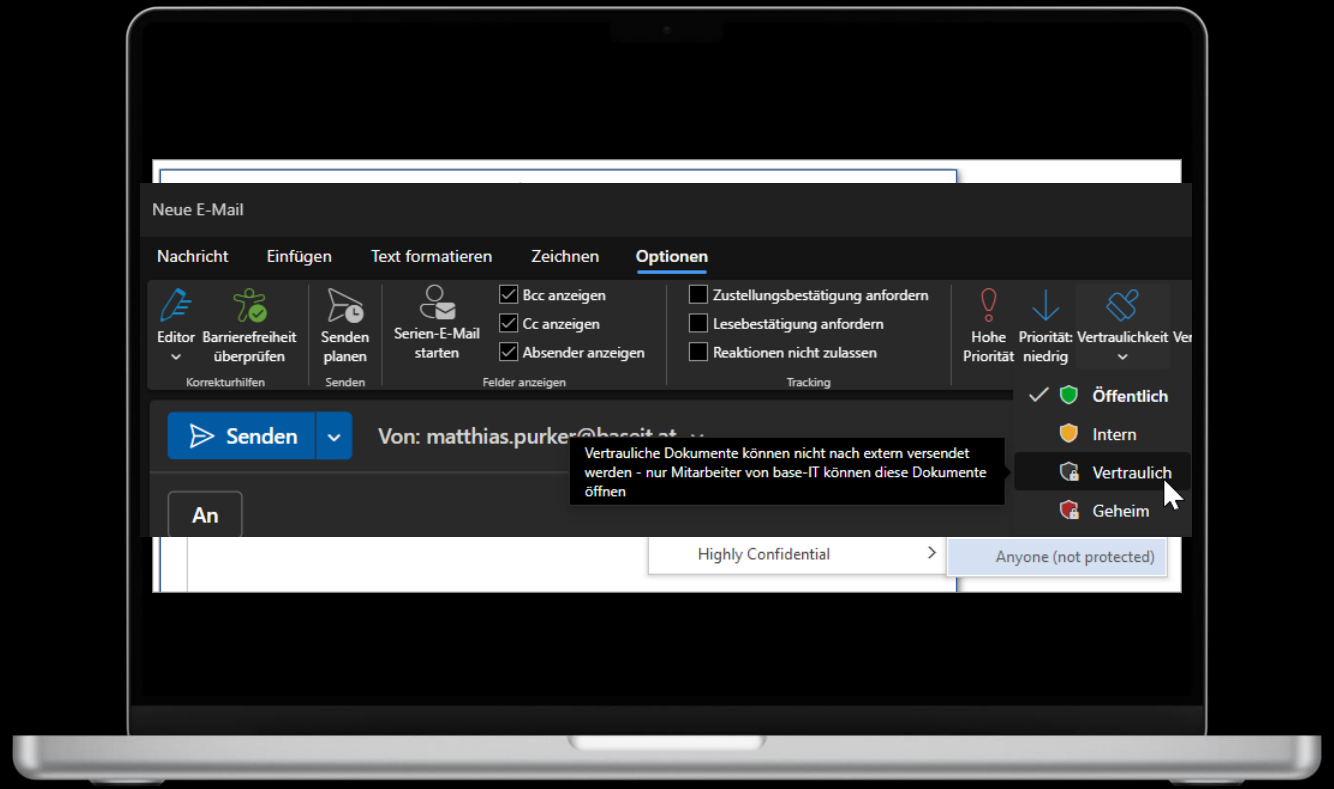
base it

AZURE INFORMATION PROTECTION (AIP)

