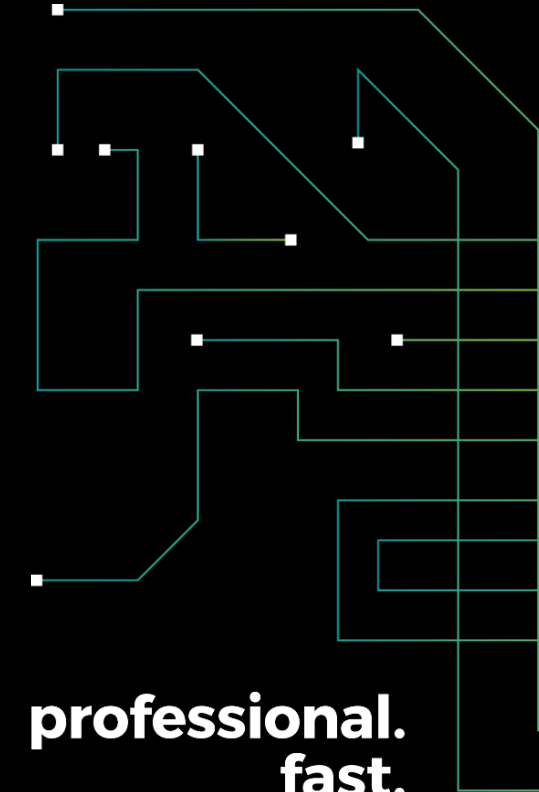


baseit

DATENSCHUTZ & COMPLIANCE NEU DEFINIERT MIT MICROSOFT 365 PURVIEW



professional.
fast.
secure.

11.4.2025/Purker Matthias

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

> Details

Description
This classifier 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-C, R, Ruby, Scala, Python Script

Recommendation

Classifier is ready for use

This classifier can now be used in purview

[Use classifiers to auto-apply sensitive info types](#)
[Use classifiers to auto-apply retention labels](#)

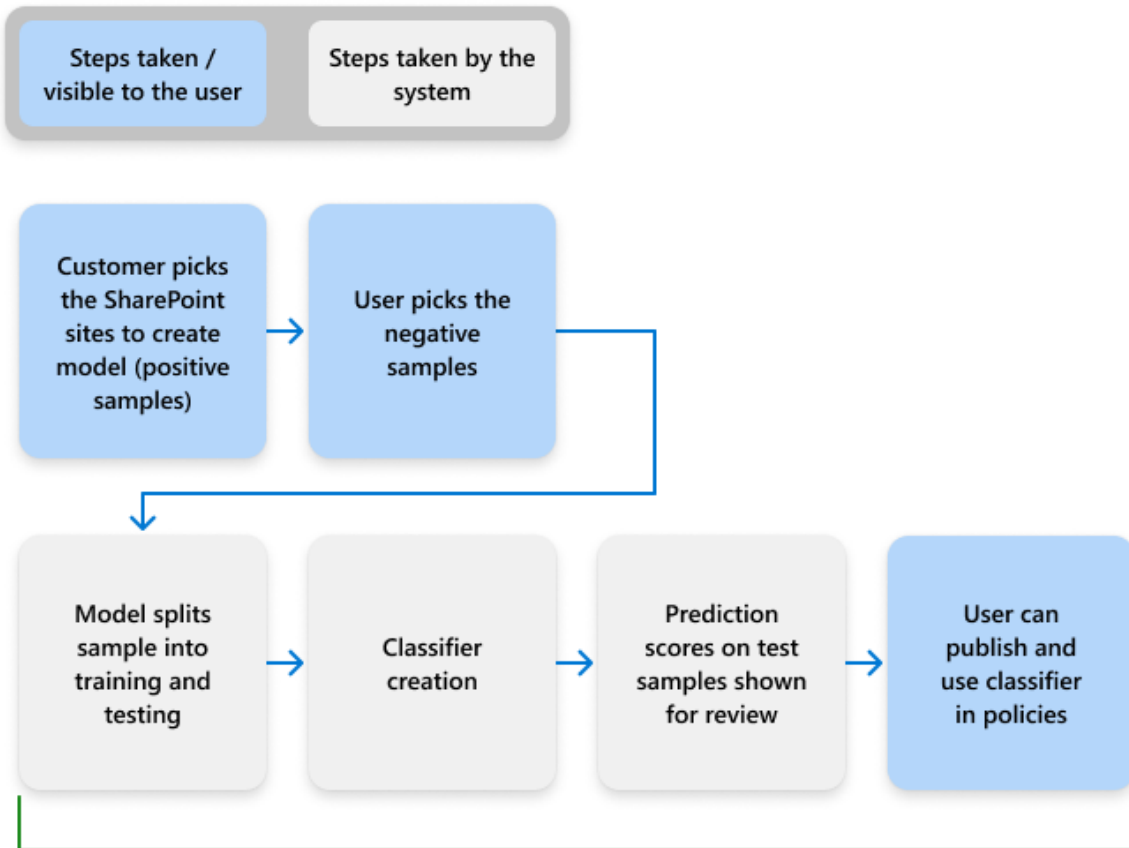
```
SSN, AccountID, FirstName, LastName, Email  
270 34 7884, B12345678, Richard, Jackson, Richard@contoso.onmicrosoft.com  
030 72 7381, B12345678, Sarah, Jefferson, sarah.jefferson@contoso.com  
757-85-7495, B12345678, Bradly, McGordon, bradly.mcgordon@testcompany.com  
781-70-8498, B12345678, Shiva, 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_date

EINFÜHRUNG MS PURVIEW

PROZESS ERSTELLUNG VON CLASSIFIER

Process flow for creating custom classifiers



Total processing time: Minimum = 3 hours; Maximum = 2 days



EINFÜHRUNG MS PURVIEW

ROLLEN IN PURVIEW

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

Role groups for Microsoft Purview solutions

Admin roles give users permission to view data and complete tasks in the Microsoft Purview portal. Give us

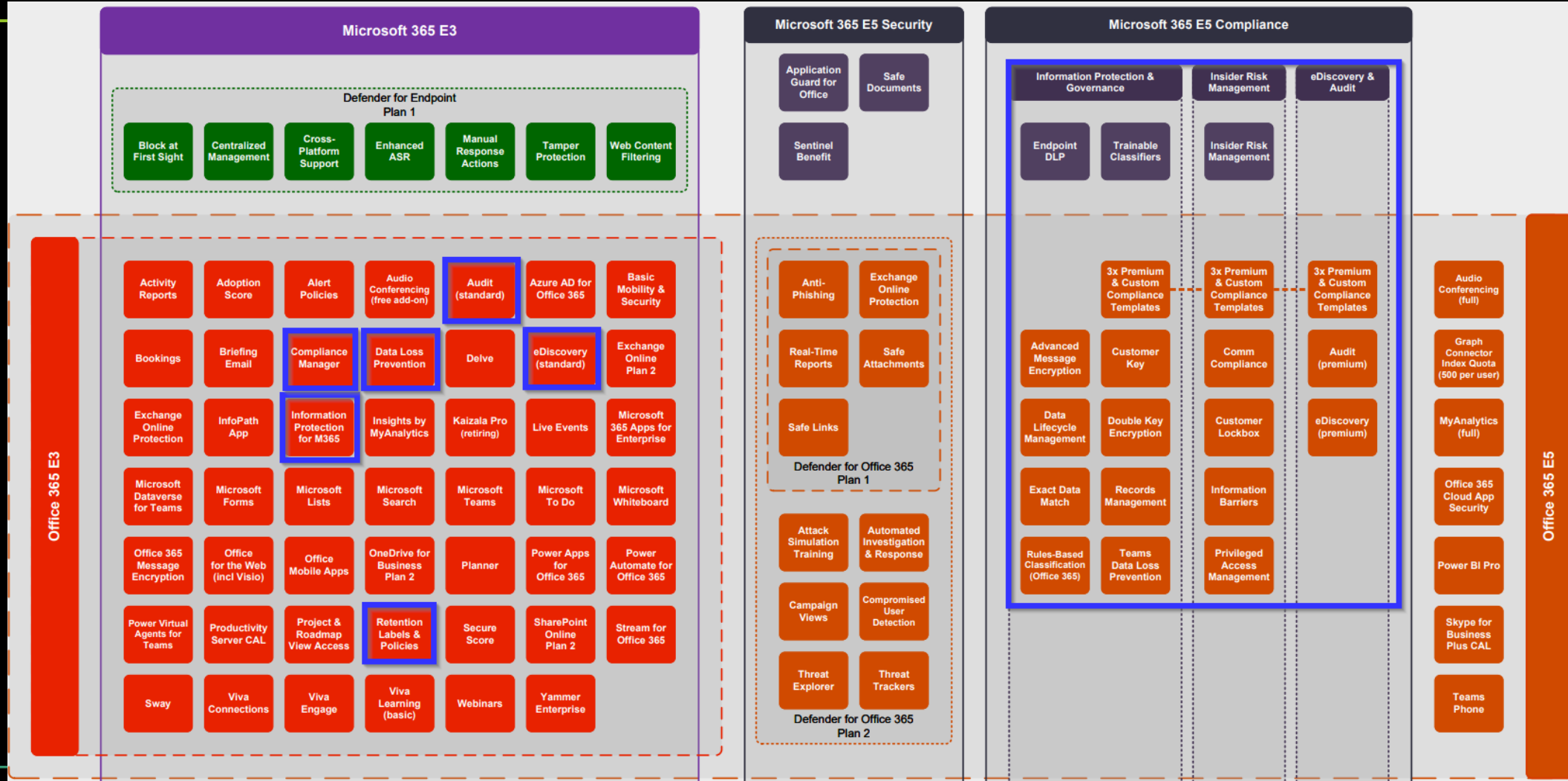
+ Create role group Refresh

Name	Type	Description
<input type="checkbox"/> Organization Management	Built-in	
<input type="checkbox"/> Compliance Administrator	Built-in	
<input type="checkbox"/> Purview Administrators	Built-in	
<input type="checkbox"/> Attack Simulator Administrators	Built-in	
<input type="checkbox"/> Attack Simulator Payload Authors	Built-in	
<input type="checkbox"/> Security Administrator	Built-in	
<input type="checkbox"/> Audit Manager	Built-in	
<input type="checkbox"/> Billing Administrator	Built-in	
