Microsoft

What's new in Insider Risk and Communication Compliance

M365 SECURITY & COMPLIANCE
Customer Experience Engineering

Agenda

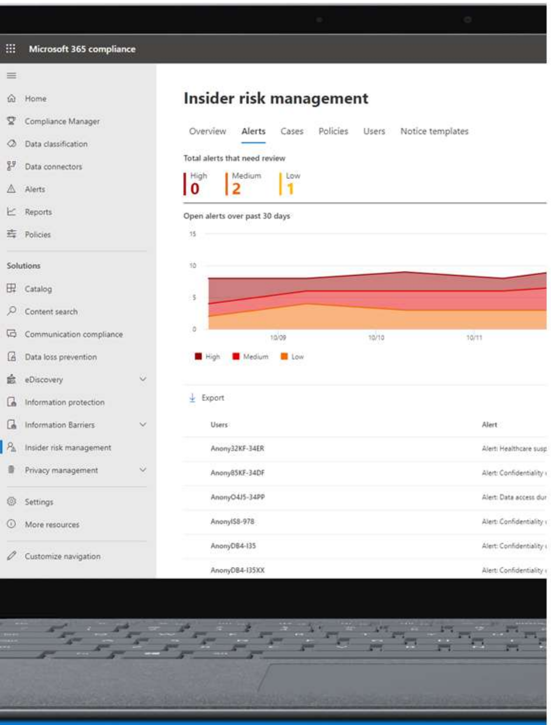
- Insider Risk Intro
- What is new in Insider Risk
- Communication Compliance Intro
- What is new in Communication Compliance
- Resources
- QnA

Microsoft

Insider Risk Management

Insider Risk Management

Quickly identify and act on insider risks with an integrated end-to-end approach



Insider risk management

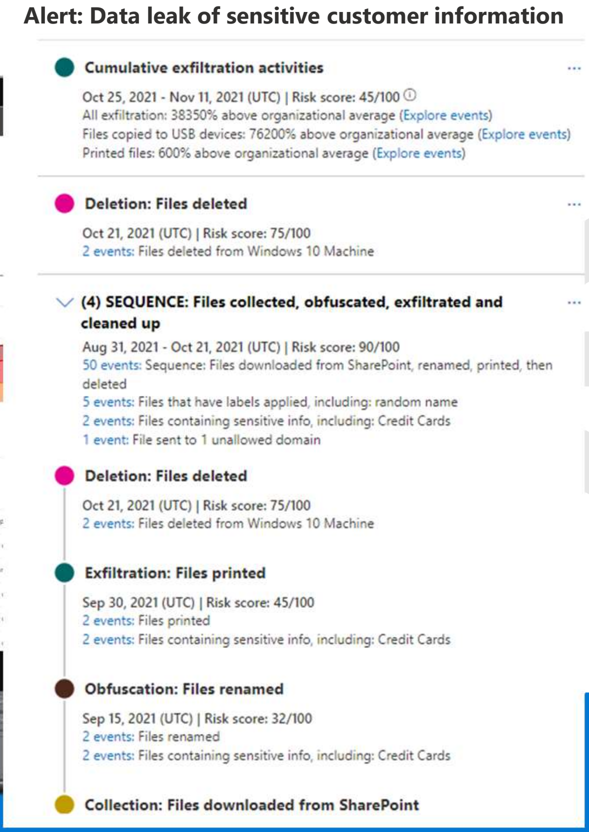
Total alerts that need review

High 0 | Medium 2 | Low 1

Open alerts over past 30 days

■ High ■ Medium ■ Low

Users	Alert
Anony32KF-34ER	Alert: Healthcare susp
Anony85KF-34DF	Alert: Confidentiality (
AnonyO4J5-34PP	Alert: Data access dur
AnonyI58-978	Alert: Confidentiality (
AnonyDB4-I35	Alert: Confidentiality (
AnonyDB4-I35XX	Alert: Confidentiality (



Alert: Data leak of sensitive customer information

● **Cumulative exfiltration activities** ···

Oct 25, 2021 - Nov 11, 2021 (UTC) | Risk score: 45/100 ⓘ
All exfiltration: 38350% above organizational average (Explore events)
Files copied to USB devices: 76200% above organizational average (Explore events)
Printed files: 600% above organizational average (Explore events)

● **Deletion: Files deleted** ···

Oct 21, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up ···

Aug 31, 2021 - Oct 21, 2021 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
5 events: Files that have labels applied, including: random name
2 events: Files containing sensitive info, including: Credit Cards
1 event: File sent to 1 unallowed domain

● **Deletion: Files deleted**

Oct 21, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

● **Exfiltration: Files printed**

Sep 30, 2021 (UTC) | Risk score: 45/100
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards

● **Obfuscation: Files renamed**

Sep 15, 2021 (UTC) | Risk score: 32/100
2 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards

● **Collection: Files downloaded from SharePoint**

Rich insights

Identify hidden risks with customizable ML templates requiring no endpoint agents.