AZURE INFORMATION PROTECTION

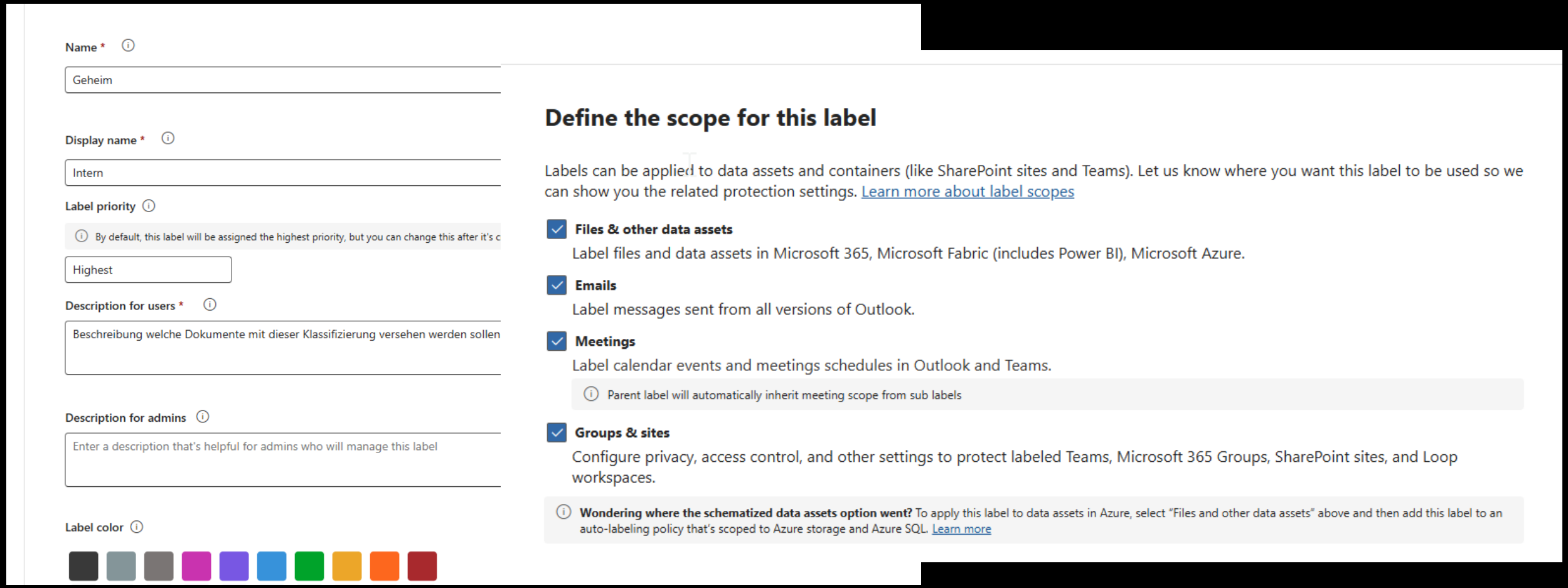
ÜBERSICHT

- Datenklassifizierung
  - Office Dateien, PDFs, PowerBI
  - E-Mails & Meetings
- Schutz & Markierung von Daten
  - Rechtevergabe
  - Verschlüsselung
  - Wasserzeichen