<input type="checkbox"/> eDiscovery Manager	Built-in	
<input type="checkbox"/> Insider Risk Management	Built-in	
<input type="checkbox"/> Insider Risk Management Admins	Built-in	
<input type="checkbox"/> Insider Risk Management Analysts	Built-in	
<input type="checkbox"/> Insider Risk Management Investigators	Built-in	



EINFÜHRUNG MS PURVIEW

LIZENZÜBERBLICK



base it

EDISCOVERY & CONTENT SEARCH

EDISCOVERY & CONTENT

SUCHE IM O365 TENANT

Content Search

Speicherorte

Bestimmte Orte

Status	Ort	Enthalten
<input checked="" type="checkbox"/> Ein	Exchange-Postfächer Microsoft 365-Gruppen Teams Yammer-Benutzernachrichten	Alle Benutzer, C
<input checked="" type="checkbox"/> Ein	SharePoint-Sites OneDrive-Sites Microsoft 365-Gruppenwebsites Teamwebsites Yammer-Netzwerke	Alle Websites a
<input checked="" type="checkbox"/> Ein	Öffentliche Exchange-Ordner	Alle

+ Bedingung hinzufügen ▾

Ergebnisse exportieren

Grundgesamtheit

Durchsuchbare Dateien: Export

Ausgabeoptionen

- Alle Elemente, außer denen mit einem unbekanntem Format, sind verschlüsselt oder wurden aus anderen Gründen nicht indiziert.
- Alle Elemente, einschließlich derer mit einem unbekanntem 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 10:06:...
Nicht durchsuchbare ...	389 Ergebnisse	117.52 MB	29.4 10:06:...
Elemente gesamt	2 835 Ergebnisse	764.67 MB	29.4 10:06:...

EDISCOVERY & CONTENT-SEARCH

UNTERSCHIEDE CONTENT-SEARCH & EDISCOVERY

Inhaltssuche

- Suchen nach Inhalten
- Schlüsselwortabfragen und Suchbedingungen
- Exportieren von Suchergebnissen
- rollenbasierte Berechtigungen

eDiscovery (Standard)

- Suche und Export
- Case Management
- Rechtliche Aufbewahrung

eDiscovery (Premium)

- Verwaltung von Verwahrer - Benachrichtigungen zur Aufbewahrung gesetzlicher Aufbewahrung -
- Erweiterte Indizierung
- Überprüfungssatzfilterung
- Tagging
- Analysen
- Vorhersagecodierungsmodelle und mehr...



