

Compliance Solutions for Microsoft 365



Vlad Catrinescu

Microsoft MVP

@vladcatrinescu <https://VladTalksTech.com>



Overview



Introduction to regulatory compliance

Microsoft's privacy principles

The Microsoft Service Trust portal

Microsoft Purview compliance solutions



Introduction to Regulatory Compliance



Regulatory Compliance for IT Professionals



Set of digital security requirements and practices

Ensure that a company's business processes are secure

Usually done to satisfy a 3rd party

- **Government**
- **Security framework**
- **Client**



Popular IT Compliance Standards & Regulations

GDPR

HIPAA

NIST SP 800-171

PCI-DSS



Example Compliance Needs



Granting individuals the right to access their data at any time



Granting individuals the right to correct or delete data about them if needed



Introducing retention periods that dictate a minimum or maximum amount of time data should be stored



Enabling governments and regulatory agencies the right to access and examine data when necessary



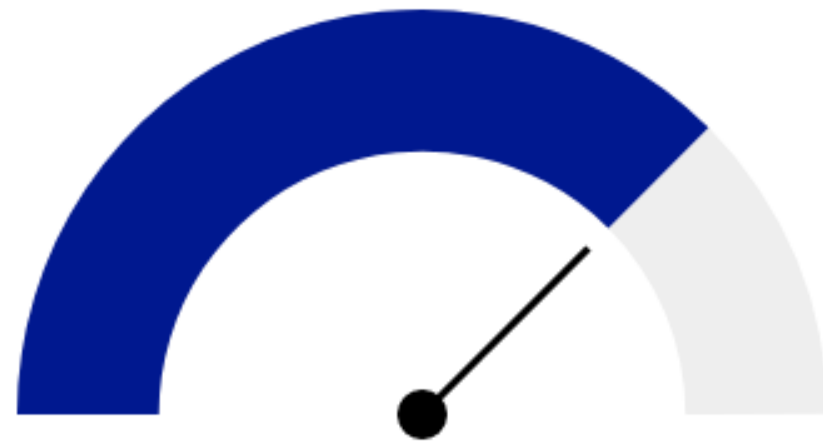
Defining rules for what data can be processed and how that should be done



Compliance in the Cloud

Overall compliance score

Your compliance score: 75%



12159/16167 points achieved

Your points achieved ⓘ

0 / 4008

Microsoft managed points achieved ⓘ

12159 / 12159

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

Security in the cloud is a partnership

– So is compliance!

Part of the requirements will be done by Microsoft

– Documentation in the Service Trust Portal

A lot of it depends on you



Microsoft's Privacy Principles



Microsoft's Privacy Principles



You're entrusting the provider with one of your most valuable assets

– Your data

Microsoft has six key privacy principles when making decisions around data



Microsoft's Six Key Privacy Principles

Control

We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency

We will be transparent about data collection and use so you can make informed decisions.

Security

We will protect the data you entrust to us through strong security and encryption.

Strong legal protections

We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

No content-based targeting

We will not use your email, chat, files or other personal content to target ads to you.

Benefits to you

When we do collect data, we will use it to benefit you and to make your experiences better.



The Microsoft Service Trust Portal



Service Trust Portal

The Service Trust Portal is a single location where you can find audit reports, Pen Tests, Security Assessments, and more information on how Microsoft manages security, privacy and compliance.

<https://servicetrust.microsoft.com/>



Free offering

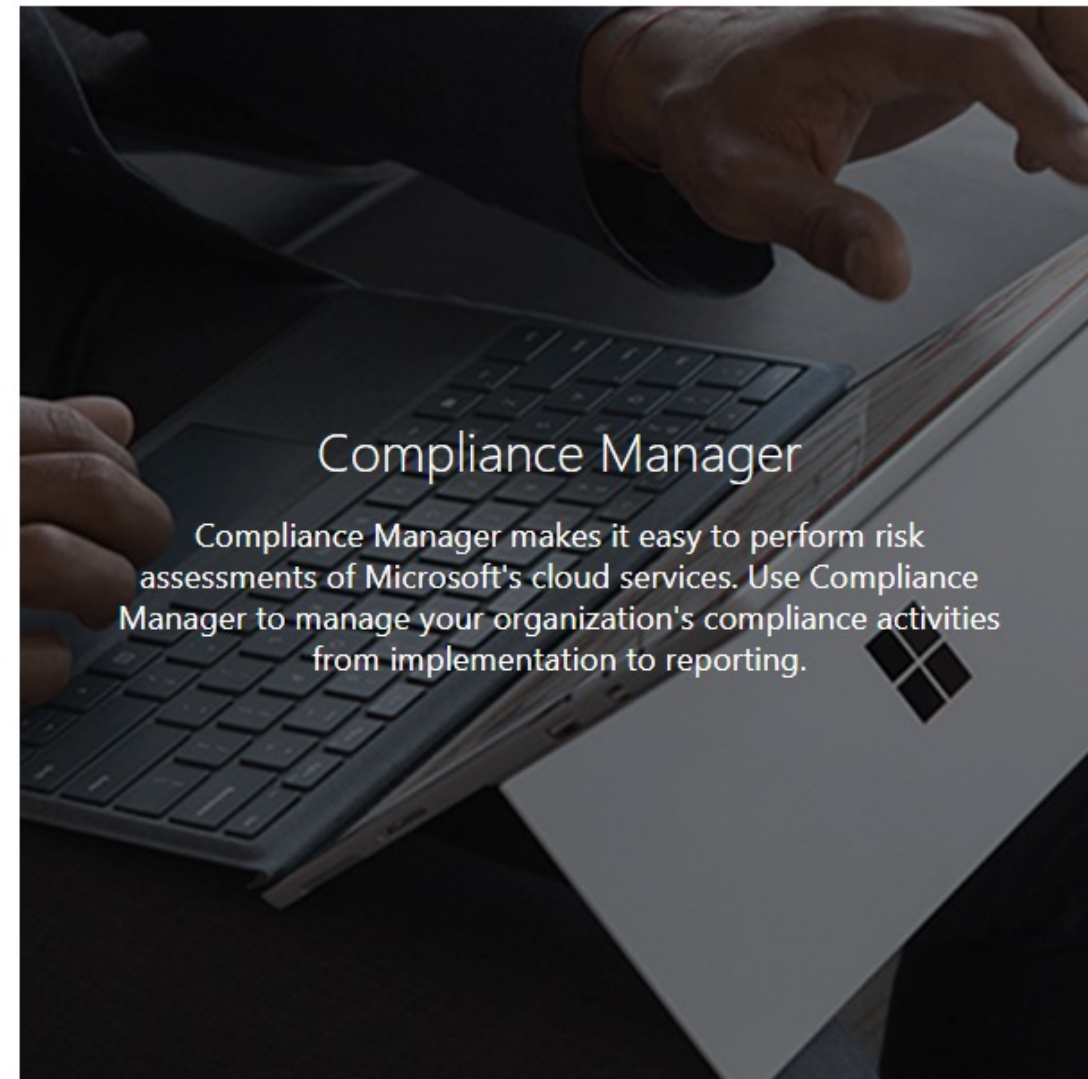
Some documents do require you to sign in your Microsoft 365 account

Signing in also gives you access to the “My Library” feature

Allowing you to save documents in an easy location

Also allows you to get updates to those documents

Documents & Resources



Compliance Manager

Compliance Manager makes it easy to perform risk assessments of Microsoft's cloud services. Use Compliance Manager to manage your organization's compliance activities from implementation to reporting.