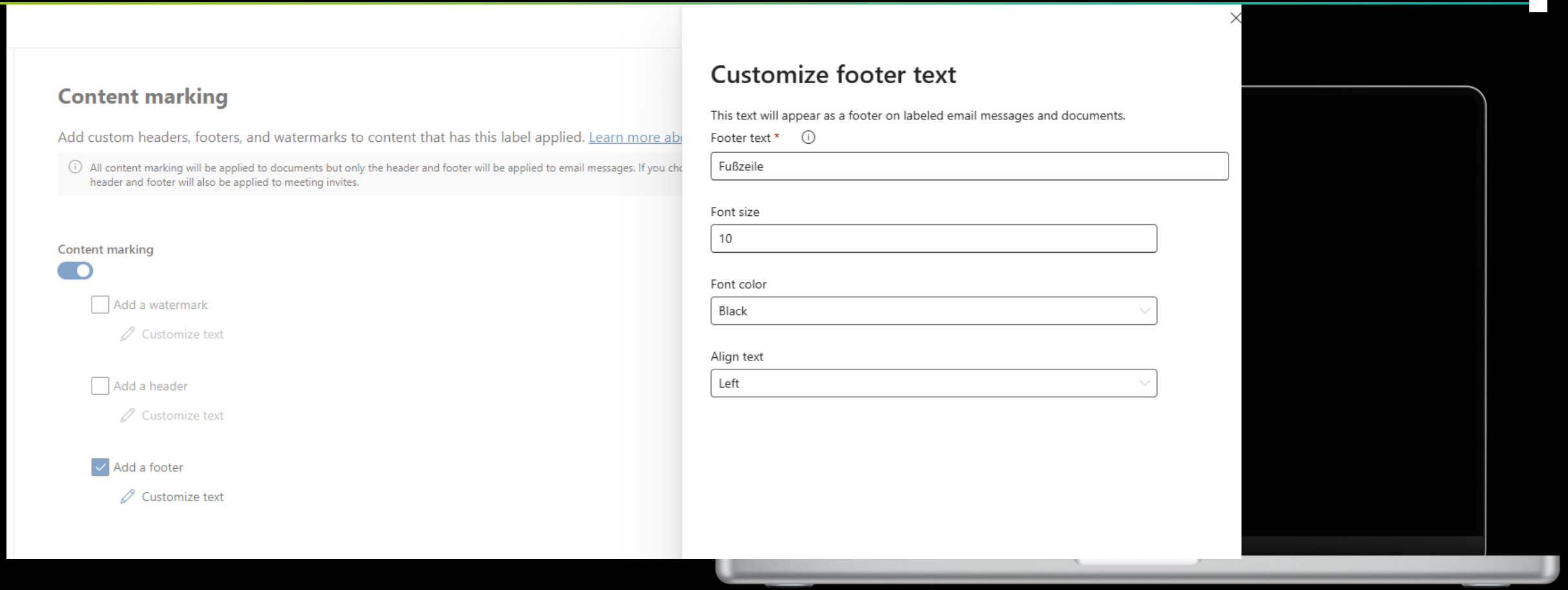
AZURE INFORMATION PROTECTION

SENSITIVITY LABEL



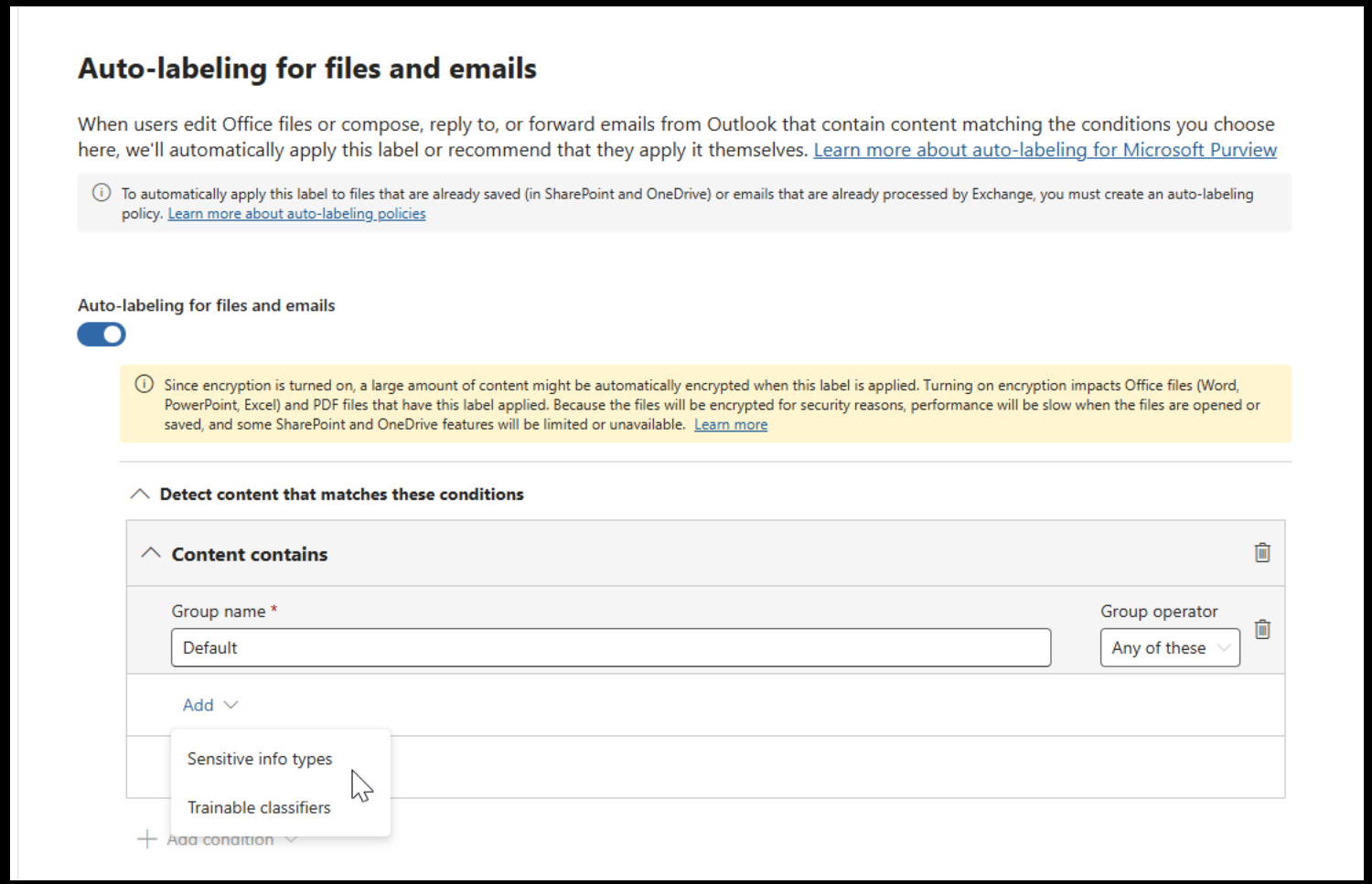
AZURE INFORMATION PROTECTION