DATA LIFECYCLE MANAGEMENT

DATA LICECYCLE MANAGEMENT

EINFÜHRUNG

- Wie lange müssen Daten aufbewahrt 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 LIFECYCLE MANAGEMENT

ERSTELLUNG RETENTION-LABEL

Define label settings

We'll apply the settings you choose to labeled items

Retain items forever or for a specific period

Create retention label

Choose what happens after the retention period

These settings determine what happens to items when the retention period ends.

- Delete items automatically**
We'll permanently remove labeled items from wherever they're stored.
- Start a disposition review**
Let the disposition reviewers you assign in the next step decide if items can be safely deleted or whether other actions (such as changing the retention period) should be taken. [Learn more](#)
- Change the label**
You can extend the period by choosing an existing label to replace this one with. [Learn more about relabeling items](#)
- Run a Power Automate flow**
Customize what happens to labeled items with a Power Automate flow. You can run a flow to meet a specific business need, such as moving labeled items to a certain location or sending email notifications. [Learn more about running a Power Automate flow](#)
- Deactivate retention settings**
Labeled items won't be retained or deleted when their retention settings are deactivated. You'll have to manually remove any items that you want deleted.

When items were last modified

When items were labeled

Product lifetime(event type)

Expiration or termination of contracts and agreements(event type)

Employee activity(event type)



DATA LIFECYCLE MANAGEMENT


VERÖFFENTLICHUNG EINES LABELS

Publish labels so users can apply them to their content.





- ✓ Choose labels to publish
- ✓ Administrative Units
- **Scope**
- Publish to users and groups
- Name your policy
- Finish

Choose where to publish labels

When published, users in your organization will be able to apply this label to items in the locations you choose.

 You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

- All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
- Let me choose specific locations.

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	 Exchange mailboxes	All mailboxes Edit	None Edit
<input checked="" type="checkbox"/> On	 SharePoint classic and communication sites	All sites Edit	None Edit
<input checked="" type="checkbox"/> On	 OneDrive accounts	All user accounts Edit	None Edit
<input checked="" type="checkbox"/> On	 Microsoft 365 Group mailboxes & sites	All microsoft 365 groups Edit	None Edit

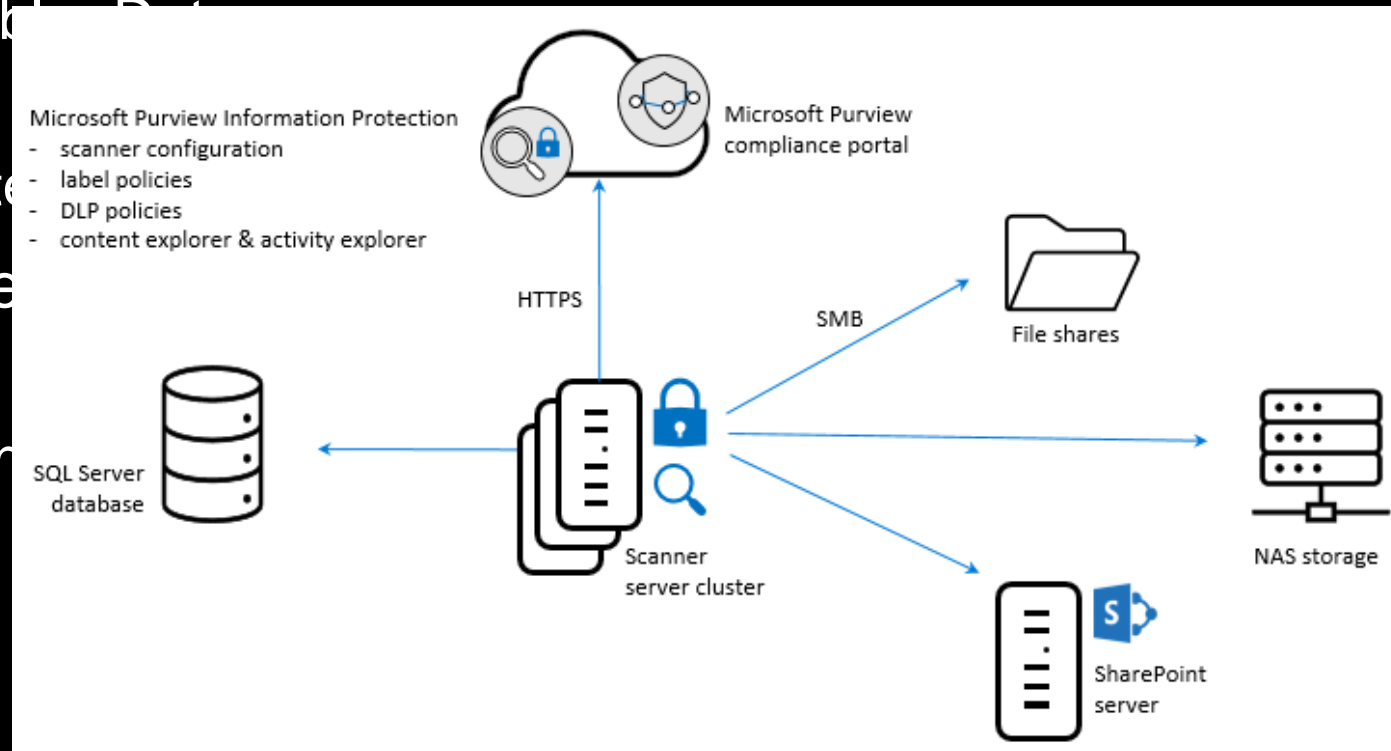


DATA LOSS PREVENTION (DLP)

DATA LOSS PREVENTION (DLP)

EINFÜHRUNG

- Ziel von DLP :
 - Erkennung des Datenflusses sensibler Daten
 - Schutz vor unsicherer Freigabe
 - Verhinderung unangemessener Datenfreigabe
- OnPremise & Endpoint Integrationen
 - Defender for Endpoint
 - Überwachung von Client-Aktivitäten



DATA LOSS PREVENTION (DLP)

RICHTLINE

Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

+ Create rule

2 items

Name	Status				
Low volume of content detected Germany Financial Data	<input checked="" type="checkbox"/> On				
Conditions Content contains any of these sensitive info types: Credit Card Number EU Debit Card Number					
Content is shared from Microsoft 365 with people outside my organization					
Actions Notify users with email and policy tips Send alerts to Administrator					
High volume of content detected Germany Financial Data	<input checked="" type="checkbox"/> On				
Conditions Content contains any of these sensitive info types: Credit Card Number EU Debit Card Number					
Content is shared from Microsoft 365 with people outside my organization					
Actions Notify users with email and policy tips Restrict access to the content for external users Send incident reports to Administrator Send alerts to Administrator					

Choose where

We'll apply the policy to data t

If your role group permissions are [permissions](#).