Privacy built in

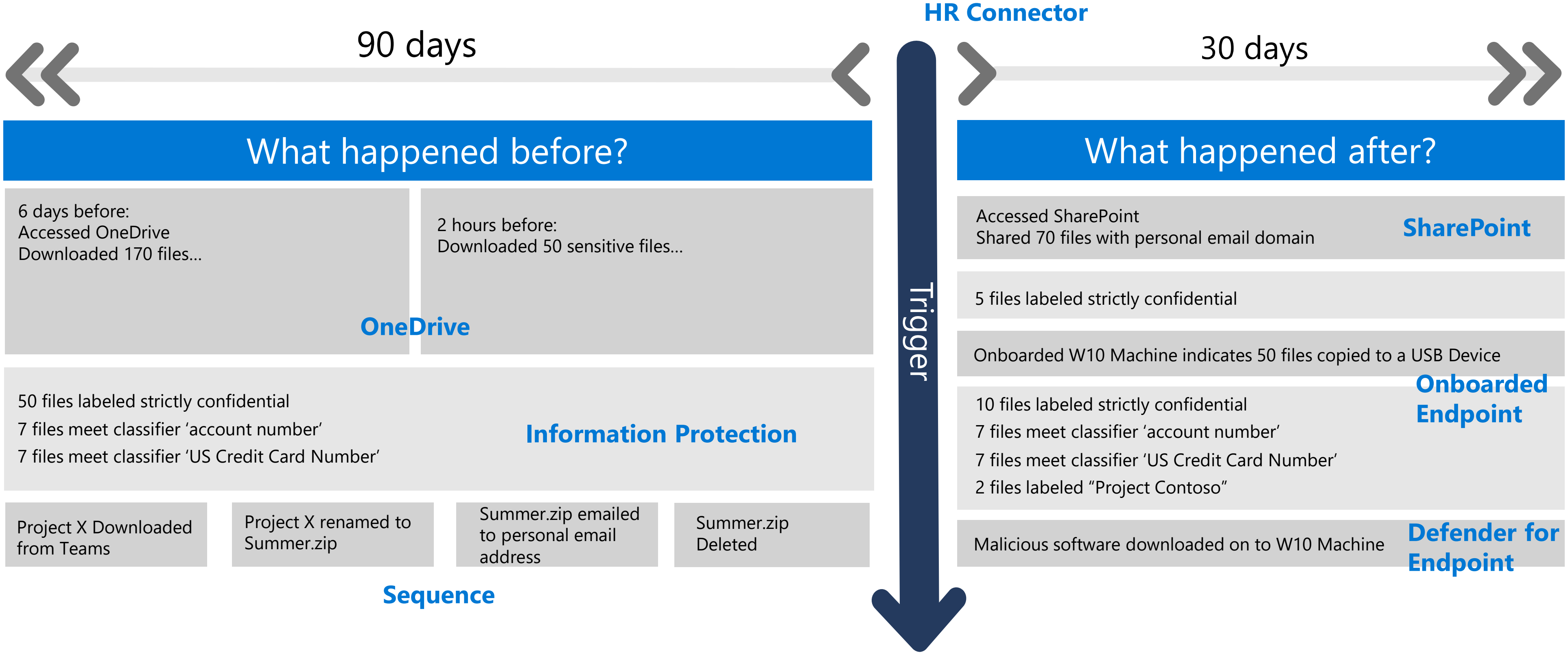
Pseudonymization and strong controls help appropriately manage data about risks.

End-to-end investigations

Integrated investigation workflows allow for collaboration across Security, HR, and Legal.

Insider Risk Management demystified

An employee enters resignation date in HR tool…



HR Connector

90 days

30 days

Trigger

What happened before?