SENSITIVITY LABEL



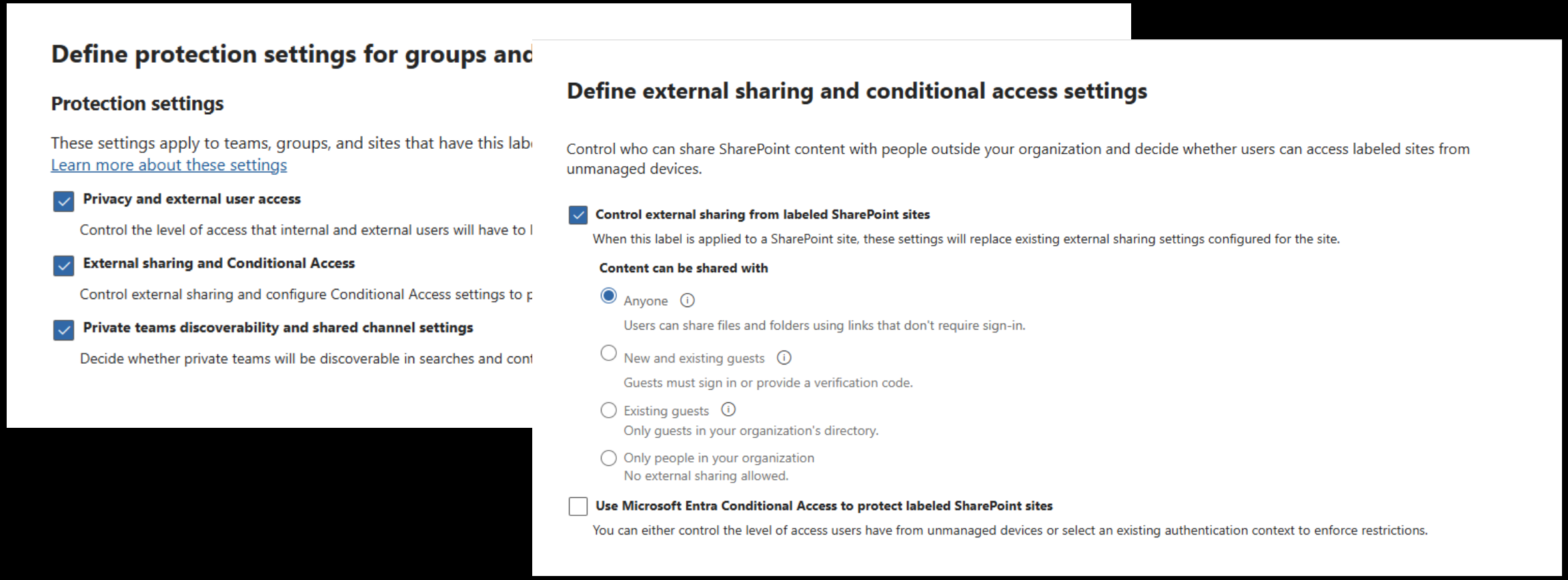
AZURE INFORMATION PROTECTION

SENSITIVITY LABEL



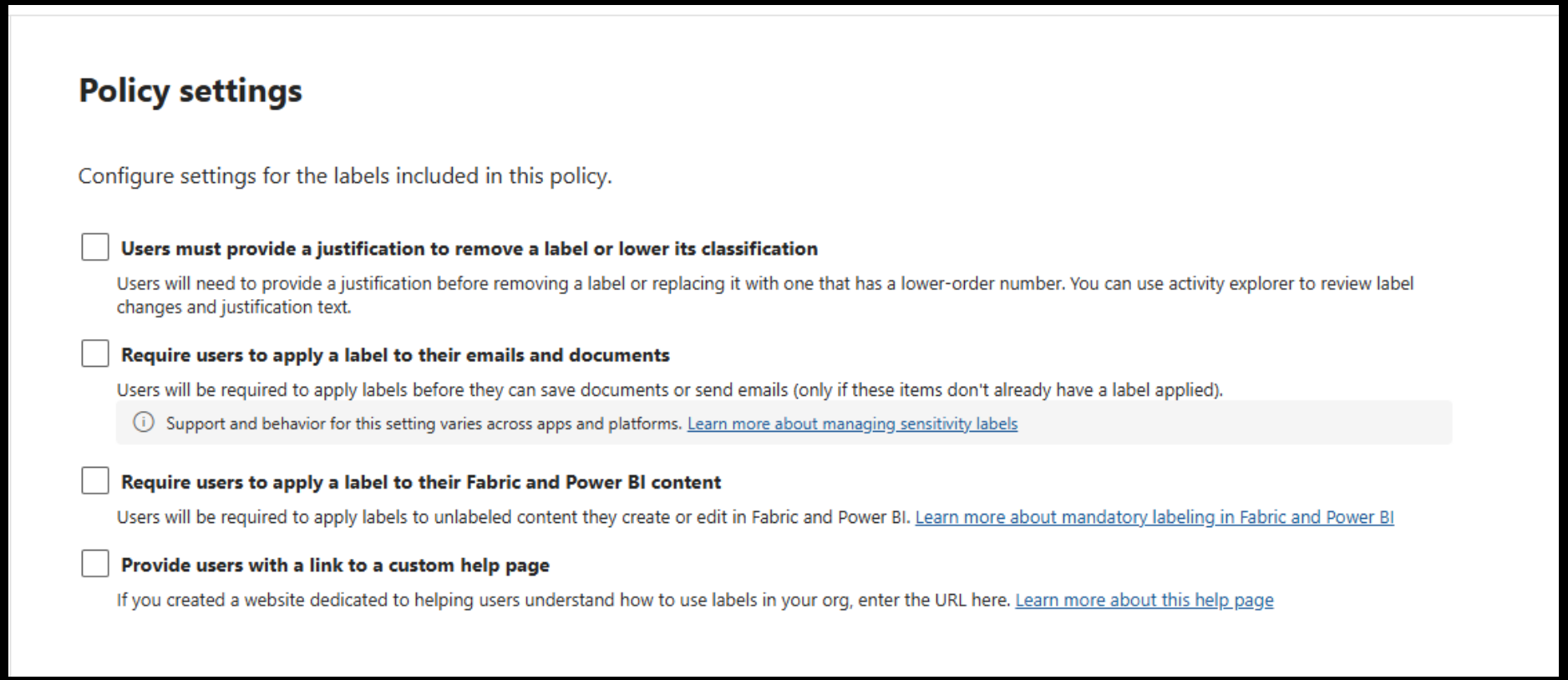