Pen Tests & Security Assessments

View reports from independent third-party penetration tests and security assessments of Microsoft's cloud services

Azure Blueprints

Define a repeatable set of Azure resources that implement and adhere to your organization's standards, patterns, and requirements and rapidly build new environments with a set of built-in components to speed up development and delivery

White Papers, FAQs, & Compliance Guides

Review the wealth of available security implementation and design information with the goal of making it easier for you to meet regulatory compliance objectives by understanding how Microsoft Cloud services keep your data secure



Demo



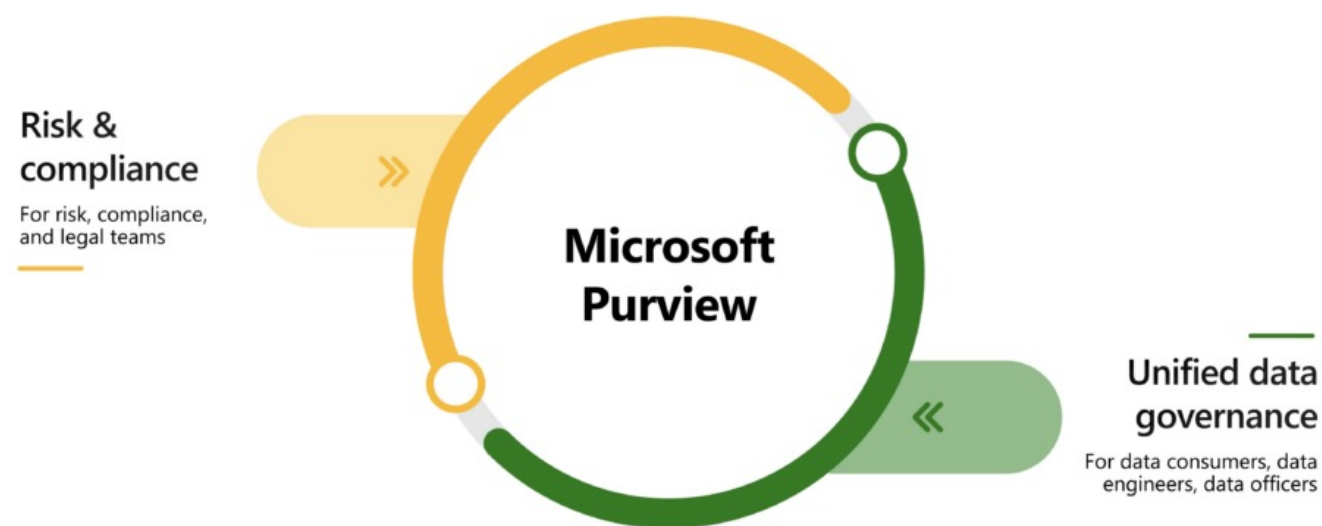
The Microsoft Service Trust Portal



Microsoft Purview Compliance Solutions



Microsoft Purview



Microsoft rebranded all their compliance solutions in April 2022

- Microsoft Purview suite of solutions

Many existing products have been rebranded

- Adding Purview inside the name

Read the announcement

- <https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/>



Microsoft Purview Products in This Course

**Microsoft Purview
Compliance
Manager**

**Microsoft Purview
Information
Protection**

**Microsoft Purview
Data Loss
Prevention**

**Microsoft Purview
Insider Risk
Management**

**Microsoft Purview
eDiscovery**

**Microsoft Purview
Audit**



Microsoft Purview Compliance Portal

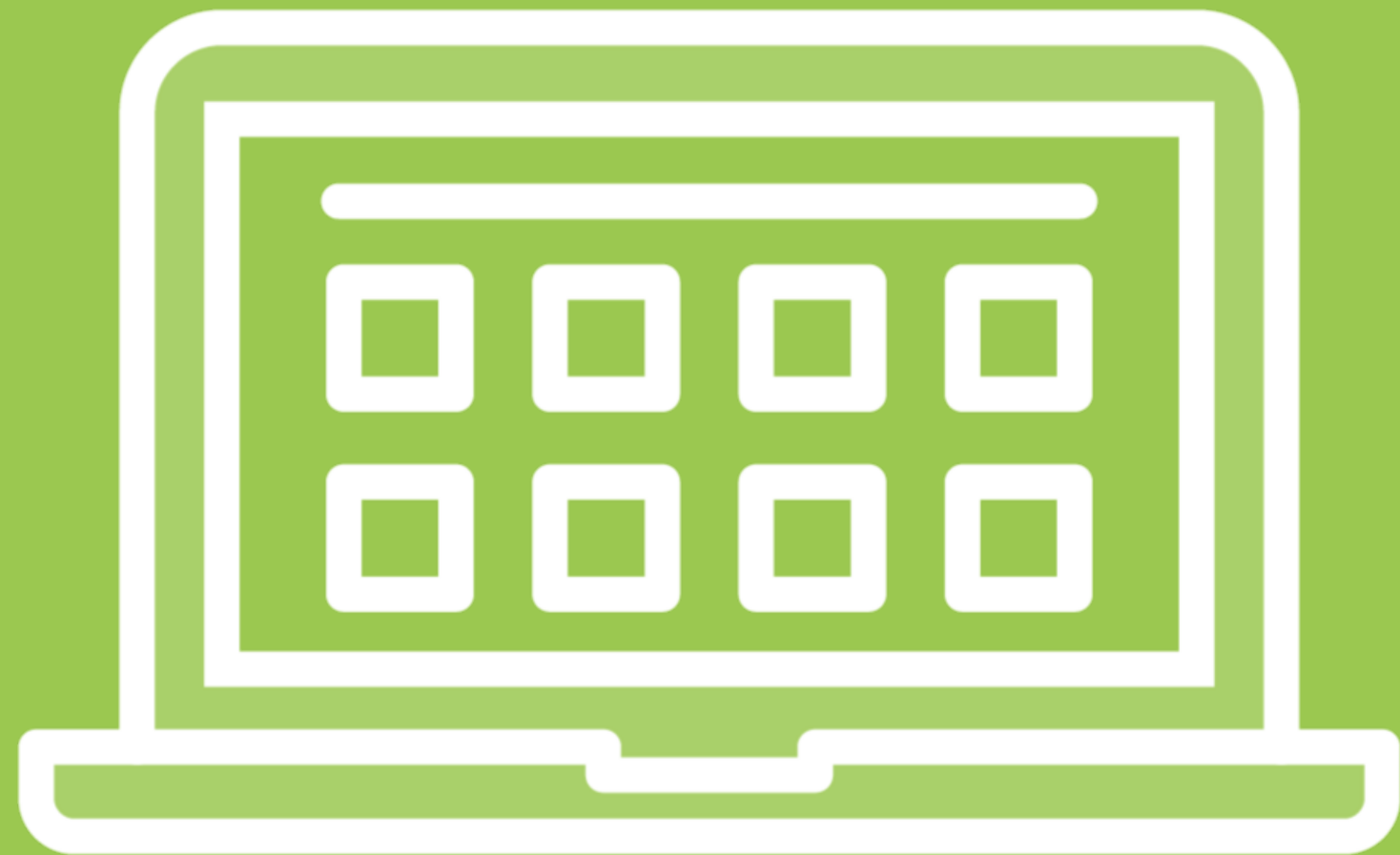


Central location for all your compliance tools and settings

– <https://compliance.microsoft.com/>

Only accessible for select administrators





Microsoft Purview Compliance Manager

Central location for all your
compliance tools and settings



Microsoft Purview Compliance Manager



Part of the Compliance Center

Helps administrators manage compliance requirements


It provides:

- **Pre-built assessments for common industry and regional standards**
 - **Custom assessments available as well**
- **Step-by-step guidance to help achieve compliance**
- **Compliance score**



Microsoft Purview Compliance Manager

Compliance Manager

 Compliance Manager settings

[Overview](#) [Improvement actions](#) [Solutions](#) [Assessments](#) [Assessment templates](#)

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

 Filter

Overall compliance score

Your compliance score: **58%**



11611/19945 points achieved

Key improvement actions

Not completed **608** Completed **4** Out of scope **0**

Improvement action	Impact	Test status	Group	Action type
Enable self-service password reset	+27 points	Failed high risk	Default Group	Technical
Conceal information with lock screen	+27 points	None	Default Group	Technical
Use IRM to protect email messages and att...	+27 points	None	Default Group	Technical
Use boundary protection devices for unclas...	+27 points	None	Default Group	Technical
Use IRM to protect online documents and s...	+27 points	None	Default Group	Technical
Require mobile devices to use encryption	+27 points	None	Default Group	Technical
Use S/MIME	+27 points	None	Default Group	Technical

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/120 points	12
Azure	0/3 points	1
Azure Active Direct...	27/537 points	28
Azure Information P...	0/297 points	11
Azure Security Center	0/1 points	1
Cloud App Security	0/76 points	12
Communication co...	0/36 points	4

Your points achieved ⓘ
90/ 8424

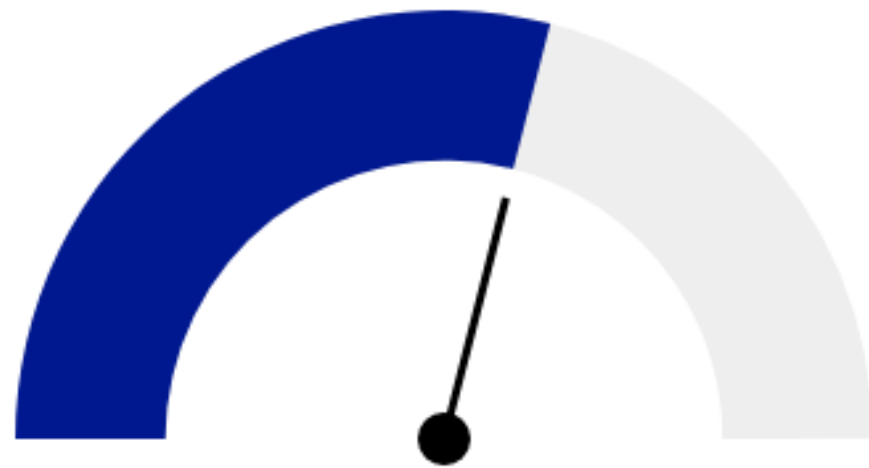
Microsoft managed points achieved ⓘ
11521/ 11521



Your Compliance Score

Overall compliance score

Your compliance score: 58%



11611/19945 points achieved

Your points achieved ⓘ

90/ 8424

Microsoft managed points achieved ⓘ

11521/ 11521

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

Quick way to understand your compliance posture

Helps prioritize actions based on potential to reduce risk

- Bigger the compliance impact – more points**



Demo



Microsoft Compliance Manager

Microsoft Compliance Score





Microsoft Purview Information Protection

Discover, classify, and protect
sensitive information wherever it lives
or travels.