Protecting sensitive info in on-pre capability. [Learn more about the](#)

Pay-as-you-go billing needs to be

Location

- Exchange email
- SharePoint sites
- OneDrive accounts
- Teams chat and chan
- Devices
- Instances
- On-premises reposi
- Fabric and Power BI v

Name

Create a D

Name *

Germany I

Description

Helps dete



DATA LOSS PREVENTION (DLP)

Edit rule

Use rules to define the type of sensitive information

Name *

Low volume of content detected Germany Financie

Description

Conditions

We'll apply this policy to content that matches the

Content contains

Group name *

Default

Sensitive info types

Credit Card Number

EU Debit Card Number

Add ▾

Create group

AND

Content is shared from Microsoft 365

Detects when content is sent in email message

with people outside my organization

Applies only to content shared from Exchange

+ Add condition ▾

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

Email notifications

[Preview and edit notification email](#)

Notify the user who sent, shared, or last modified the content.

Notify these people:

- The person who sent, shared, or modified the content
- Owner of the SharePoint site or OneDrive account
- Owner of the SharePoint or OneDrive content

Send the email to these additional people:

[+ Add or remove users](#)

Attach matching email message to the notification (applies only to Exchange)

Policy tips

Support and behavior for policy tips varies across apps and platforms. [Learn where policy tips are supported](#)

- Customize the policy tip text
- Show the policy tip as a dialog for the end user before send (available for Exchange workload only)
 - To help ensure all email messages display the pop-up before they're sent, you must first configure Group Policy Object (GPO) settings to allow for full evaluation. [Learn more](#)
- Provide a compliance URL for the end user to learn more about your organization's policies (available for Exchange workload only)

User overrides

Allow overrides from Microsoft 365 files and Microsoft Fabric items

Allow users to override policy restrictions in Fabric (including Power BI), Exchange, SharePoint, OneDrive, and Teams.

Incident reports

Use this severity level in admin alerts and reports:

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

Insider risk level for Adaptive Protection is

Content is received from

Under IP address is

When the policy tip

Contains words

Matches patterns

Site contains words or

Site matches patterns

ier of

not be scanned

complete scanning

Content is password

operator

of these ▾

number of

is

contains words

matches patterns

Content contains words or

Content matches patterns

contains words or phrases

matches patterns

ty is

Equals or is greater than

It contains words or phrases

It matches patterns

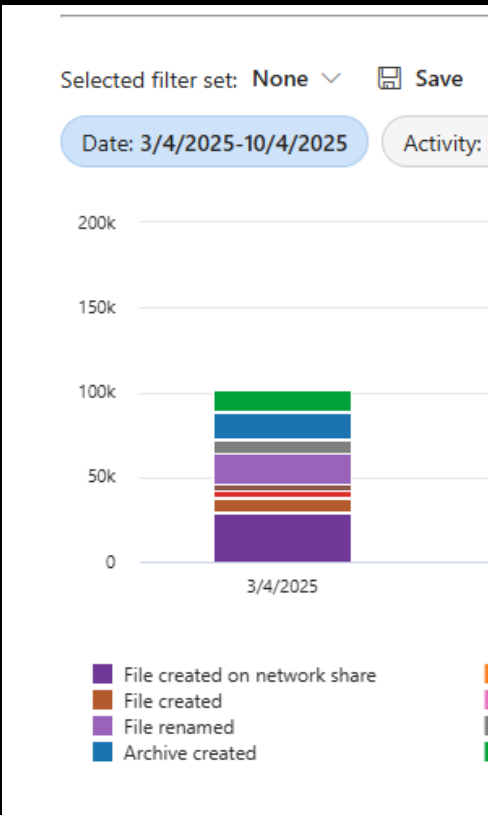
words or phrases

patterns

DATA LOSS PREVENTION (DLP)

PRAXISBEISPIELE

■ Monitoring von



Data explorer

4 locations with items containing All Full Names

Choose a classifier or a label

Filter on labels, classifiers, or categories

Sensitive info types

- All Full Names: 5315
- Philippines Passport Number: 2638
- buchhaltung: 1883
- Indonesia Passport Number: 1462
- All Medical Terms And Conditions: 1443

[See all 180](#)

Sensitivity labels

- Öffentlich: 14
- PAG Geheim: 7
- Befunde: 6
- Intern: 5
- 201001 - Streng Vertraulich Arial: 5

[See all 13](#)

Microsoft 365

Export

Data source	Sensitive info types	Sensitivity labels	Trainable classifiers	EDM classifiers	Retention labels	Items
Copilot	All Full Names, Philip...		Customer Complaint...	None		2429
OneDrive	All Full Names, Philip...	Öffentlich, Intern, 20...	Customer Complaint...	None		290
SharePoint	All Full Names, Philip...	Öffentlich, Befunde, I...	Customer Complaint...	None		151
Teams	All Full Names, Philip...		Customer Complaint...	None		2445

INSIDER RISK MANAGEMENT

INSIDER RISK MANAGEMENT

EINFÜHRUNG

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

Policy indicators

Built-In Indicators Custom Indicators

Insider risk policy templates define the type of risk activities you want to detect and investigate. Each template is based on indicators that trigger alerts when users perform related activities. Cho

⚠ Set up billing to use pay-as-you-go indicators. Cloud service, cloud storage, generative AI, and Fabric indicators have switched to our pay-as-you-go billing model. To use these indicators, —no upfront costs, no commitment. [Learn more about pay-as-you-go billing](#)

+ New indicator variant

- Office indicators
- Device indicators
- Microsoft Defender for Endpoint indicators (preview)
- Risky browsing indicators (preview)
- Physical access indicators
- Microsoft Defender for Cloud Apps indicators
- Health record access indicators
- Cumulative exfiltration detection
- Risk score boosters
- Cloud storage indicators
- Cloud service indicators
- Generative AI apps (preview) New
- Microsoft Fabric indicators
- Communication compliance indicators New
- Microsoft Entra ID Protection indicators (preview) New
- Data loss prevention (DLP) alert indicators (preview) New

INSIDER RISK MANAGEMENT

RICHTLINIEN-BEISPIEL

Choose a policy template

Insider risk management > New insider risk policy

Policy templates specify the

Data theft

Data theft by departing

Data leaks

Data leaks

Data leaks by risky user

Data leaks by priority user

Risky AI usage (preview)

Risky AI usage (preview)

Security policy violations (preview)

Security policy violations (preview)

Security policy violations by departing users (preview)

Security policy violations by risky users (preview)

Security policy violations by priority users (preview)

- Policy template
- Name and description
- Admin units
- Users and groups**
- Content to prioritize
- Triggering event
- Indicators
- Finish

Choose users, groups, & adaptive scopes

Choose users, groups, and adaptive scopes within your organization who this policy will apply to.