6 days before:
Accessed OneDrive
Downloaded 170 files…

2 hours before:
Downloaded 50 sensitive files…

OneDrive

50 files labeled strictly confidential
7 files meet classifier 'account number'
7 files meet classifier 'US Credit Card Number'

Information Protection

Project X Downloaded from Teams

Project X renamed to Summer.zip

Summer.zip emailed to personal email address

Summer.zip Deleted

Sequence

What happened after?

Accessed SharePoint
Shared 70 files with personal email domain

SharePoint

5 files labeled strictly confidential

Onboarded W10 Machine indicates 50 files copied to a USB Device

Onboarded Endpoint

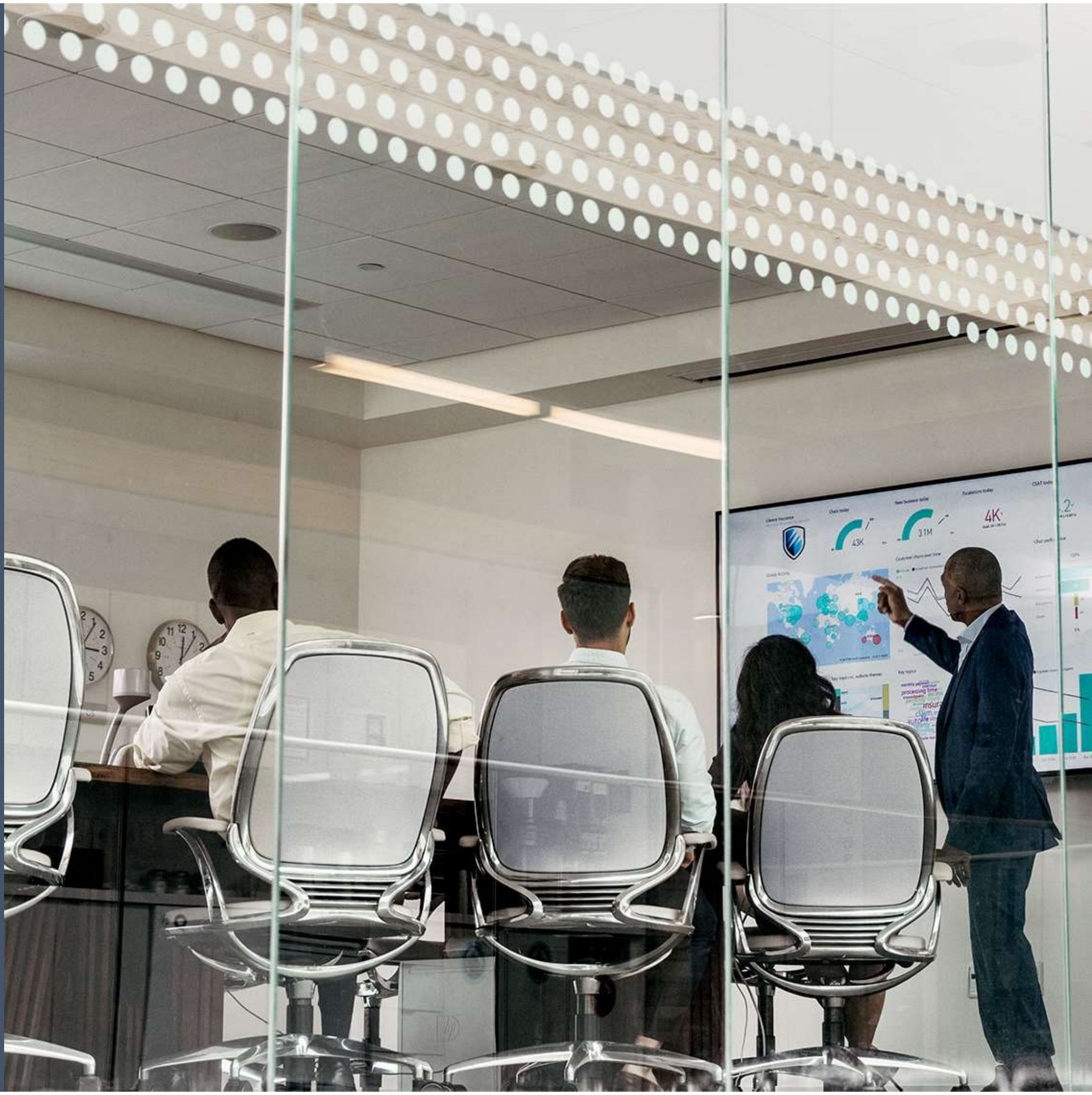
10 files labeled strictly confidential
7 files meet classifier 'account number'
7 files meet classifier 'US Credit Card Number'
2 files labeled "Project Contoso"