Microsoft Purview Information Protection

Microsoft Purview Information Protection discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss.



Microsoft Purview Information Protection

Know Your Data

Understand your data landscape and identify important data across your hybrid environment



Protect Your Data

Apply flexible protection actions that include encryption, access restrictions, and visual markings



Prevent Data Loss

Detect risky behavior and prevent accidental oversharing of sensitive information



Govern Your Data

Automatically retain, delete, and store data and records in a compliant manner



Let's Talk Features

Sensitivity Labels

Retention Policies

Data Loss Prevention

Records Management



Sensitivity Labels

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered



Sensitivity Labels Features



Enforce protection settings such as encryption or watermarks on labeled content

Protect content in Microsoft 365 apps across different platforms and devices

Protect content in third-party apps and services



Sensitivity Labels Work with Containers

Sensitivity labels can be applied at the container level

Microsoft 365 Groups

Microsoft Teams

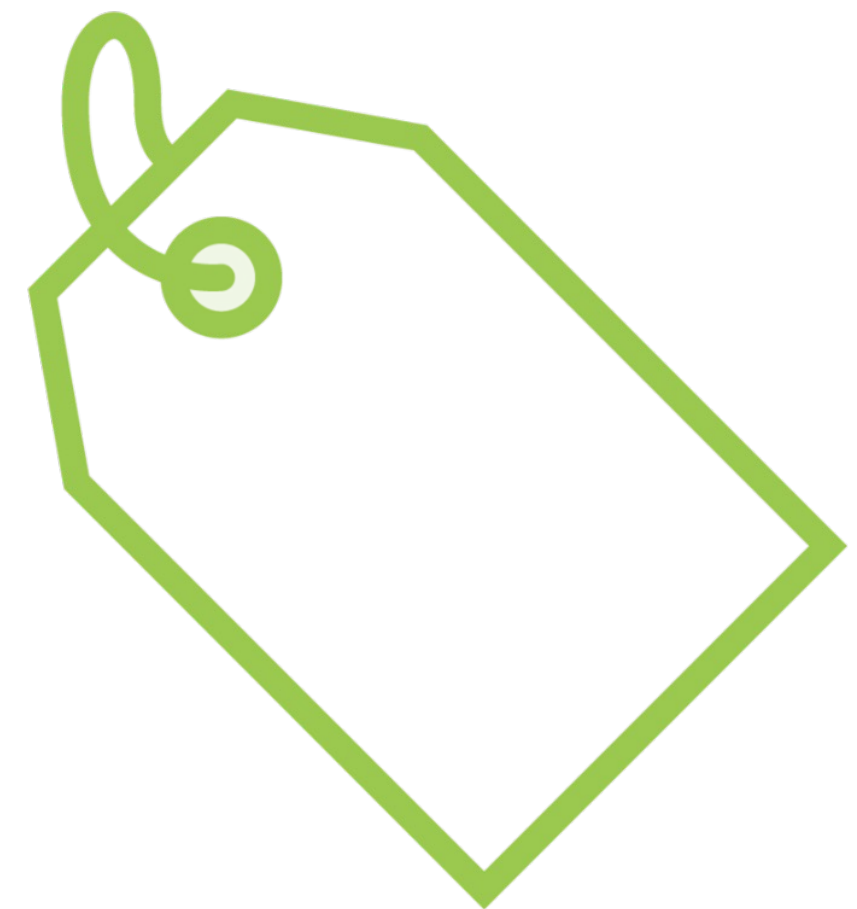
SharePoint sites

Using the label you can configure

Privacy (public or private)

External user access

Access from unmanaged device



Sensitivity Labels

LOBOMANTICS

Microsoft Purview

✓

Name & description

✓

Scope

●

Items

✓

Encryption

●

Content marking

●

Auto-labeling for files and emails

○

Groups & sites

○

Schematized data assets (preview)

○

Finish

Content marking

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

i

All content marking will be applied to documents but only headers and footers will be applied to email messages.

Content marking

☐

Add a watermark

Customize text

☐

Add a header

Customize text

☐

Add a footer

Customize text

Back

Next

Cancel

Retention Policies

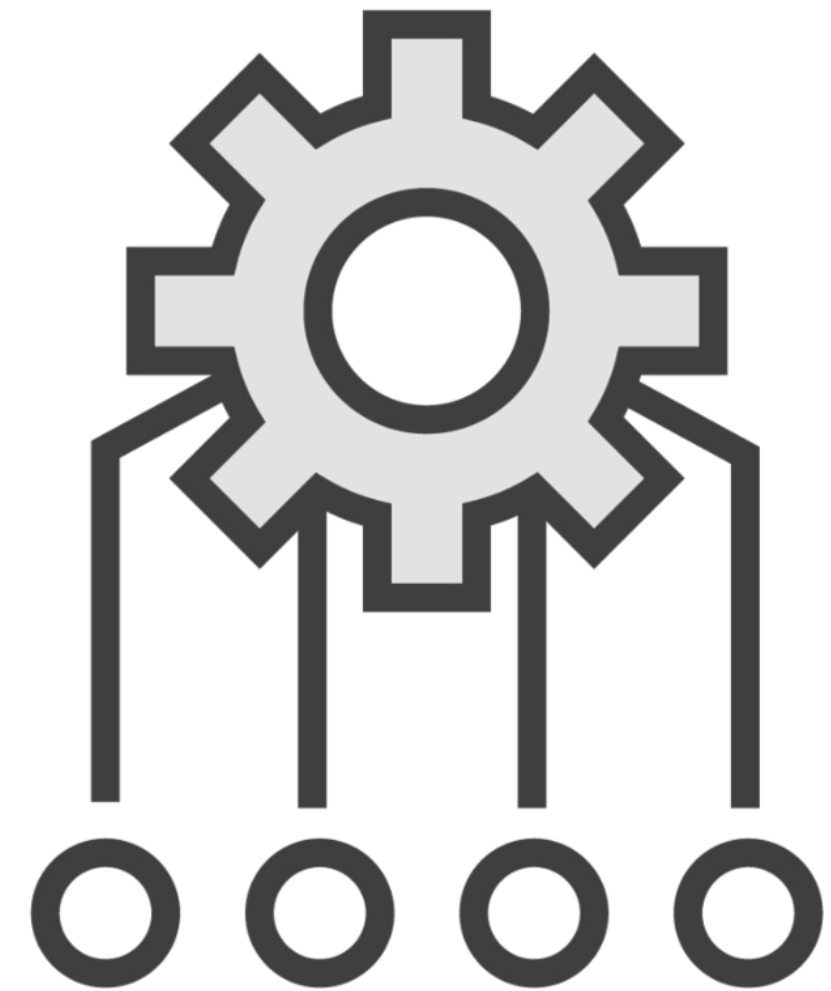
Retention policies help you to more effectively manage the information in your organization. Use retention policies to keep data that's needed to comply with your organization's internal policies, industry regulations, or legal needs, and to delete data that's considered a liability, that you're no longer required to keep, or has no legal or business value.