- All users, groups, and adaptive scopes
- Specific users, groups, and adaptive scopes

User performs an activity matching specified user policy.

Activities detected include ⓘ

- Downloading files from SharePoint
- Printing files
- Copying data to personal cloud storage services



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](#)

- Downloading content from SharePoint
- Sending email with attachments to recipients outside the organization
- Printing files
- Creating or copying files to USB
- Using a browser to upload files to the web
- 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](#)

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

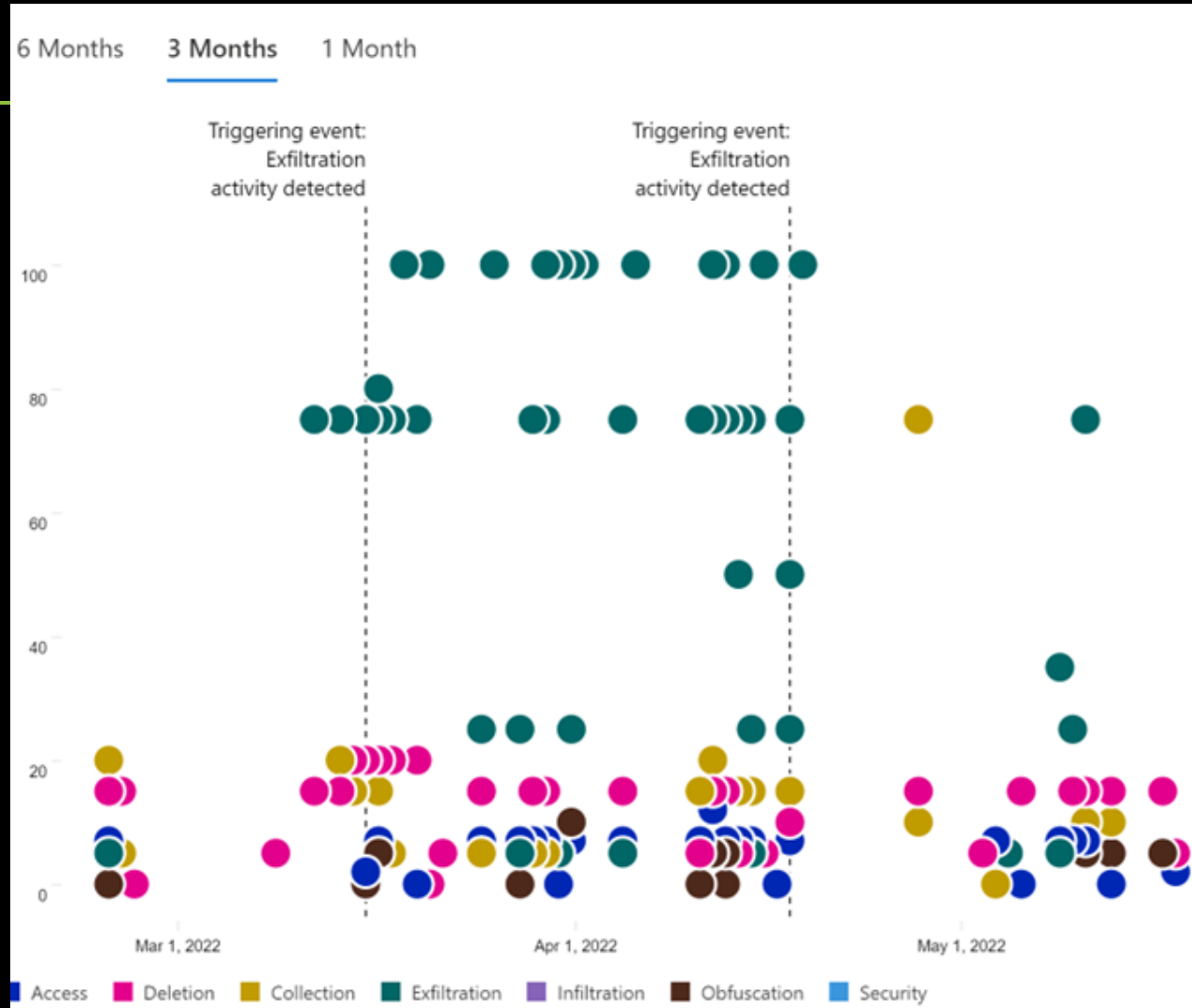
Choose threshold type for indicators

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 > Alerts > Alert: Confidentiality obligation during departure

Alert: Confidentiality obligation during departure

High severity Risk score: 90/100 Alert created on Oct 24, 2024

Only activity with priority content was scored for this alert

Activity that generated this alert

Data exfiltration: Files uploaded to cloud storage
87/100 High severity | Oct 23, 2024 (UTC)
2 events: Files downloaded from 1 unallowed site
2 events: Files that have labels applied, including: Project Alpha
[View all activity](#)

[Reduce alerts for this activity](#)

Triggering event

Feb 7, 2024 (UTC)
Sending email with attachments to recipients outside the organization

User details

#Anonymized#EAAAAX/0qYHAUM637U+DMdGtK(A6I)/QwDdHr3AHNEkui+ga5EXMZ3KPysCaVSuqsp1GZZgdTzBefaCL6Hm31wbtmUo=
[View all activity](#)

User alert history

Last 30 days

Data leaks quick policy -ankitapal	1 alert
Data test	1 alert

[View full user history](#)

All risk factors Activity explorer **User activity** Forensic evidence

Filters: [Show: All scored activity for this user](#) [Risk category: Any](#) [Activity type: Any](#) [Reset all](#)

Sort by: Date occurred

Communication risk: Messages violating financial regulatory compliance shared

October 23, 2024 (UTC) | Risk score: 25/100
15 events: Messages violating financial regulatory compliance classifiers, including: Customer Complaints, Regulatory Collusion, Stock Manipulation, Gifts & Entertainment, Unauthorized Disclosure, Money Laundering shared with 10 users

Data exfiltration: Files copied to USB device

October 23, 2024 (UTC) | Risk score: 79/100
2 events: Files copied to USB devices
2 events: Files containing sensitive info, including: Credit Cards

Data exfiltration: Files copied to USB device

October 22, 2024 (UTC) | Risk score: 79/100
2 events: Files copied to USB devices
2 events: Files containing sensitive info, including: Credit Cards

Data exfiltration: Files copied to USB device

October 22, 2024 (UTC) | Risk score: 79/100
2 events: Files copied to USB devices
2 events: Files containing sensitive info, including: Credit Cards

Data exfiltration: Files copied to USB device

October 22, 2024 (UTC) | Risk score: 79/100
2 events: Files copied to USB devices
2 events: Files containing sensitive info, including: Credit Cards

Resignation date

Oct 5, 2024 Oct 28, 2024

Access Deletion Collection Exfiltration Infiltration Obfuscation Security Custom Indicator Defense Evasion Privilege Escalation Sequence Cumulative Exfiltration



INSIDER RISK MANAGEMENT

Microsoft Purview Insider Risk Management

Continuously evaluate
and publish risk level.