Malicious software downloaded on to W10 Machine

Defender for Endpoint

Microsoft

Insider Risk Management – What’s New



CF0

Aka.ms/InsiderRiskBlog

Platform Improvements

New capabilities	Product availability
Getting the most out of your investment with a guided experience	Preview - November
Alert review and triage enhancements	Preview - November
Enhanced policy trigger customization	Preview - November
Historical lookback into email-based exfiltration activities	Preview - November
Cumulative exfiltration activity Detection enhancements	Preview - November
Expanded coverage with macOS support	Preview - November
Integration with Microsoft Sentinel	Preview - November
Healthcare policy template and indicators	Preview - November

Slide 7

CF0 Looks like you have captured the full list (and in the order found in the blog). Can you include the aka link in the top right? Aka.ms/InsiderRiskBlog
Caitlin Fitzgerald, 2021-11-29T20:00:13.014

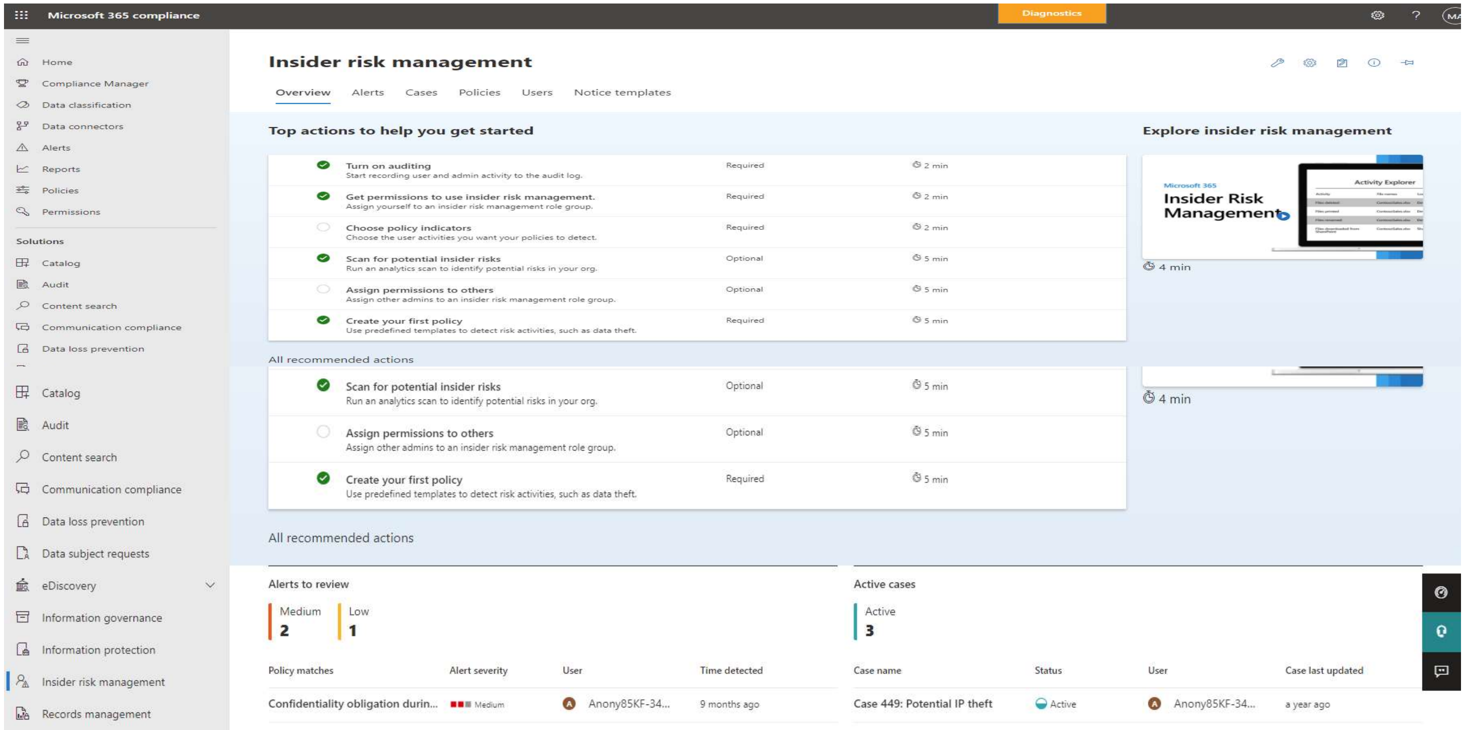
PD0 0 Done
Patrick David, 2021-11-29T20:26:09.359