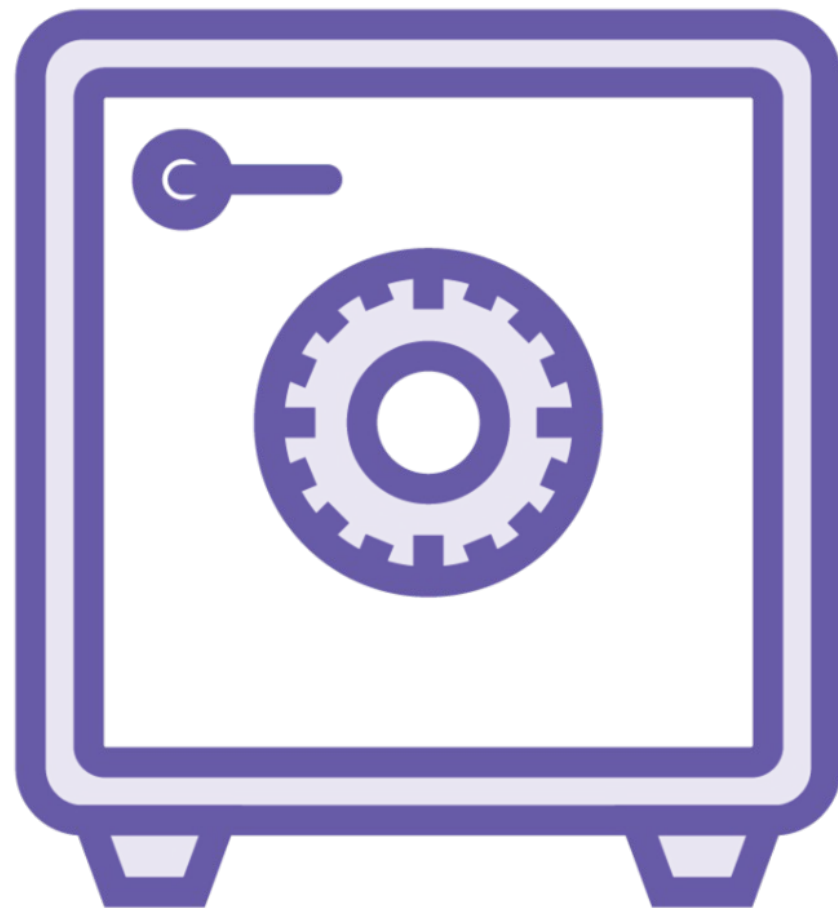
Retention Policies & Microsoft 365

Retention policies in Microsoft 365 work with

SharePoint Online
OneDrive for Business
Microsoft Teams
Microsoft 365 Groups



Retention Policies - Retain Data



Ensure data is retained for a specified period of time

- **Regardless of what happens in the user app**

Data is available for eDiscovery

You can decide what to do with the data after the specified period

- **Do nothing**
- **Delete the data**



Retention Policies – Delete Data

Retention policies can be used to delete data after a certain period of time

Permanently deleted from all storage locations on the service



Retention Policies & Microsoft Teams Example

**Retain Teams chats
and/or channel
messages for a
specified duration
and then do
nothing**

**Retain Teams chats
and/or channel
messages for a
specified duration
and then delete
the data**

**Delete Teams
chats and/or
channel messages
after a specified
duration**

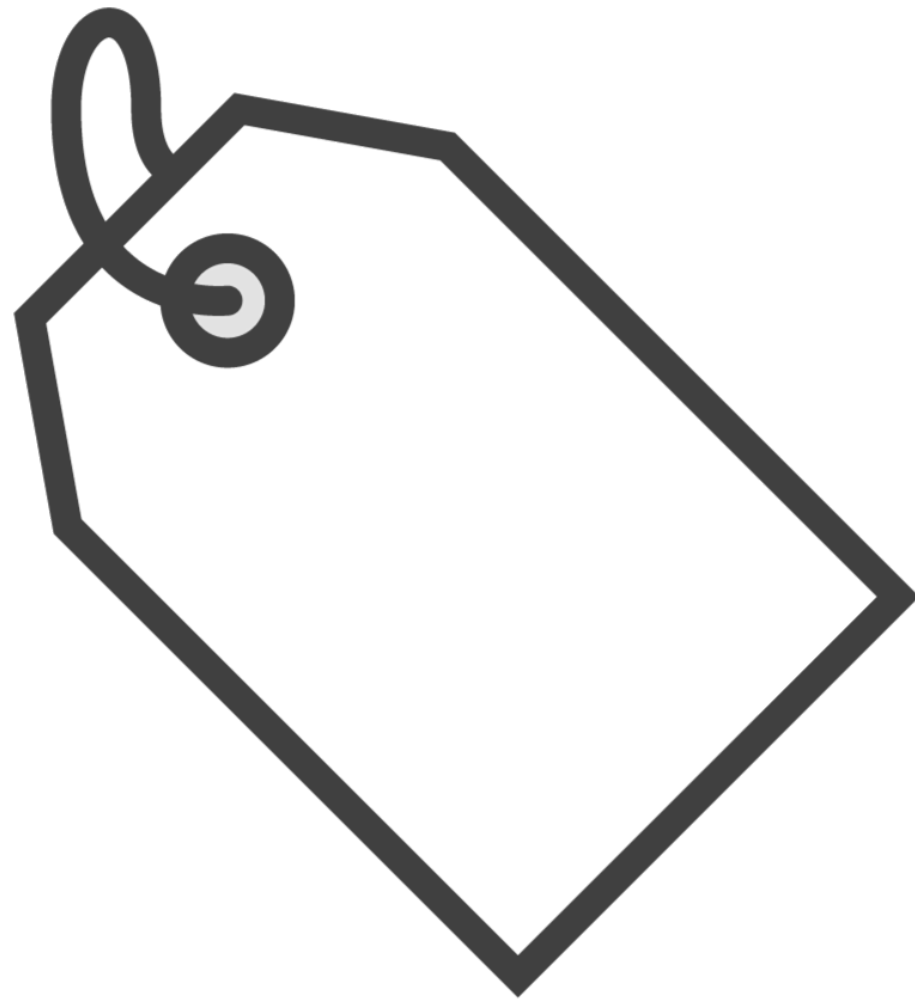


Records Management

Records management (RM) is the supervision and administration of digital or paper records, regardless of format. Records management activities include the creation, receipt, maintenance, use and disposal of records. Documentation may exist in contracts, memos, paper files, electronic files, reports, emails, videos, instant message logs or database records.



Microsoft Purview Records Management



Microsoft 365 Records Management leverages Retention Policies

Behavior is different from a user experience / feature point of view

Retention labels keep a copy of the content hidden from the user

- User is allowed to delete / modify content from the user interface**

Records also block actions in the user interface



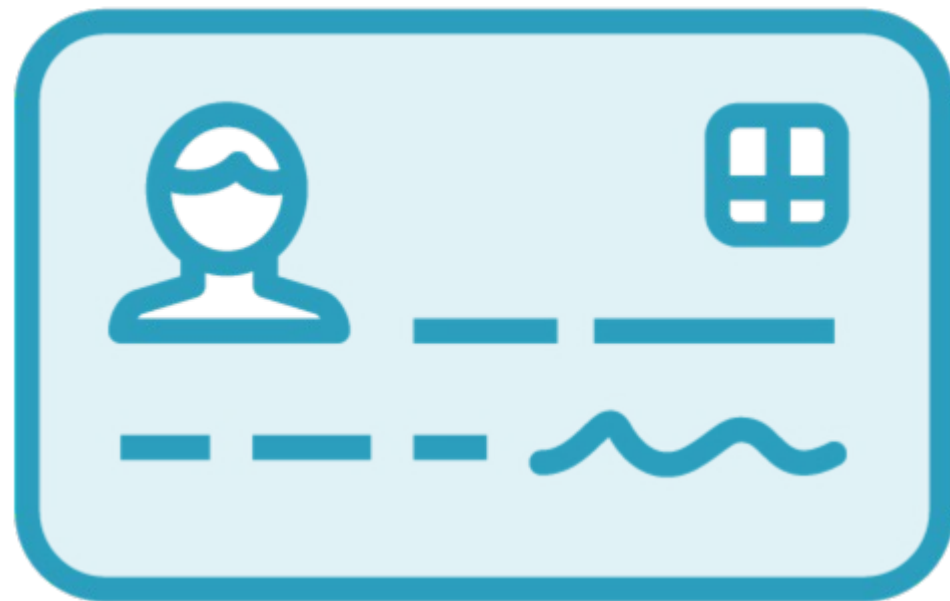


Microsoft Purview Data Loss Prevention

Microsoft Purview Data Loss Prevention provides unified data loss prevention capabilities across endpoints, apps, and services.