Microsoft Purview Data Loss Prevention

Dynamically prevent
unauthorized **use**.

Microsoft Entra Conditional Access

Dynamically prevent
unauthorized **access**.

Microsoft Purview Data Lifecycle Management

Dynamically **preserve**
deleted files.



Elevated
risk



Block action



Block access



Preserve data



Moderated
risk



Block action,
allow override



Terms of use



Minor
risk



Policy tip

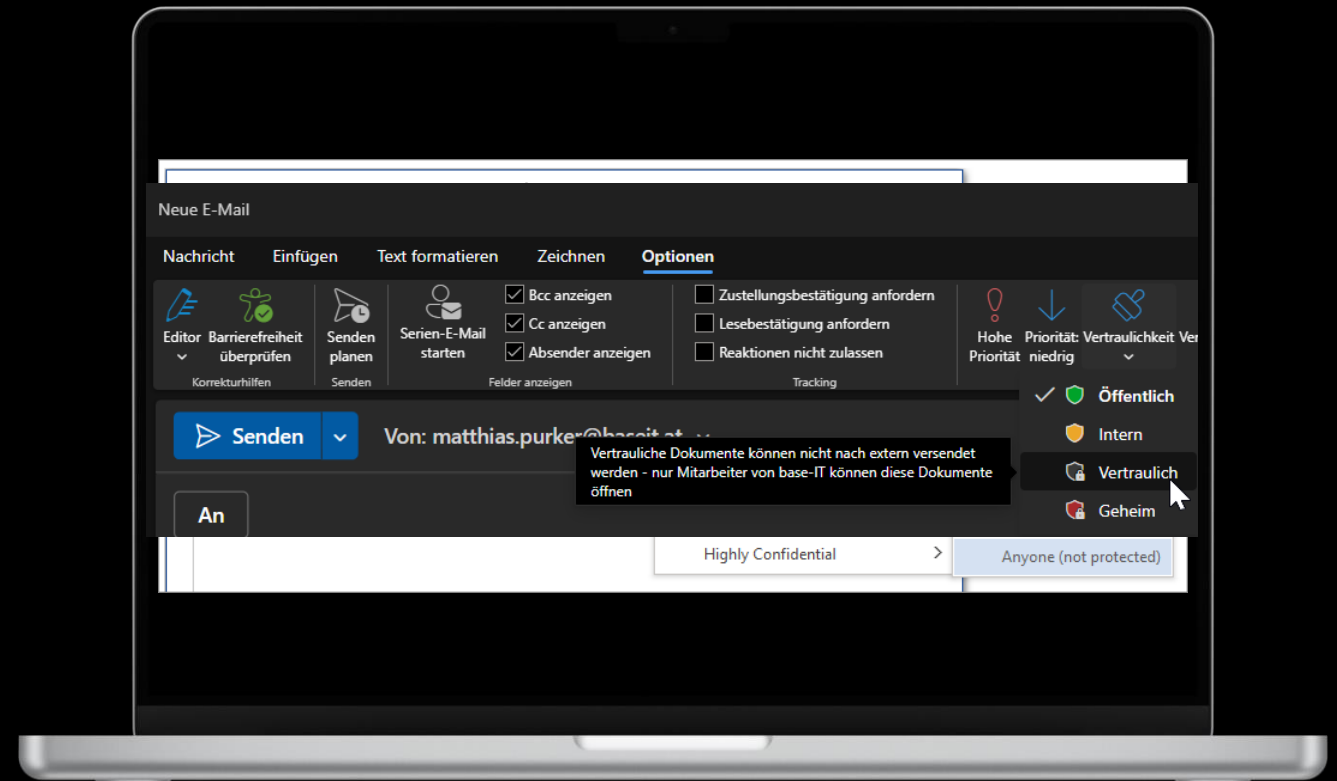


AZURE INFORMATION PROTECTION (AIP)

AZURE INFORMATION PROTECTION

ÜBERSICHT

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



AZURE INFORMATION PROTECTION

SENSITIVITY LABEL

Name * ⓘ

Geheim

Display name * ⓘ

Intern

Label priority ⓘ

ⓘ By default, this label will be assigned the highest priority, but you can change this after it's c

Highest

Description for users * ⓘ

Beschreibung welche Dokumente mit dieser Klassifizierung versehen werden sollen

Description for admins ⓘ

Enter a description that's helpful for admins who will manage this label

Label color ⓘ



Define the scope for this label

Labels can be applied to data assets and containers (like SharePoint sites and Teams). Let us know where you want this label to be used so we can show you the related protection settings. [Learn more about label scopes](#)

Files & other data assets

Label files and data assets in Microsoft 365, Microsoft Fabric (includes Power BI), Microsoft Azure.