AZURE INFORMATION PROTECTION

SENSITIVITY LABEL



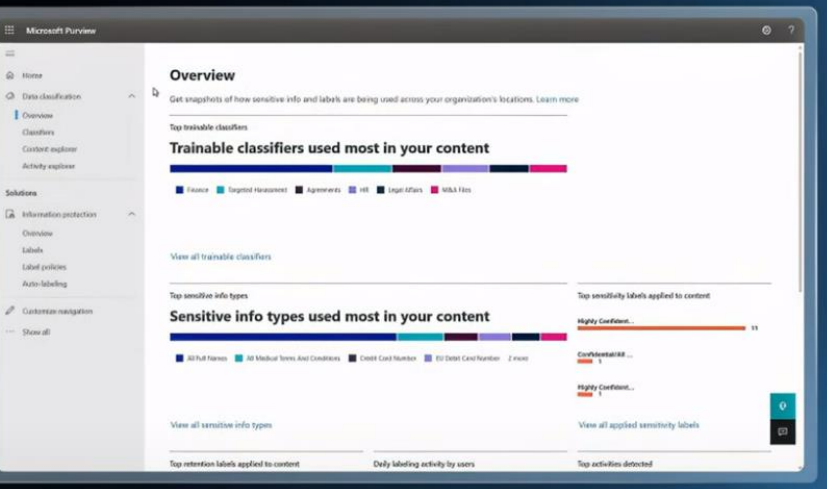
AZURE INFORMATION PROTECTION
LABEL PUBLISHING