Data Loss Prevention (DLP)



Set of tools to identify sensitive data from being shared

- Credit card number
- Social Security number
- Passport number

You can also create custom sensitive information

- Client case numbers
- Patient number

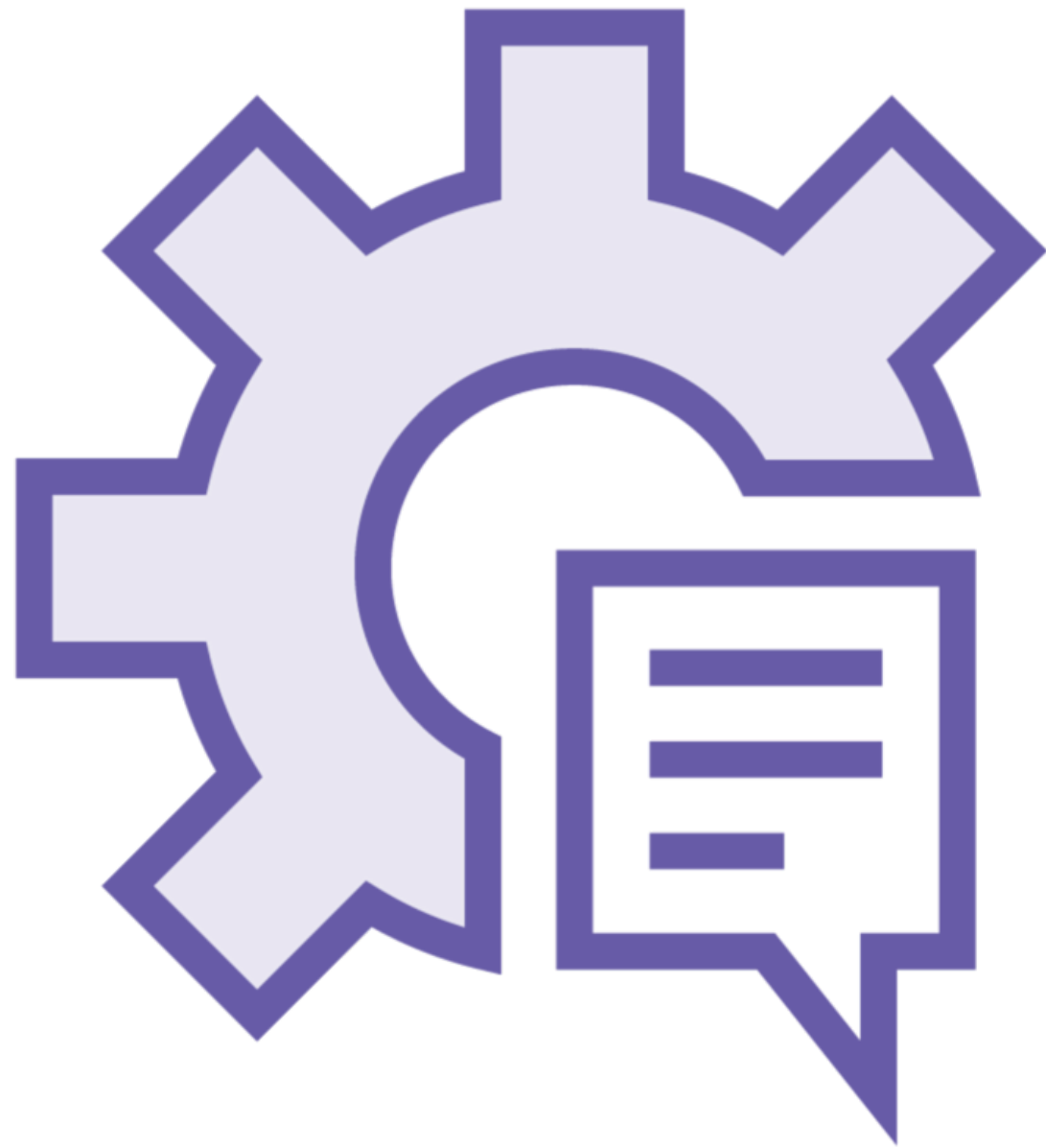
Microsoft Purview Data Loss Prevention

Can identify information across
Exchange Online
SharePoint Online
OneDrive for Business
Microsoft Teams

Also works with non-cloud services
On-premises SharePoint Server
File shares



Data Loss Prevention Policies



You create different policies for the type of content you want to protect

- **Type of sensitive information**
- **Locations to check**
- **Action to do if sensitive information found**
 - **Show a pop-up warning**
 - **Block the sharing**
 - **Lock & move content to a quarantine location**

Data Loss Prevention Inside Microsoft Teams

The screenshot displays the Microsoft Teams interface. On the left is a dark sidebar with navigation icons for Activity, Communities, Chat, Adobe Creative Cloud, Teams, Calendar, Calls, and a menu of more options. The main area is divided into a 'Feed' section on the left and a channel view on the right. The channel is named 'Target Dates' and has tabs for Posts, Files, and Wiki. A notification in the Feed states: 'Your message has been blocked 1:40 PM IT Systems Refresh > Target Dates Message contains sensitive content'. In the channel view, a post by 'Vlad Catrinescu' from 2/24 at 1:30 PM says 'Here are the slides for Milestone 5!' and includes a file 'M5_AC.pptx' from 'Dropbox > IT Systems Refresh > Target Dates'. Below this, a post by 'John Smith' is shown with a red blocked message icon and the text 'This message was blocked. What can I do?'. The blocked message content is a table titled 'Test Credit Card Account Numbers'.

Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904

At the bottom of the interface is a text input field with the placeholder 'Start a new conversation. Type @ to mention someone.' and a row of icons for adding content (text, link, emoji, GIF, video, screen, voice, and more).



Data Loss Prevention – Other Users View

The screenshot displays the Microsoft Teams application interface. On the left, a dark sidebar contains navigation icons for Activity, Chat, Teams, Calendar, Calls, Files, and a menu of more options. The main area is divided into two panes. The left pane, titled 'Teams', lists 'Your teams' including 'IT Systems Refresh' (selected), 'General', 'Stakeholders', and 'Target Dates'. Below this is a section for 'Hidden teams' with 'Microsoft 365 Adoption', 'Accounting Team', and 'Marketing Collaboration ...'. The right pane shows the 'Target Dates' channel. At the top, it indicates 'Team' and '2 Guests'. The channel tabs are 'Posts', 'Files', and 'Wiki'. The channel history shows two messages: a system message from Vlad Catrinescu about channel visibility and name change, and a message from Vlad Catrinescu dated 2/24 1:30 PM with the text 'Here are the slides for Milestone 5!' and a file attachment 'M5_AC.pptx' from Dropbox. Below this is a message that has been blocked, indicated by a red circle with a slash and the text 'This message was blocked due to sensitive content. What's this?'. At the bottom, there is a text input field with the placeholder 'Start a new conversation. Type @ to mention someone.' and a row of icons for adding content (text, link, emoji, GIF, video, screen, etc.).





Microsoft Purview Insider Risk Management

Detect, investigate, and act on
malicious and inadvertent activities in
your organization



Insider Risk Management

Microsoft Purview Insider Risk Management is a compliance solution that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization



Insider Risk Scenarios

**Leaks of sensitive
data and data
spillage**

**Intellectual
property (IP) theft**

Insider trading

Fraud

**Confidentiality
violations**

**Regulatory
compliance
violations**



Insider Risk Management Workflow

Policy



Alerts



Triage



Investigate



Action



Collaboration

Compliance, HR, Legal, Security



Insider Risk Policy Example

Categories

Data theft

Security policy
violations (preview)

Data leaks

Templates

Data theft by
departing users

Data theft by departing users

Detects data theft by departing users near their resignation or termination date.

[Learn more about this template](#)

Prerequisites

- (Optional) [HR data connector](#) configured to periodically import resignation and termination date details for users in your organization.
- (Optional) To [detect activity on devices](#), you must have devices onboarded to the compliance center and device indicators selected.
- (Optional) [Physical badging connector](#) configured to periodically import access events to priority physical locations

Triggering event

Risk scores will be assigned to a user's activity based on the triggering event you'll choose later in this wizard. Alerts will then be generated based on their severity.