Preview

Recommended Actions *to Drive Ease-of-use!*

Ease of setup and use are the top considerations for purchase by decision makers

In-product guided experience helps you setup with confidence and ensure you're getting the maximum value



Insider risk management

Top actions to help you get started

✓	Turn on auditing Start recording user and admin activity to the audit log.	Required	2 min
✓	Get permissions to use insider risk management. Assign yourself to an insider risk management role group.	Required	2 min
○	Choose policy indicators Choose the user activities you want your policies to detect.	Required	2 min
✓	Scan for potential insider risks Run an analytics scan to identify potential risks in your org.	Optional	5 min
○	Assign permissions to others Assign other admins to an insider risk management role group.	Optional	5 min
✓	Create your first policy Use predefined templates to detect risk activities, such as data theft.	Required	5 min

All recommended actions

✓	Scan for potential insider risks Run an analytics scan to identify potential risks in your org.	Optional	5 min
○	Assign permissions to others Assign other admins to an insider risk management role group.	Optional	5 min
✓	Create your first policy Use predefined templates to detect risk activities, such as data theft.	Required	5 min

Explore insider risk management

All recommended actions

Alerts to review

Medium 2 | Low 1

Policy matches	Alert severity	User	Time detected
Confidentiality obligation durin...	Medium	Anony85KF-34...	9 months ago