- Verteilung der Labels auf Usergruppen

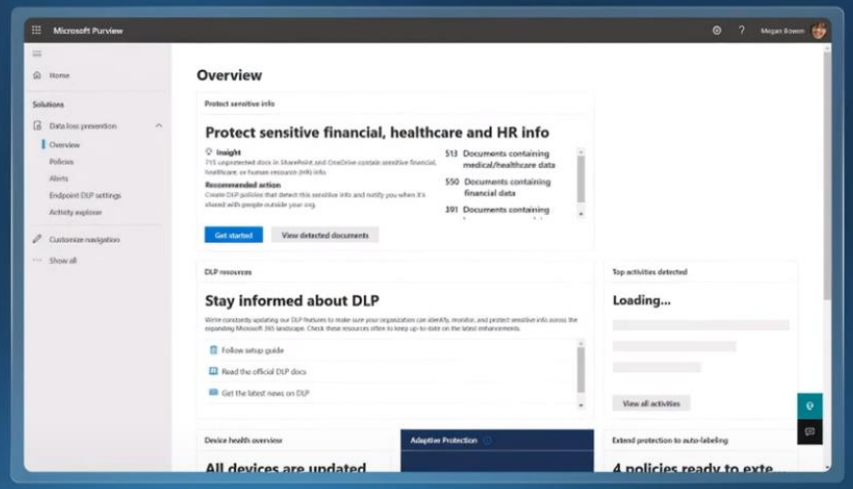


PURVIEW
STÄRKEN DER KOMBINATION

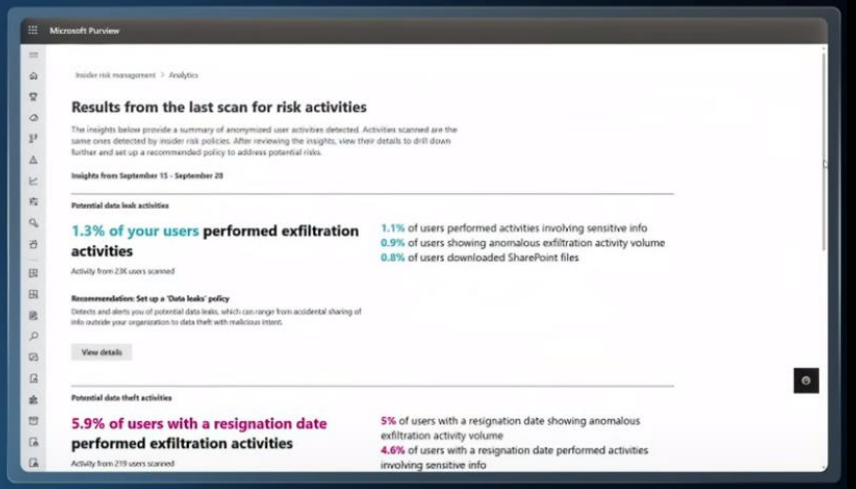
Information Protection



Data Loss Prevention



Insider Risk Management

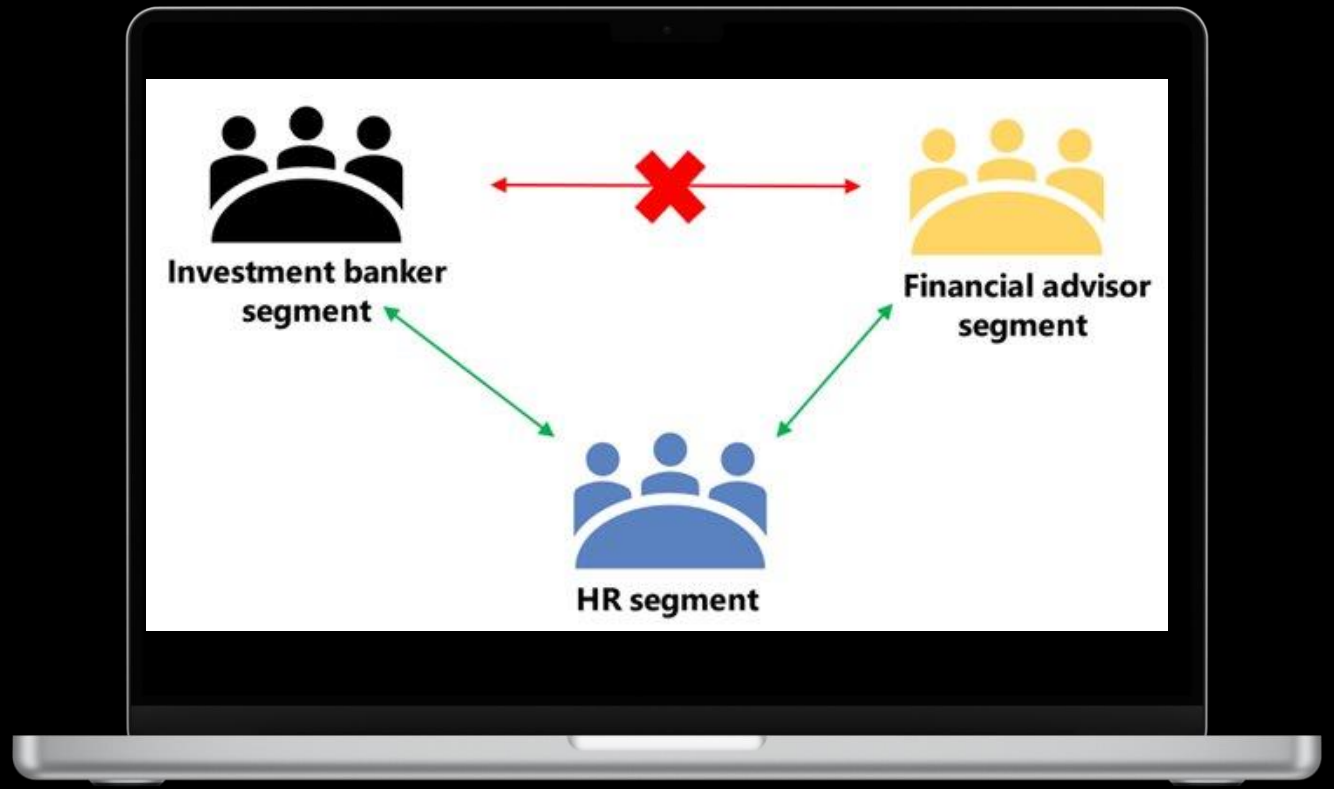


base it

INFORMATION BARRIER

INFORMATION BARRIER

- Erstellung von Segmenten
- Trennung von Diensten
  - Teams-Chat/Call
  - User-Suche
  - Team-Mitglieder
  - Datei-Sharing
- Exchange ist out of Scope