Options include:

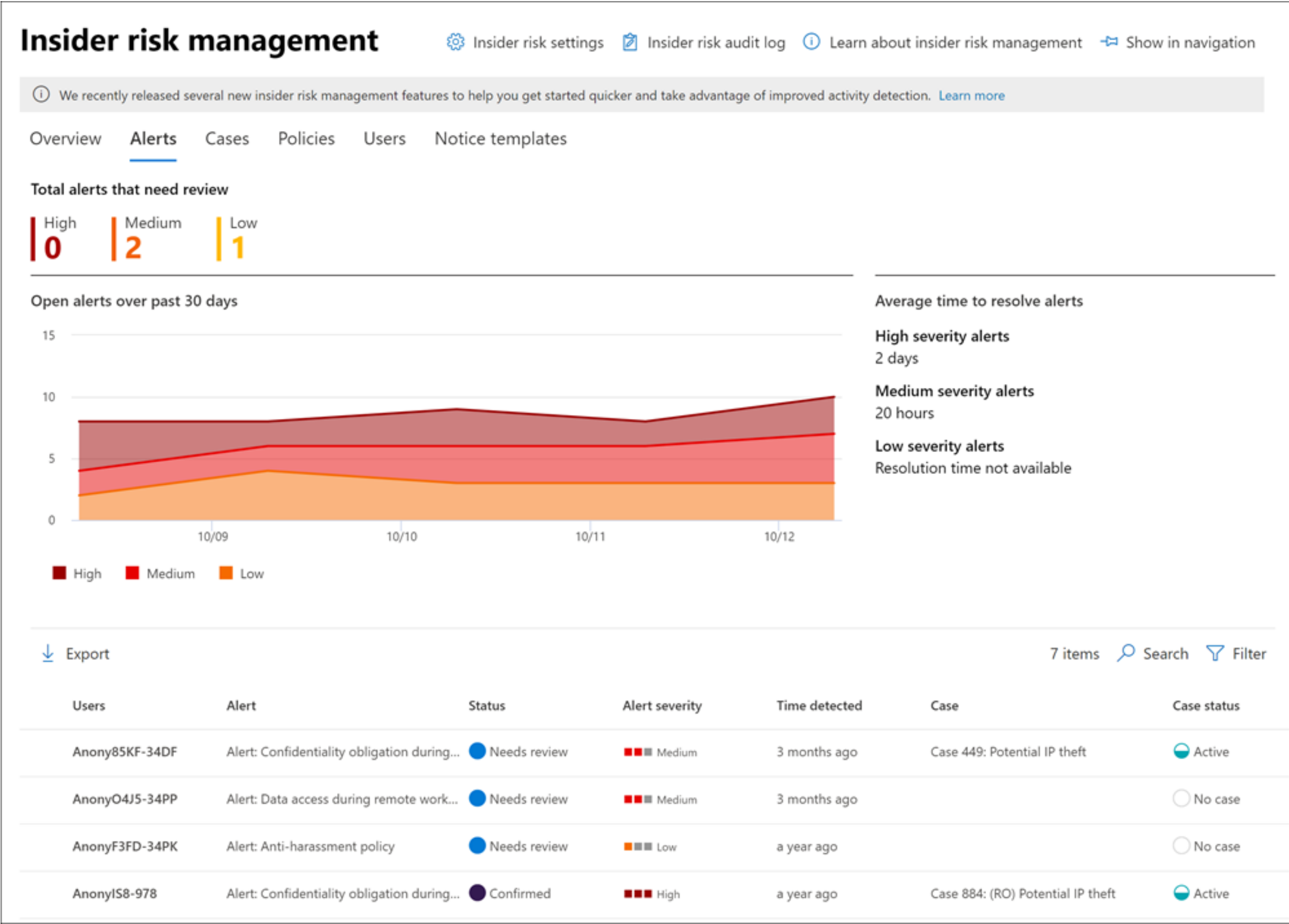
- (Recommended) HR data connector events. Scores assigned when the connector imports termination or resignation dates for a user.
- User account deleted from Azure AD. Scores assigned when a user's account is deleted from Azure AD.

Detected activities include

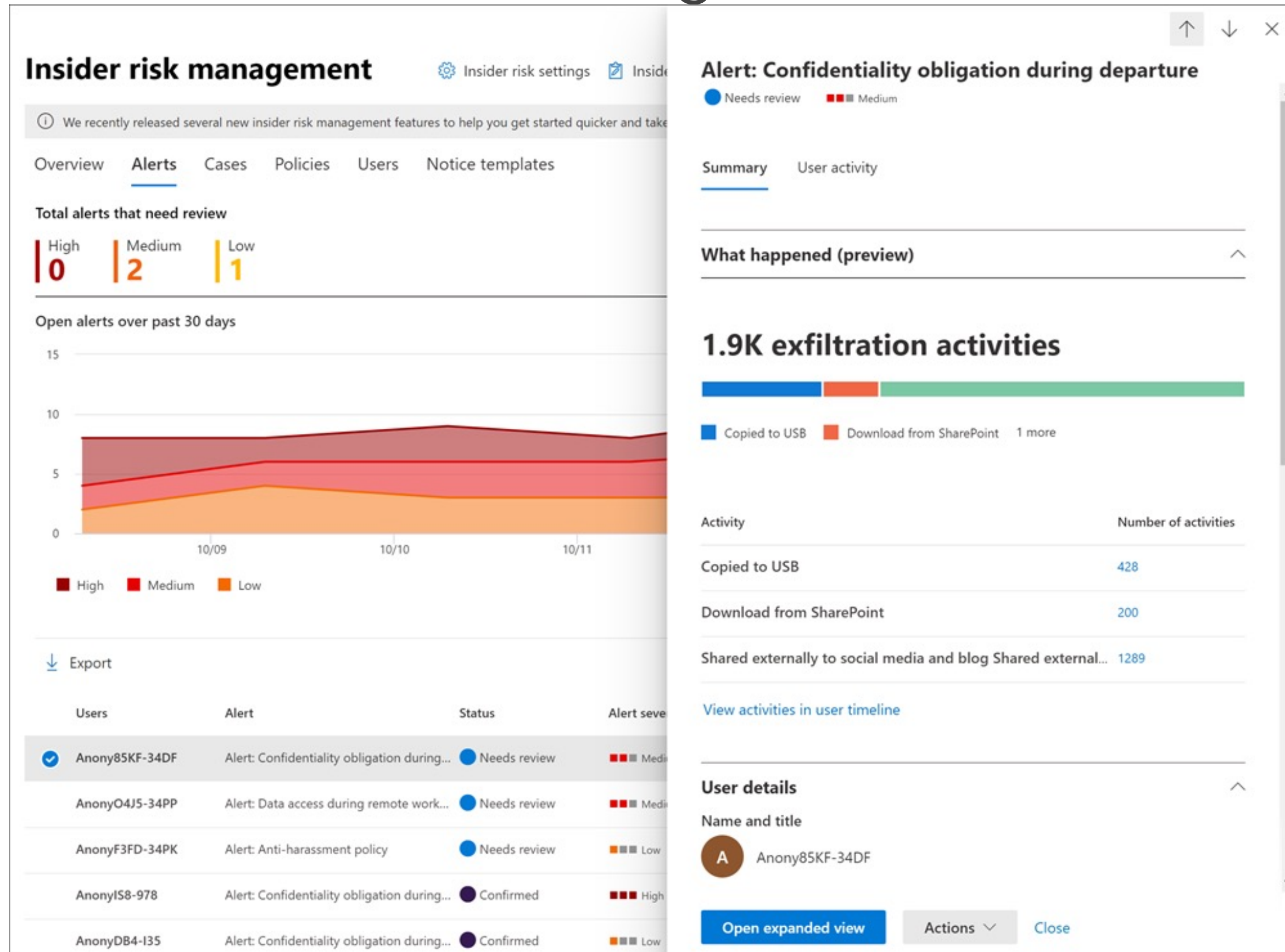
- Downloading files from SharePoint
- Printing files
- Copying data to personal cloud storage services



Insider Risk Alerts



Triage



Investigate

Insider risk management > Cases > Case 449: Potential IP theft

Case 449: Potential IP theft

Resolve case

Case actions ▾

Case overview

Alerts

User activity

Activity explorer (preview)

Content explorer

Case notes

Contributors

Deletion: Files deleted

Jan 3, 2021 (UTC) | Risk score: 75/100

2 events: Files deleted from Windows 10 Machine

> (4) SEQUENCE: Files exfiltrated and cleaned up

Nov 11, 2020 - Jan 3, 2021 (UTC) | Risk score: 90/100

50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted ([Explore content](#))

5 events: Files that have labels applied, including: random name ([Explore content](#))

2 events: Files containing sensitive info, including: Credit Cards ([Explore content](#))

1 event: File sent to 1 unallowed domain ([Explore content](#))

Exfiltration: Files printed

Dec 13, 2020 (UTC) | Risk score: 45/100

2 events: Files printed

2 events: Files containing sensitive info, including: Credit Cards

0 Files with labels applied

Exfiltration: Emails with attachments sent outside the organization

Dec 3, 2020 (UTC) | Risk score: 67/100

5 events: Emails sent outside the organization ([Explore content](#))