Emails

Label messages sent from all versions of Outlook.

Meetings

Label calendar events and meetings schedules in Outlook and Teams.

ⓘ Parent label will automatically inherit meeting scope from sub labels

Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, SharePoint sites, and Loop workspaces.

ⓘ **Wondering where the schematized data assets option went?** To apply this label to data assets in Azure, select "Files and other data assets" above and then add this label to an auto-labeling policy that's scoped to Azure storage and Azure SQL. [Learn more](#)



AZURE INFORMATION PROTECTION

SENSITIVITY LABEL

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. [Learn more about content marking](#)

ⓘ All content marking will be applied to documents but only the header and footer will be applied to email messages. If you check the header and footer will also be applied to meeting invites.

Content marking



Add a watermark

 Customize text

Add a header

 Customize text

Add a footer

 Customize text

Customize footer text

This text will appear as a footer on labeled email messages and documents.

Footer text * ⓘ

Fußzeile

Font size

10

Font color

Black

Align text

Left



AZURE INFORMATION PROTECTION

SENSITIVITY LABEL

Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. [Learn more about auto-labeling for Microsoft Purview](#)

① To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. [Learn more about auto-labeling policies](#)

Auto-labeling for files and emails



① Since encryption is turned on, a large amount of content might be automatically encrypted when this label is applied. Turning on encryption impacts Office files (Word, PowerPoint, Excel) and PDF files that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

^ Detect content that matches these conditions

^ Content contains

Group name *	Group operator
<input type="text" value="Default"/>	<input type="text" value="Any of these"/>
Add	
<ul style="list-style-type: none">Sensitive info typesTrainable classifiers	
+ Add condition	



AZURE INFORMATION PROTECTION

SENSITIVITY LABEL

Define protection settings for groups and sites

Protection settings

These settings apply to teams, groups, and sites that have this label. [Learn more about these settings](#)

Privacy and external user access

Control the level of access that internal and external users will have to the content.

External sharing and Conditional Access

Control external sharing and configure Conditional Access settings to protect content.

Private teams discoverability and shared channel settings

Decide whether private teams will be discoverable in searches and content suggestions.

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

Anyone ⓘ

Users can share files and folders using links that don't require sign-in.

New and existing guests ⓘ

Guests must sign in or provide a verification code.

Existing guests ⓘ

Only guests in your organization's directory.

Only people in your organization

No external sharing allowed.

Use Microsoft Entra Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.



AZURE INFORMATION PROTECTION

LABEL PUBLISHING

■ Verteilung der Labels auf Usergruppen

Policy settings

Configure settings for the labels included in this policy.

- Users must provide a justification to remove a label or lower its classification**
Users will need to provide a justification before removing a label or replacing it with one that has a lower-order number. You can use activity explorer to review label changes and justification text.
- Require users to apply a label to their emails and documents**
Users will be required to apply labels before they can save documents or send emails (only if these items don't already have a label applied).
 ⓘ Support and behavior for this setting varies across apps and platforms. [Learn more about managing sensitivity labels](#)
- Require users to apply a label to their Fabric and Power BI content**
Users will be required to apply labels to unlabeled content they create or edit in Fabric and Power BI. [Learn more about mandatory labeling in Fabric and Power BI](#)
- Provide users with a link to a custom help page**
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. [Learn more about this help page](#)



PURVIEW

STÄRKEN DER KOMBINATION

Information Protection

The screenshot shows the 'Overview' page for Information Protection in Microsoft Purview. It features a navigation sidebar on the left with options like Home, Data classification, Overview, Classifiers, Content explorer, Activity explorer, Solutions, Information protection, Labels, Label policies, Auto-labeling, and Custom navigation. The main content area includes a sub-header 'Overview' with a brief description. Below this, there are two main sections: 'Trainable classifiers used most in your content' and 'Sensitive info types used most in your content'. Each section contains a horizontal bar chart with various categories and a 'View all' link. At the bottom, there are links for 'Top retention labels applied to content', 'Daily labeling activity by users', and 'Top activities detected'.

Data Loss Prevention

The screenshot shows the 'Overview' page for Data Loss Prevention in Microsoft Purview. It features a navigation sidebar on the left with options like Home, Solutions, Data loss prevention, Overview, Policies, Alerts, Endpoint DLP settings, Activity explorer, and Custom navigation. The main content area includes a sub-header 'Overview' with a brief description. Below this, there are two main sections: 'Protect sensitive financial, healthcare and HR info' and 'Stay informed about DLP'. The first section includes a 'Get started' button and a 'View detected documents' button. The second section includes a 'DLP resources' section with links to 'Follow setup guide', 'Read the official DLP docs', and 'Get the latest news on DLP'. At the bottom, there are links for 'Device health overview', 'Adaptive Protection', and 'Extend protection to auto-labeling'.