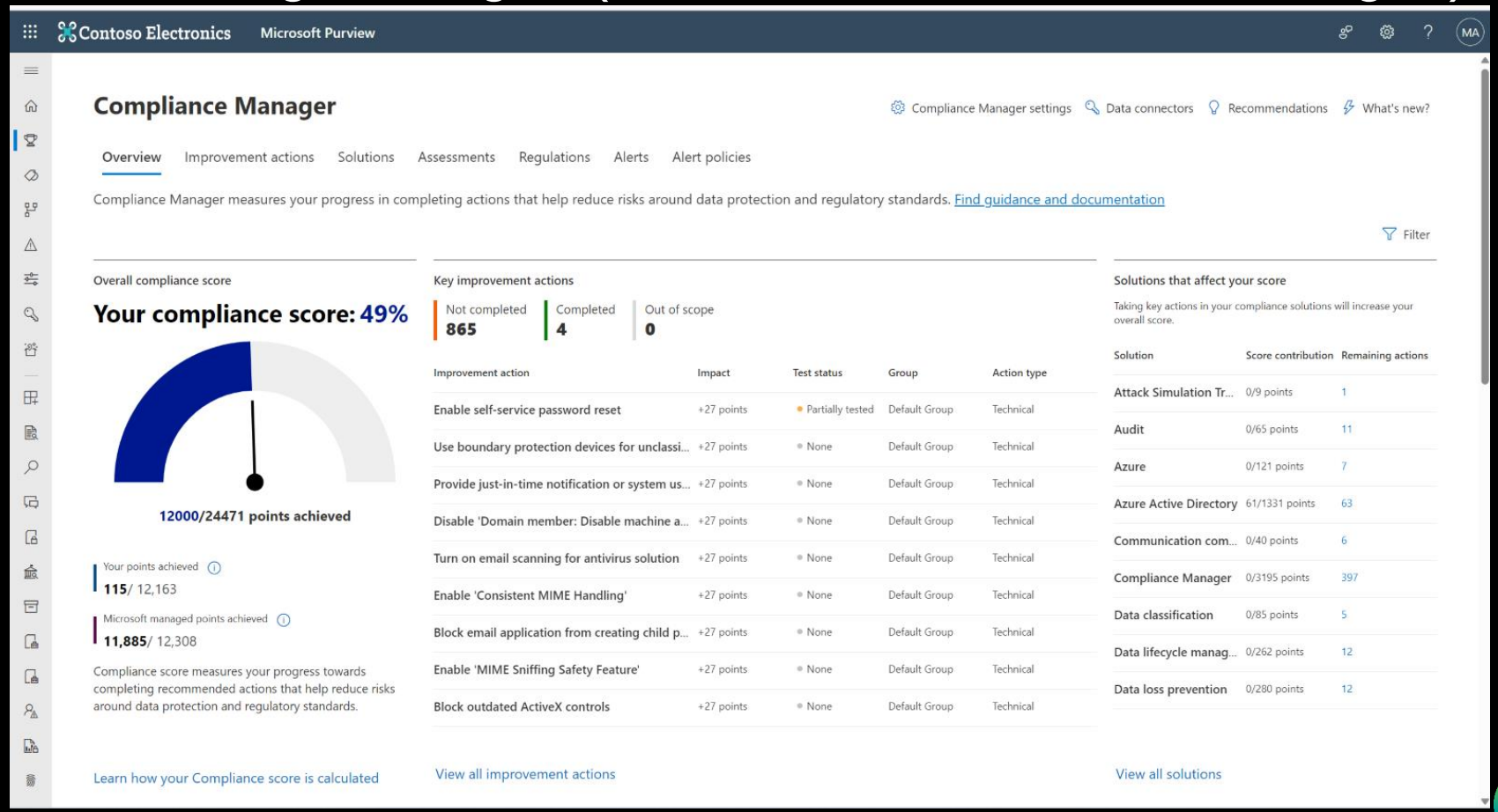


base it

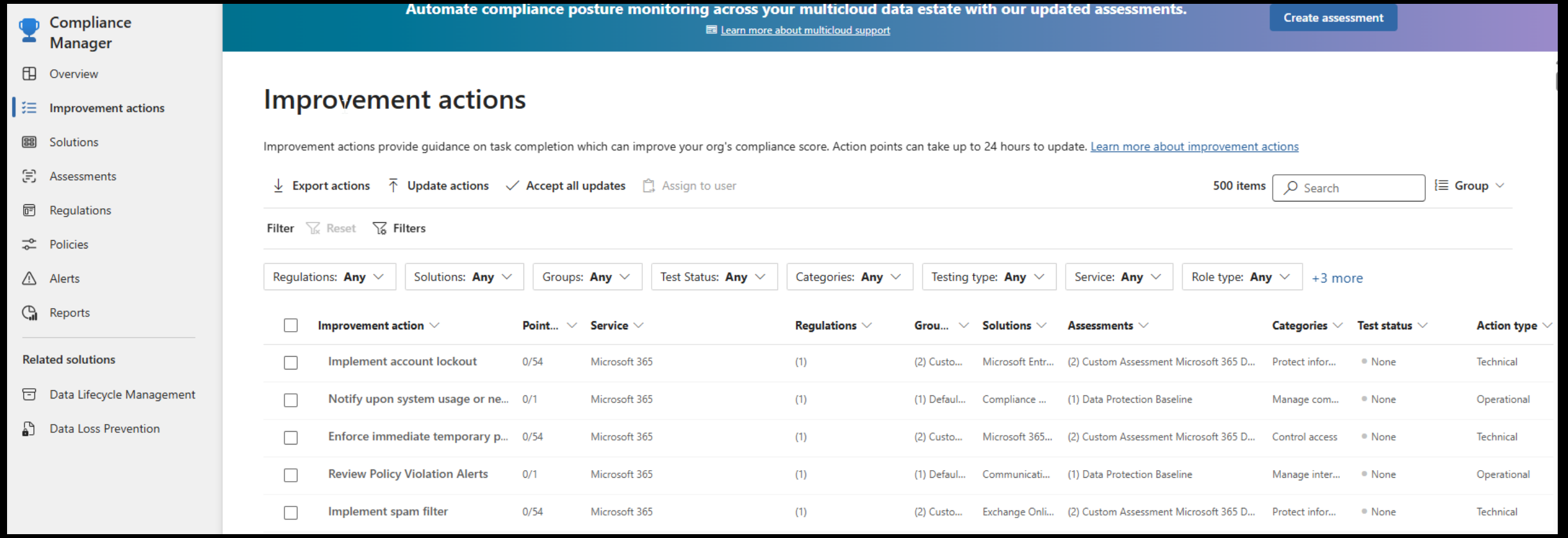
COMPLIANCE MANAGER

COMPLIANCE MANAGER
TENANT ASSESSMENT

- Assessment basierend auf Regulierungen (GDPR,NIS2, ISO-Zertifizierungen)



COMPLIANCE MANAGER
IMPROVEMENT ACTIONS



base it

Haider Straße 23 | 4052 Ansfelden | AT

+43 7229 87800 - 0 | office@baseit.at |

www.baseit.at

Base-IT GmbH (unserebroschuere.at)

Management System ISO/IEC 27001:2013

TÜVRheinland ZERTIFIZIERT

www.tuv.com ID 9000002884

Microsoft Solutions Partner