0 events: Emails sent to 0 unallowed domains ([Explore content](#))

0 Emails that contain sensitive info

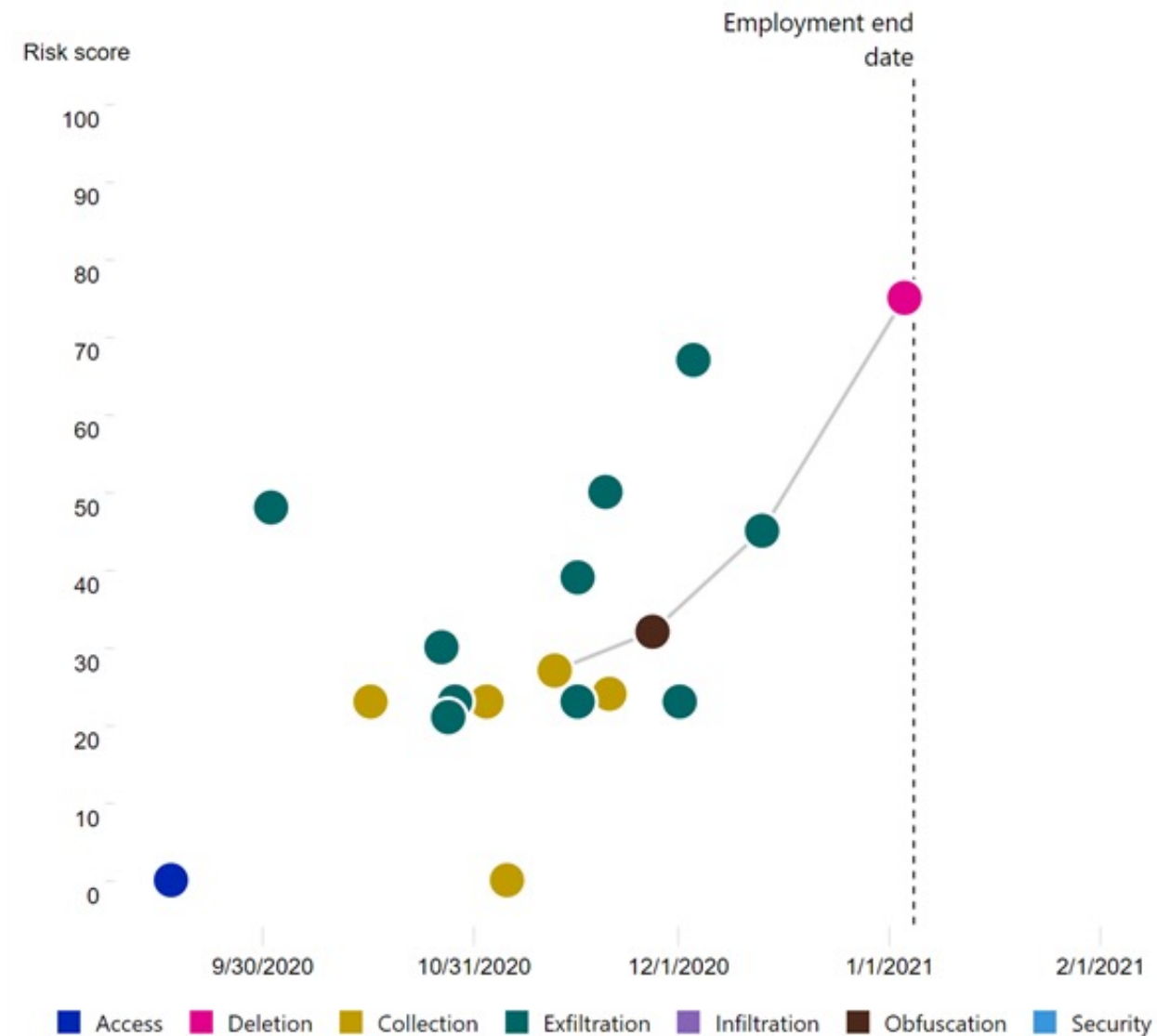
Exfiltration: Emails with attachments sent outside the organization

Dec 1, 2020 (UTC) | Risk score: 23/100

6 Months

3 Months

1 Month



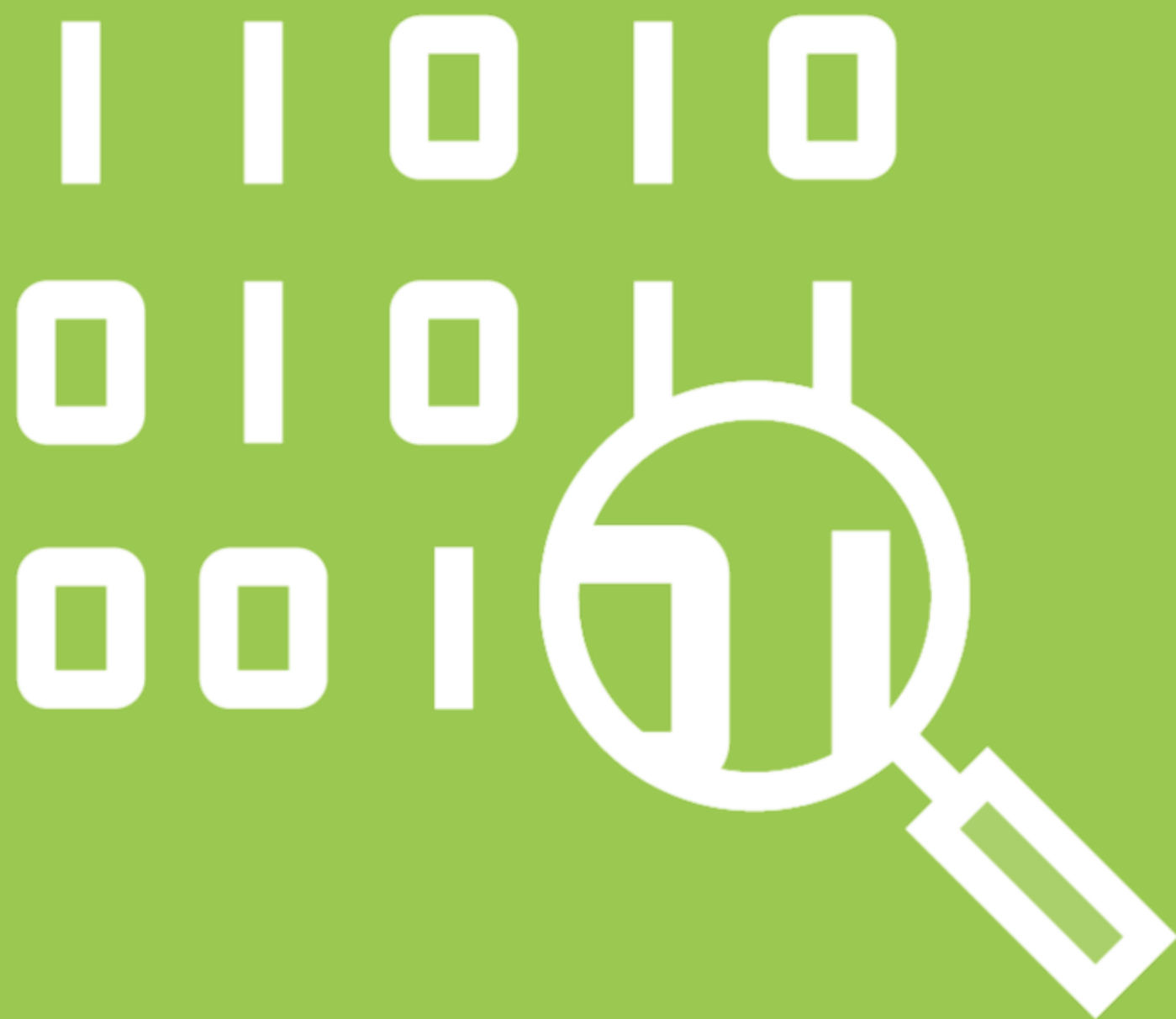
Action

Notice

Refresher Training

**eDiscovery
(Premium)**





Microsoft Purview eDiscovery

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.