Insider Risk Management

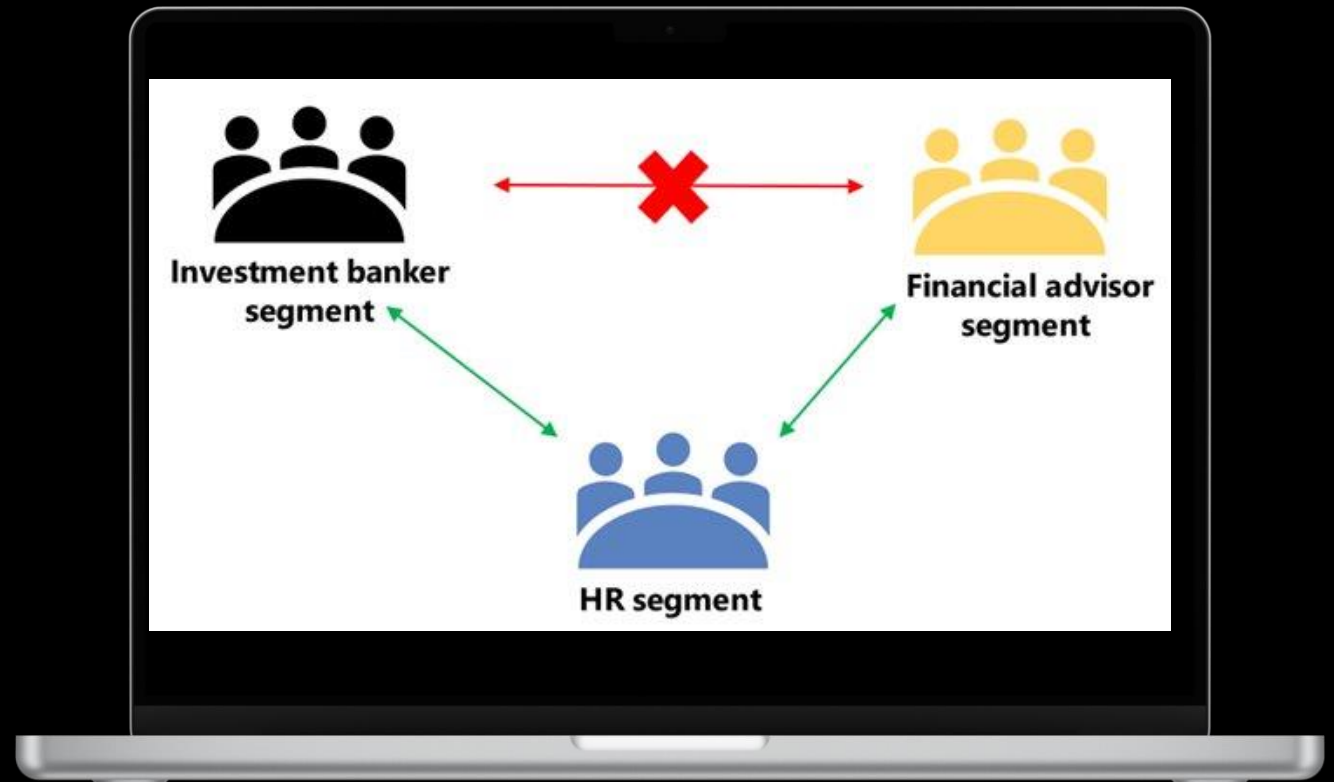
The screenshot shows the 'Results from the last scan for risk activities' page in Microsoft Purview. It features a navigation sidebar on the left with options like Home, Insider risk management, Analytics, Results from the last scan for risk activities, Insights from September 13 - September 20, Potential data leak activities, Recommendation: Set up a 'Data leak' policy, Potential data theft activities, and Activity from 219 users scanned. The main content area includes a sub-header 'Results from the last scan for risk activities' with a brief description. Below this, there are two main sections: 'Potential data leak activities' and 'Potential data theft activities'. Each section includes a 'View details' button and a 'View all activities' button.



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

Overview | Improvement actions | Solutions | Assessments | Regulations | Alerts | Alert policies

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

Overall compliance score

Your compliance score: 49%

12000/24471 points achieved

Your points achieved: 115 / 12,163

Microsoft managed points achieved: 11,885 / 12,308

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

Key improvement actions

Improvement action	Impact	Test status	Group	Action type
Enable self-service password reset	+27 points	Partially tested	Default Group	Technical
Use boundary protection devices for unclassified data	+27 points	None	Default Group	Technical
Provide just-in-time notification or system usage reporting	+27 points	None	Default Group	Technical
Disable 'Domain member: Disable machine accounts' policy	+27 points	None	Default Group	Technical
Turn on email scanning for antivirus solution	+27 points	None	Default Group	Technical
Enable 'Consistent MIME Handling'	+27 points	None	Default Group	Technical
Block email application from creating child processes	+27 points	None	Default Group	Technical
Enable 'MIME Sniffing Safety Feature'	+27 points	None	Default Group	Technical
Block outdated ActiveX controls	+27 points	None	Default Group	Technical

Solutions that affect your score

Solution	Score contribution	Remaining actions
Attack Simulation Tr...	0/9 points	1
Audit	0/65 points	11
Azure	0/121 points	7
Azure Active Directory	61/1331 points	63
Communication com...	0/40 points	6
Compliance Manager	0/3195 points	397
Data classification	0/85 points	5
Data lifecycle manag...	0/262 points	12
Data loss prevention	0/280 points	12



COMPLIANCE MANAGER

IMPROVEMENT ACTIONS

Create assessment

Automate compliance posture monitoring across your multicloud data estate with our updated assessments. [Learn more about multicloud support](#)

Compliance Manager

- Overview
- Improvement actions
- Solutions
- Assessments
- Regulations
- Policies
- Alerts
- Reports

Related solutions

- Data Lifecycle Management
- Data Loss Prevention

Improvement actions

Improvement actions provide guidance on task completion which can improve your org's compliance score. Action points can take up to 24 hours to update. [Learn more about improvement actions](#)

↓ Export actions
↑ Update actions
✓ Accept all updates
📄 Assign to user
500 items

Search

☰ Group

Filter ✕ Reset 🔍 Filters

Regulations: Any

Solutions: Any

Groups: Any

Test Status: Any

Categories: Any

Testing type: Any

Service: Any

Role type: Any

+3 more

<input type="checkbox"/> Improvement action	Point...	Service	Regulations	Grou...	Solutions	Assessments	Categories	Test status	Action type
<input type="checkbox"/> Implement account lockout	0/54	Microsoft 365	(1)	(2) Custo...	Microsoft Entr...	(2) Custom Assessment Microsoft 365 D...	Protect infor...	• None	Technical
<input type="checkbox"/> Notify upon system usage or ne...	0/1	Microsoft 365	(1)	(1) Defaul...	Compliance ...	(1) Data Protection Baseline	Manage com...	• None	Operational
<input type="checkbox"/> Enforce immediate temporary p...	0/54	Microsoft 365	(1)	(2) Custo...	Microsoft 365...	(2) Custom Assessment Microsoft 365 D...	Control access	• None	Technical
<input type="checkbox"/> Review Policy Violation Alerts	0/1	Microsoft 365	(1)	(1) Defaul...	Communicati...	(1) Data Protection Baseline	Manage inter...	• None	Operational
<input type="checkbox"/> Implement spam filter	0/54	Microsoft 365	(1)	(2) Custo...	Exchange Onli...	(2) Custom Assessment Microsoft 365 D...	Protect infor...	• None	Technical

40 | professional. fast. secure.



baseit

Haider Straße 23 | 4052 Ansfelden | AT
+43 7229 87800 - 0 | office@baseit.at |
www.baseit.at

[Base-IT GmbH \(unserebroschuere.at\)](http://Base-IT GmbH (unserebroschuere.at))



Management System
ISO/IEC 27001:2013
www.tuv.com
ID 900002884