Active cases

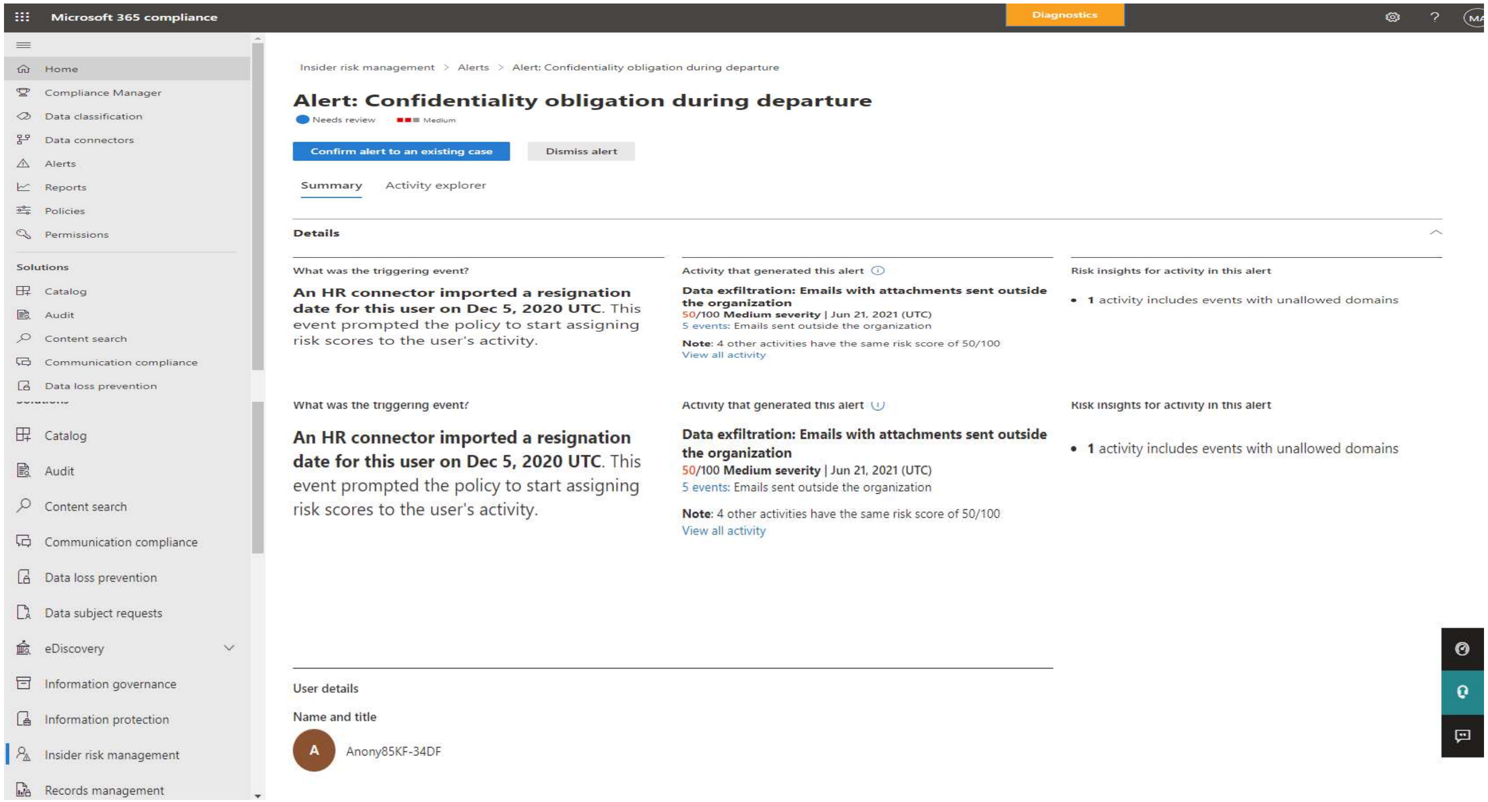
Active 3

Case name	Status	User	Case last updated
Case 449: Potential IP theft	Active	Anony85KF-34...	a year ago

Preview

Alert Review - *Reduce Time-to-action!*

Make it easier to understand the context of an alert and reduce time-to-action



Insider risk management > Alerts > Alert: Confidentiality obligation during departure

Alert: Confidentiality obligation during departure

● Needs review ▬ Medium

Details

What was the triggering event?

An HR connector imported a resignation date for this user on Dec 5, 2020 UTC. This event prompted the policy to start assigning risk scores to the user's activity.

Activity that generated this alert

Data exfiltration: Emails with attachments sent outside the organization

50/100 **Medium severity** | Jun 21, 2021 (UTC)

5 events: Emails sent outside the organization

Note: 4 other activities have the same risk score of 50/100

View all activity

Risk insights for activity in this alert

- **1** activity includes events with unallowed domains

What was the triggering event?

An HR connector imported a resignation date for this user on Dec 5, 2020 UTC. This event prompted the policy to start assigning risk scores to the user's activity.

Activity that generated this alert

Data exfiltration: Emails with attachments sent outside the organization

50/100 **Medium severity** | Jun 21, 2021 (UTC)

