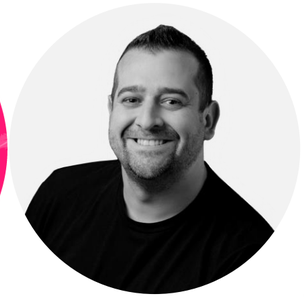
Protecting from Insider Risk in Microsoft 365



Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Introduction to insider risk management

Communication compliance

Information barriers

Introduction to Insider Risk Management

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

https://learn.microsoft.com/en-us/purview/insider-risk-management

Insider Risk Scenarios

- Leaks of sensitive data and data spillage
- Intellectual property (IP) theft
- Insider trading
- Confidentiality violations
- Fraud
- 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

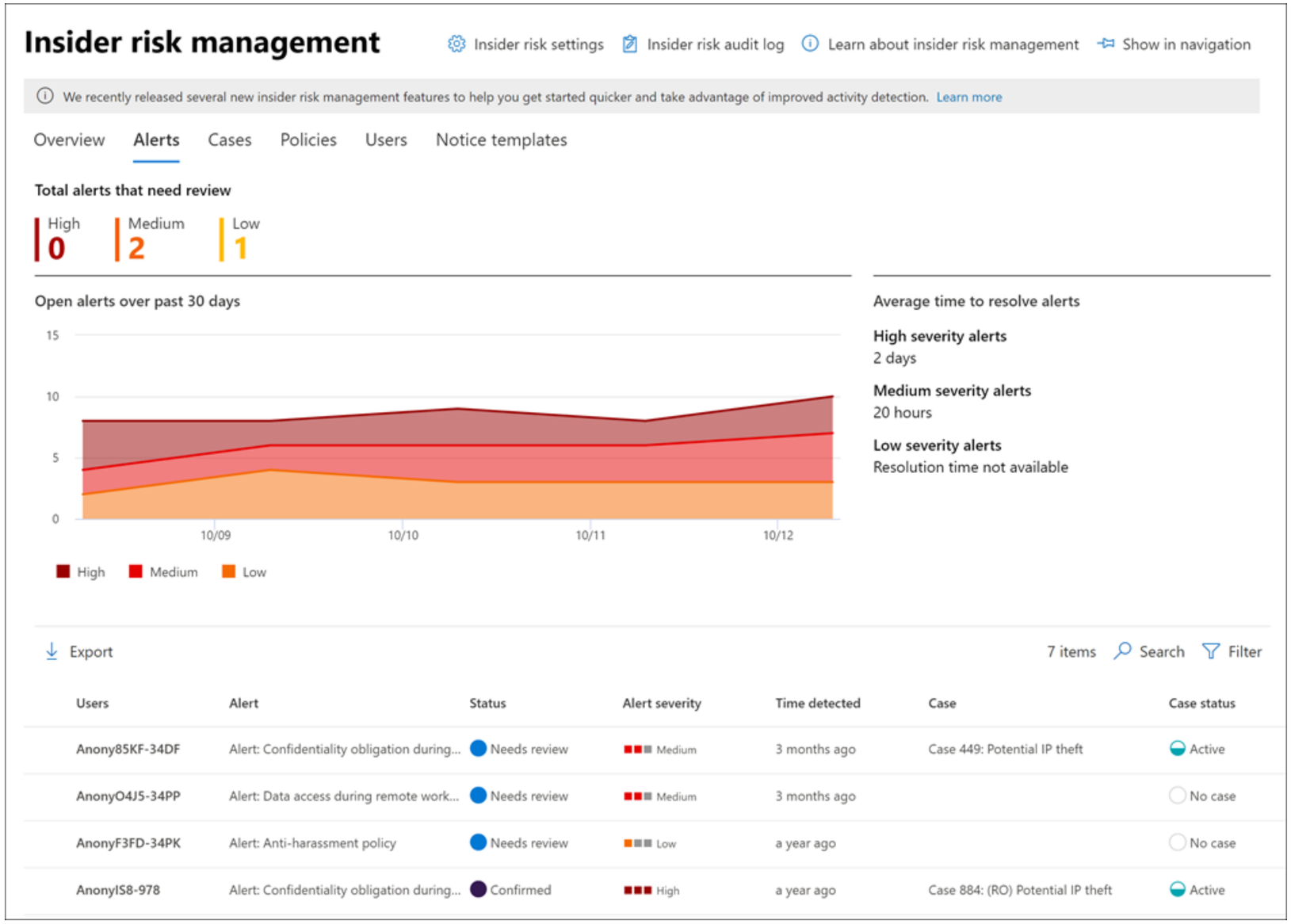
Triggering event
Risk scores will be assigned to a user's activity based on the triggering event you'll choose later in this wizard. Alerts will then be generated based on their severity. Options include:

- (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.

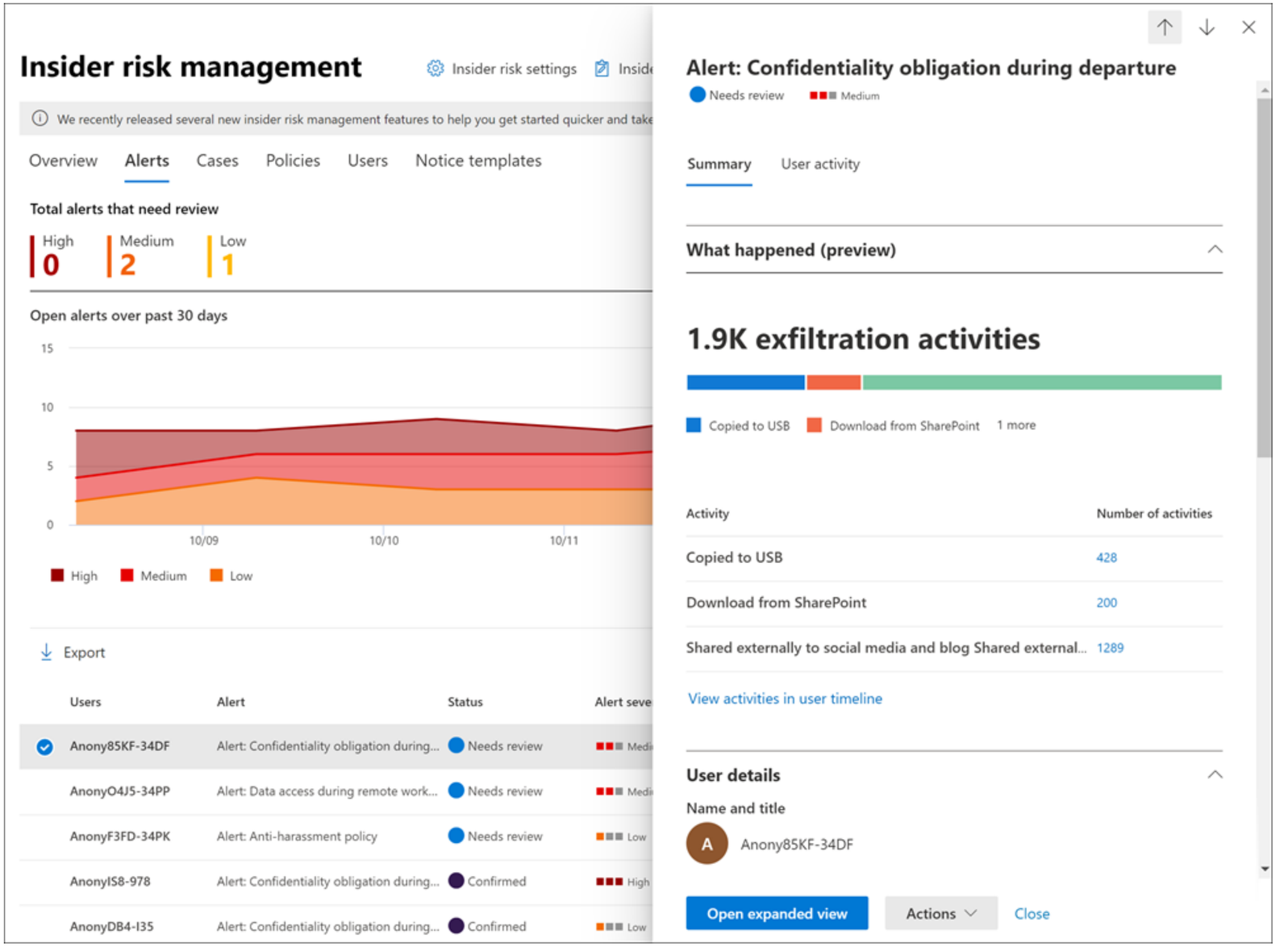
Detected activities include

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

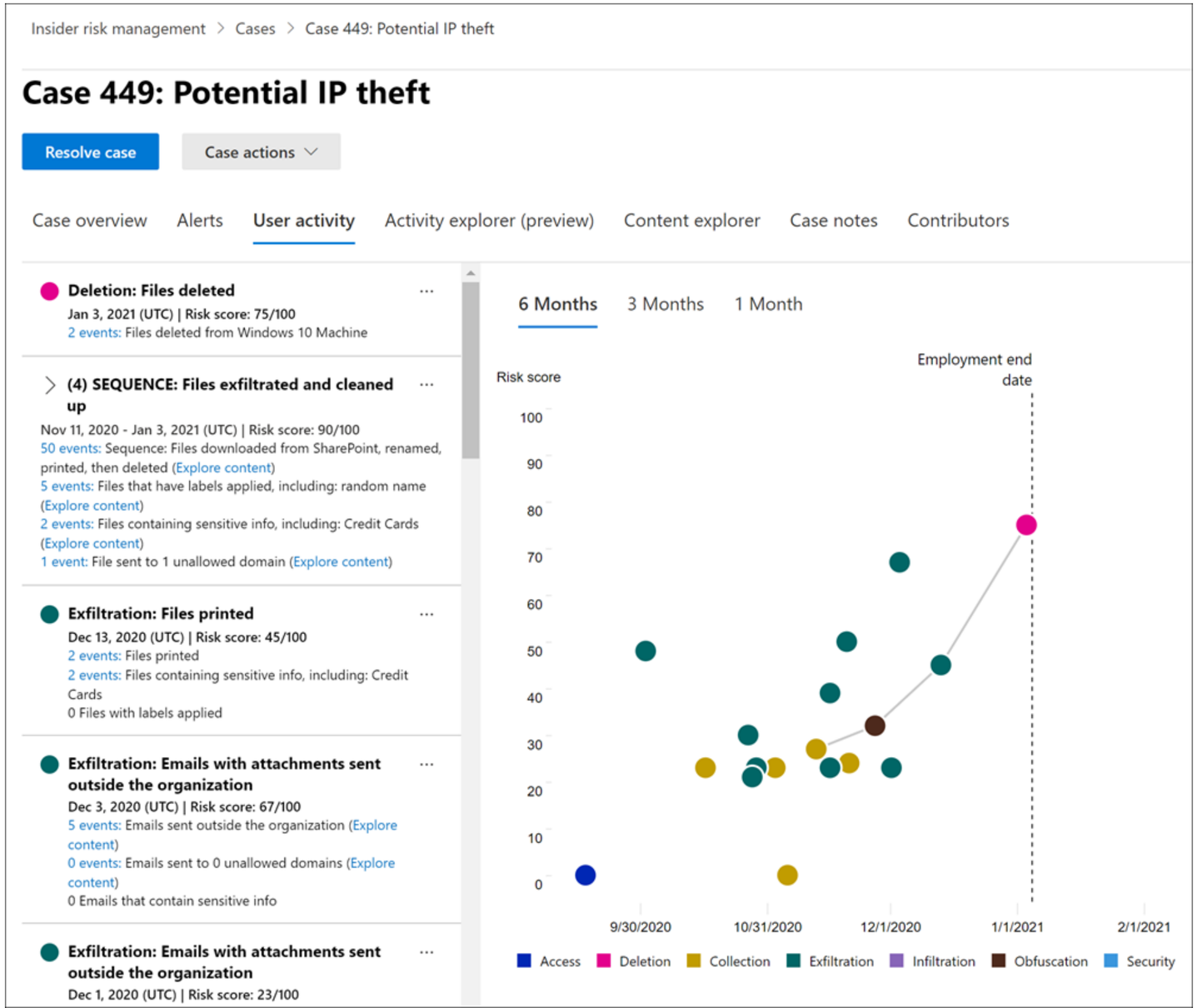
Insider Risk Alerts



Triage


Insider risk management
Insider risk settings
We recently released several new insider risk management features to help you get started quicker and take
Overview
Alerts
Cases
Policies
Users
Notice templates
Total alerts that need review
High
0
Medium
2
Low
1
Open alerts over past 30 days
15
10
5
0
10/09
10/10
10/11
High
Medium
Low
Export
Users
Alert
Status
Alert seve
Anony85KF-34DF
Alert: Confidentiality obligation during...
Needs review
AnonyO4J5-34PP
Alert: Data access during remote work...