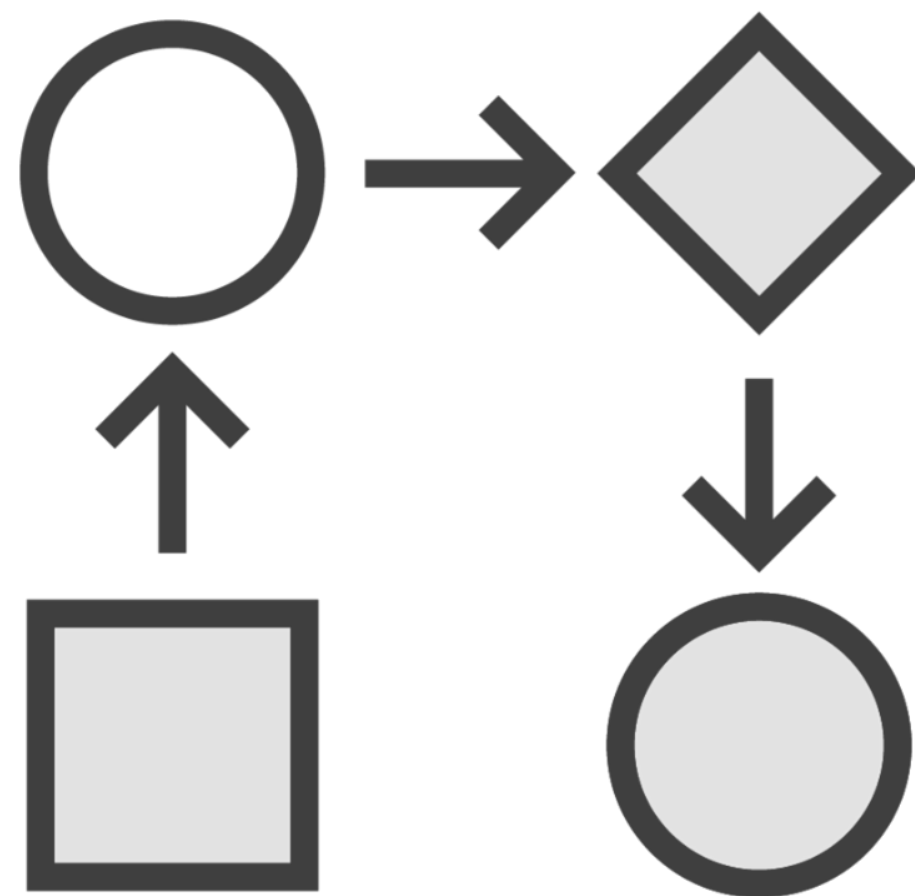


Electronic Discovery

Electronic discovery (sometimes known as e-discovery, ediscovery, eDiscovery, or e-Discovery) is the electronic aspect of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation. ESI includes, but is not limited to, emails, documents, presentations, databases, voicemail, audio and video files, social media, and web sites.



Six Stages of eDiscovery



Identification

- Identify documents that might contain information related to the subject

Preservation

- Data identified as potentially relevant is placed in a legal hold

Collection

- Transfer of data from the systems to their legal counsel



Six Stages of eDiscovery

Processing

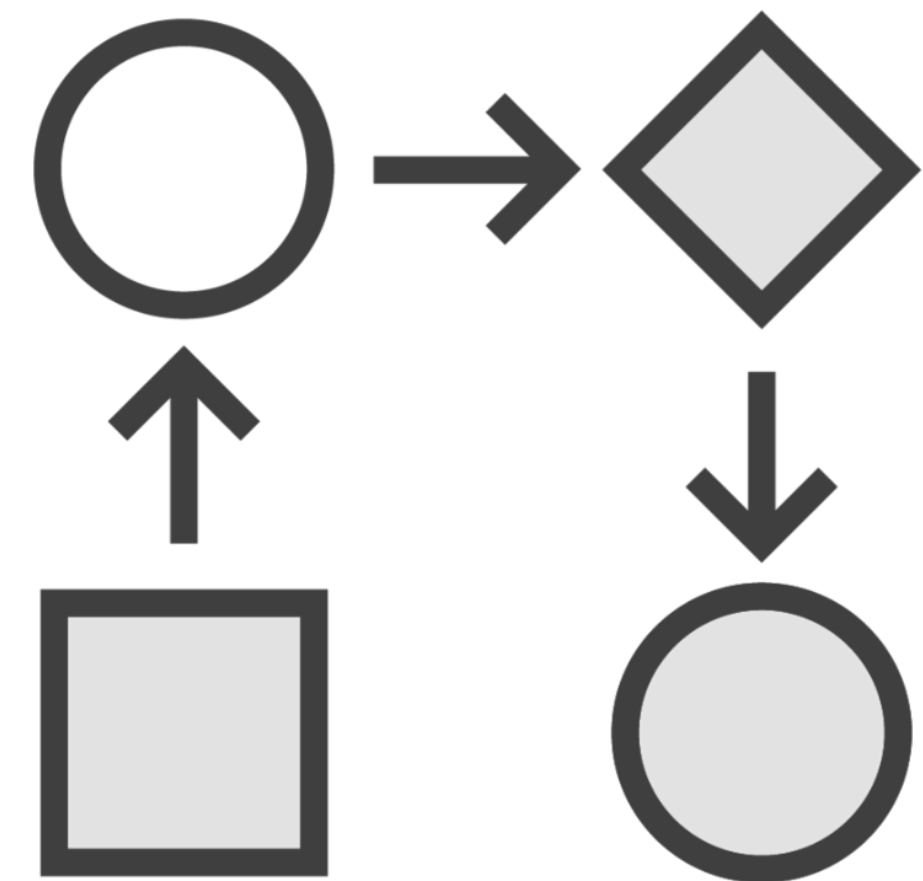
Data is processed for further review and analysis

Review

Review specific documents and reduce data to what is most relevant to the case

Production

Documents are exported in their native format or in an industry-standard format



eDiscovery in the Microsoft Cloud

Content Search

**eDiscovery
(Standard)**

**eDiscovery
(Premium)**



Microsoft Tools & eDiscovery Stages

Content Search

Identification

Collection

eDiscovery (Standard)

Identification

Preservation

Collection

eDiscovery (Premium)

Identification

Preservation

Collection

Processing

Review

Production



Why Do We Have Three Tools?



Each tool has different licensing requirements

- **The more features – the more licensing is required**



Demo



Content Search





Microsoft Purview Audit

Solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.



Auditing for Microsoft 365



Unified Audit Log

- **Centralized Audit Log that contains most Microsoft 365 activities**

Audit records retained between 90 days and 10 years


- **Depending on the user license**

APIs allow you to export audit logs into your own systems to keep longer




- **You can also simply export to CSV**



Audit Log Example



Microsoft Purview



Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Trials

Solutions

Catalog

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Information barriers

Export

	Date ↓	IP Address	User
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 12:58 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 17, 2022 11:09 AM	2603:10b6:4:b9::36	vlad@globomantics.org
<input type="checkbox"/>	Jul 17, 2022 3:39 AM		ServicePrincipal_a8a371
<input checked="" type="checkbox"/>	Jul 17, 2022 12:21 AM	52.232.129.84	vlad@globomantics.org
<input type="checkbox"/>	Jul 17, 2022 12:21 AM	52.232.129.84	vlad@globomantics.org
<input type="checkbox"/>	Jul 16, 2022 7:54 PM		ServicePrincipal_cb81a9
<input type="checkbox"/>	Jul 16, 2022 7:37 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 16, 2022 7:37 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 16, 2022 7:37 PM		NT AUTHORITY\SYSTEM
<input type="checkbox"/>	Jul 16, 2022 7:37 PM		NT AUTHORITY\SYSTEM

Detail

Date

2022-07-17 00:21:43

IP Address

52.232.129.84

Users

vlad@globomantics.org

Activity

Performed search query

Item

Detail

Search Query Performed from undefined

AppAccessContext

```
{  "ClientAppId": "dcad865d-9257-4521-ad4d-bae3e137b345",  "ClientAppName": "Microsoft SharePoint Online - SharePoint Home",  "CorrelationId": "64cb6b4e-7553-423c-86ed-2b4913b05967"}  
```

CreationTime

2022-07-17T04:21:43

Close

Alerts

Send alerts based on the activities in Unified Audit Log

Be proactive when certain actions happen in the organization



Microsoft Purview Audit (Premium) Features

**Long-term
retention of audit
logs**

**Access to crucial
events for
investigations**

**High-bandwidth
access to the
Office 365
Management
Activity API**



Demo



Exploring the Unified Audit Log



Conclusion



Introduction to regulatory compliance

Microsoft's privacy principles

The Microsoft Service Trust portal

Microsoft Purview compliance solutions

- Microsoft Purview Compliance Manager
- Microsoft Purview Information Protection
- Microsoft Purview Data Loss Prevention
- Microsoft Purview Insider Risk Management
- Microsoft Purview eDiscovery
- Microsoft Purview Audit



Up Next:
Course Conclusion