5 events: Emails sent outside the organization

Note: 4 other activities have the same risk score of 50/100

View all activity

Risk insights for activity in this alert

- **1** activity includes events with unallowed domains

User details

Name and title

A Anony85KF-34DF

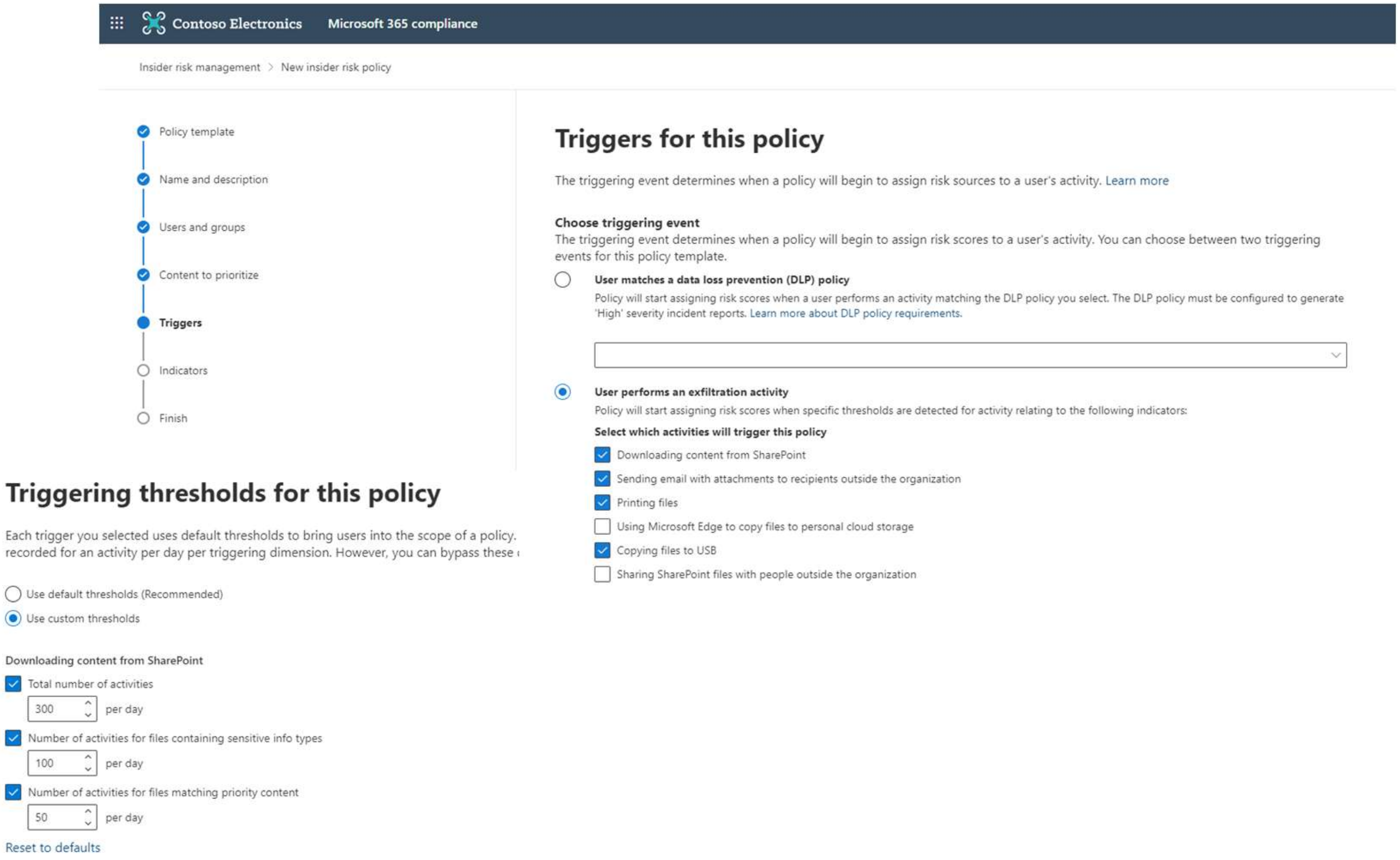
Policy Trigger Customization Enhancements

Preview

Further tune your policies to trigger on specific events and custom thresholds including:

- Printing Files
- Using Edge to copy files to cloud storage
- Copy Files to USB
- Share SharePoint files with people outside the organization

Helps with greater alignment of insider risk policies with organizational risk appetite



Triggers for this policy

The triggering event determines when a policy will begin to assign risk sources to a user's activity. Learn more

Choose triggering event

The triggering event determines when a policy will begin to assign risk scores to a user's activity. You can choose between two triggering events for this policy template.

○ **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.

● **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

☑ Downloading content from SharePoint
☑ Sending email with attachments to recipients outside the organization
☑ Printing files
☐ Using Microsoft Edge to copy files to personal cloud storage
☑ Copying files to USB
☐ Sharing SharePoint files with people outside the organization

Triggering thresholds for this policy

Each trigger you selected uses default thresholds to bring users into the scope of a policy. recorded for an activity per day per triggering dimension. However, you can bypass these

○ Use default thresholds (Recommended)
● Use custom thresholds

Downloading content from SharePoint

☑ Total number of activities
300 per day
☑ Number of activities for files containing sensitive info types
100 per day
☑ Number of activities for files matching priority content
50 per day