Needs review
AnonyF3FD-34PK
Alert: Anti-harassment policy
Needs review
Low
AnonyIS8-978
Alert: Confidentiality obligation during...
Confirmed
High
AnonyDB4-I35
Alert: Confidentiality obligation during...
Confirmed
Low
Alert: Confidentiality obligation during departure
Needs review
Medium
Summary
User activity
What happened (preview)
1.9K exfiltration activities
Copied to USB
Download from SharePoint
1 more
Activity
Number of activities
Copied to USB
428
Download from SharePoint
200
Shared externally to social media and blog Shared external...
1289
View activities in user timeline
User details
Name and title
A
Anony85KF-34DF
Open expanded view
Actions
Close

Investigate



Action

Notice

Refresher Training

eDiscovery (Premium)

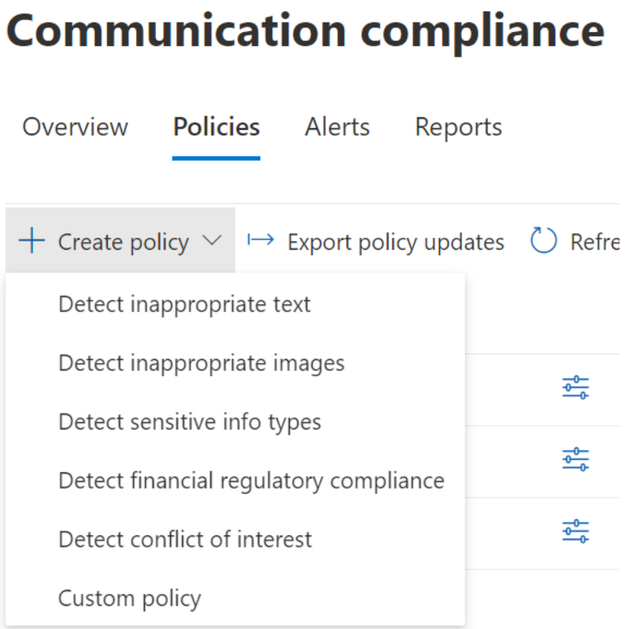
Communication Compliance

Communication Compliance

Microsoft Purview Communication Compliance is an insider risk solution that helps minimize communication risks by helping you detect, capture, and act on potentially inappropriate messages in your organization. Pre-defined and custom policies allow you to check internal and external communications for policy matches so they can be examined by designated reviewers

https://learn.microsoft.com/en-us/purview/communication-compliance

Communication Compliance



Quickly detect, capture, and remediate communications that go against your policies

- Offensive or threatening language
- Sensitive information
- Financial regulatory compliance
- Conflict of interest
- Custom

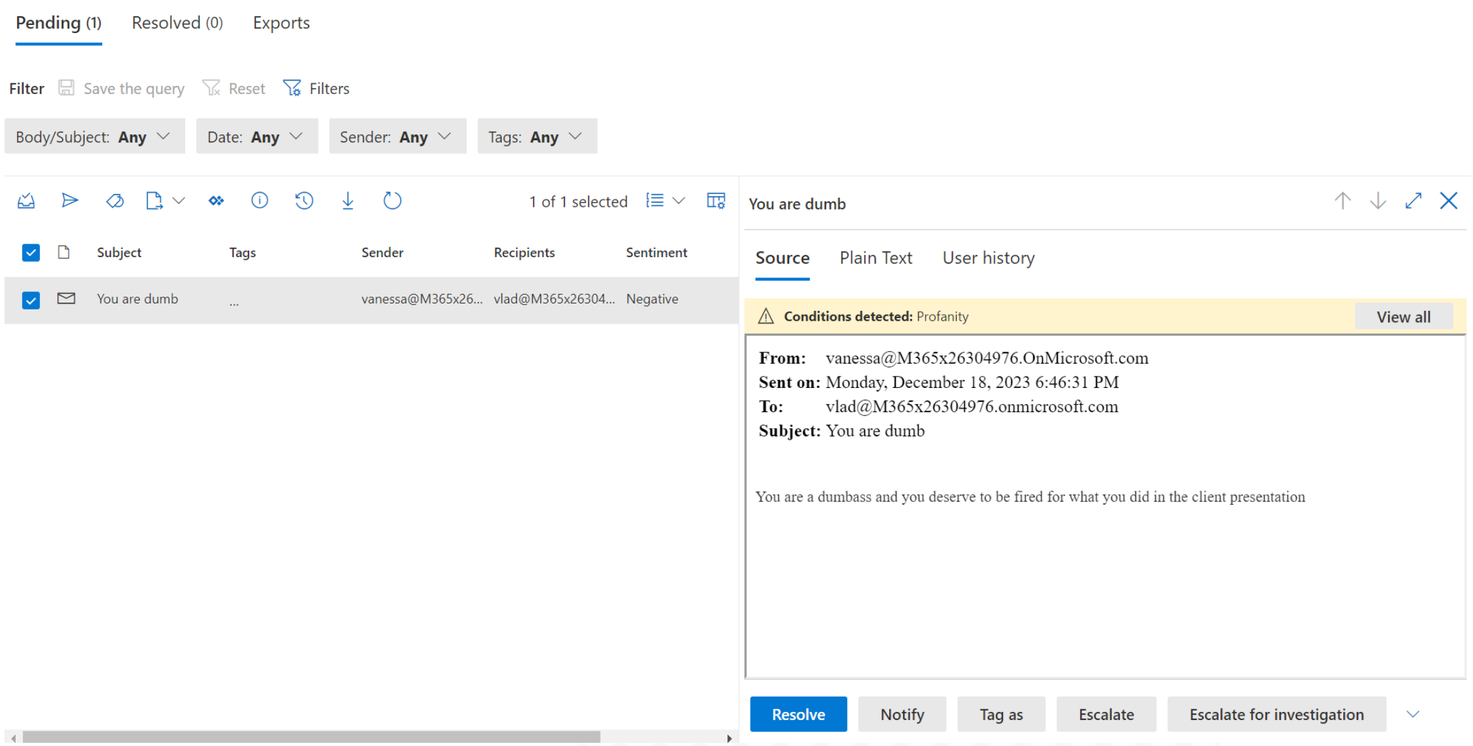
Works in

- E-mail
- Microsoft Teams
- Viva Engage
- Third-party communication

Communication that goes against policies will automatically be detected

Allowed users can review and:

- Resolve
- Tag
- Notify
- Escalate
- Remove message (Teams only)



Demo

Communication compliance

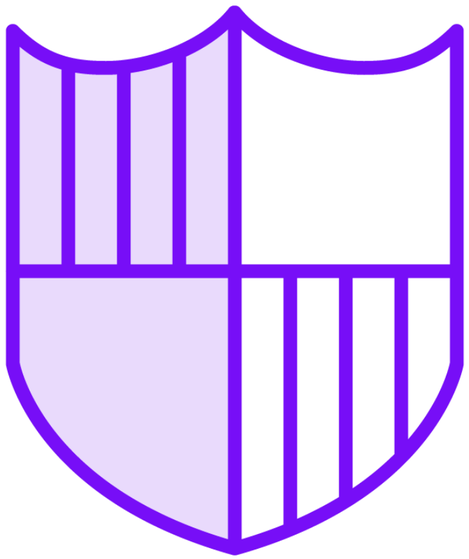
Microsoft Purview Information Barriers

Information Barriers

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. Often used in highly regulated industries, IB can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers

Information Barriers



Useful example

- A day trader cannot call someone on the marketing team
- A research team can only call or chat online with a product development team

Information barriers work with Microsoft Teams, SharePoint, and OneDrive for Business

Information barriers only support two-way restrictions

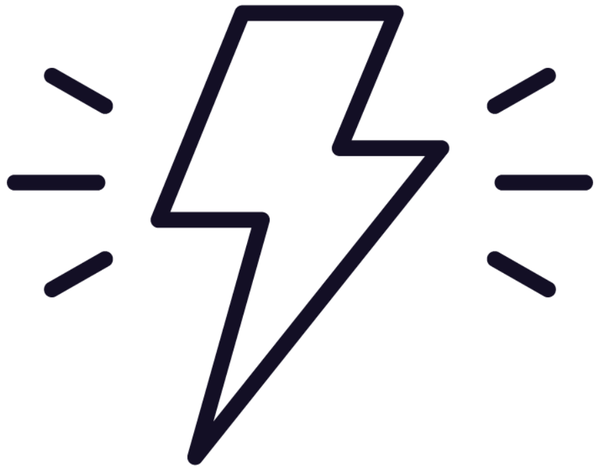
Information Barrier Triggers

Adding a member to a team

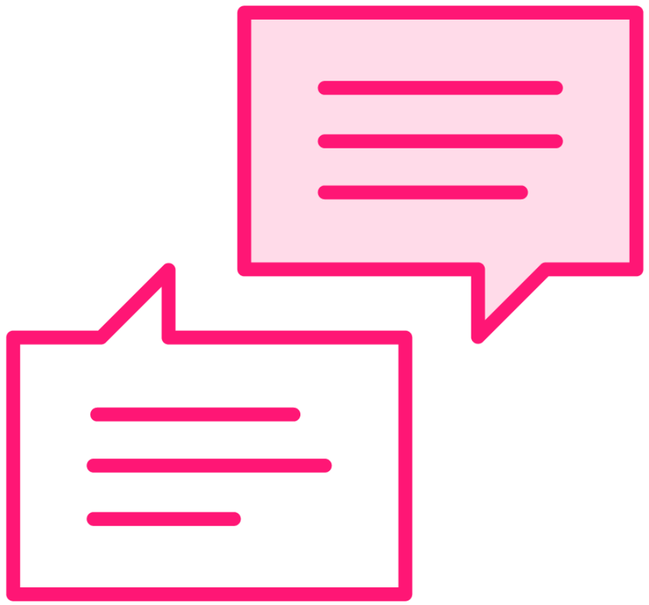
Initiating a new chat

User is invited to a meeting

A user places a phone call (VOIP) in Teams



Information Barriers: Existing Chats



1:1 chats

- Communication will be blocked, and chat remains read only

Group chat

- Users who violate policy will be removed from chat
- Chat becomes read only

Module Conclusion

Introduction to insider risk management

- Mitigate internal risks in your organization

Communication compliance

- Quickly detect, capture, and remediate communications that go against your policies

Information barriers

- Prevent individuals or groups from communicating with each other

Up Next:

eDiscovery in Microsoft 365