Reset to defaults

Preview

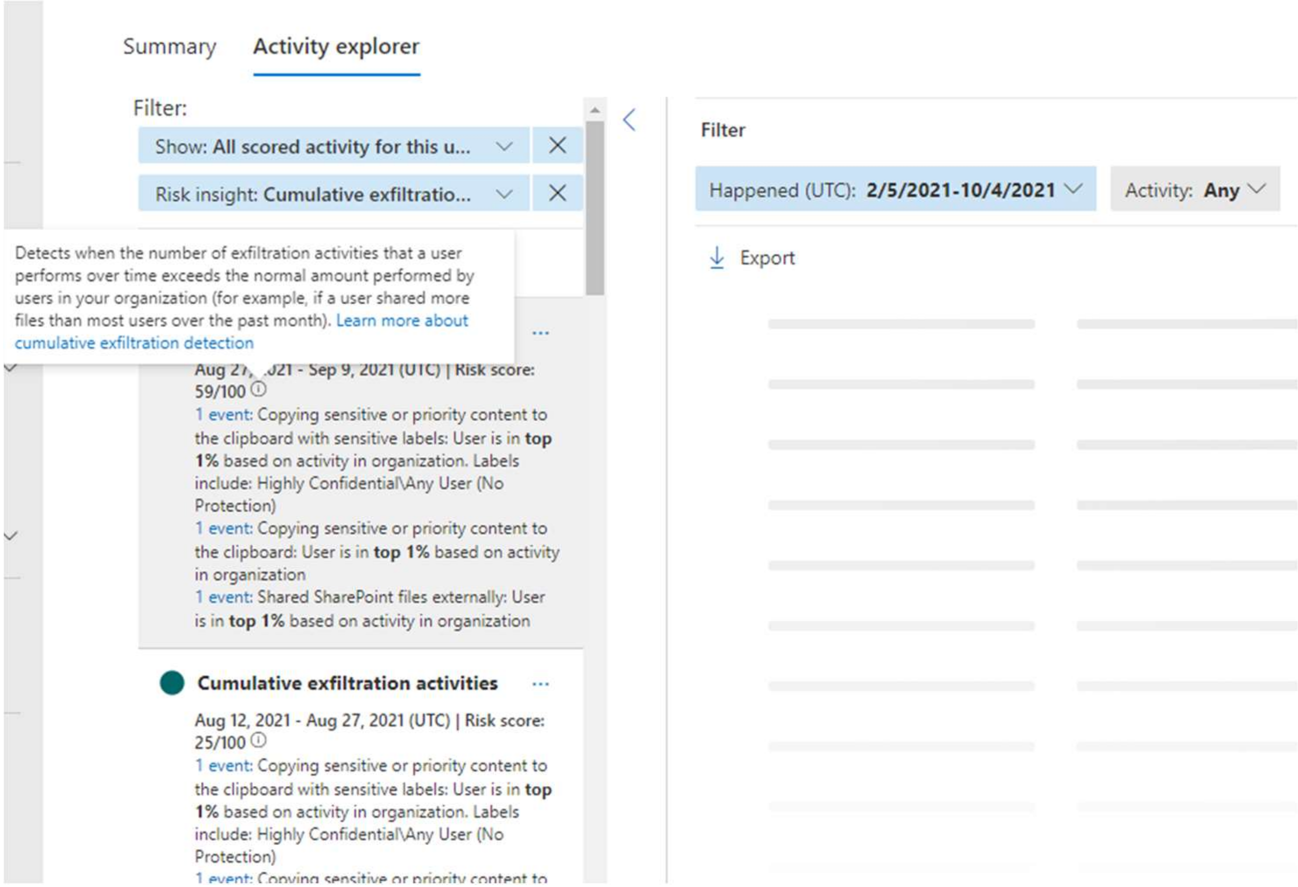
Enhancements to Cumulative Exfiltration Anomaly Detection (CEAD)

Detects when the number of exfiltration activities that a user performs over 30 days exceeds the organizational median

- ○ Example: User shares more files than most

Enhancements:

- ○ Added clarity on activity percent
- ○ Leverages sensitivity labels to prioritize sensitive documents



Filter:

Show: All scored activity for this u...

Risk insight: Cumulative exfiltratio...

Detects when the number of exfiltration activities that a user performs over time exceeds the normal amount performed by users in your organization (for example, if a user shared more files than most users over the past month). Learn more about cumulative exfiltration detection

Aug 27, .021 - Sep 9, 2021 (UTC) | Risk score: 59/100

1 event: Copying sensitive or priority content to the clipboard with sensitive labels: User is in **top 1%** based on activity in organization. Labels include: Highly Confidential\Any User (No Protection)

1 event: Copying sensitive or priority content to the clipboard: User is in **top 1%** based on activity in organization

1 event: Shared SharePoint files externally: User is in **top 1%** based on activity in organization

Cumulative exfiltration activities

Aug 12, 2021 - Aug 27, 2021 (UTC) | Risk score: 25/100

1 event: Copying sensitive or priority content to the clipboard with sensitive labels: User is in **top 1%** based on activity in organization. Labels include: Highly Confidential\Any User (No Protection)

1 event: Copying sensitive or priority content to

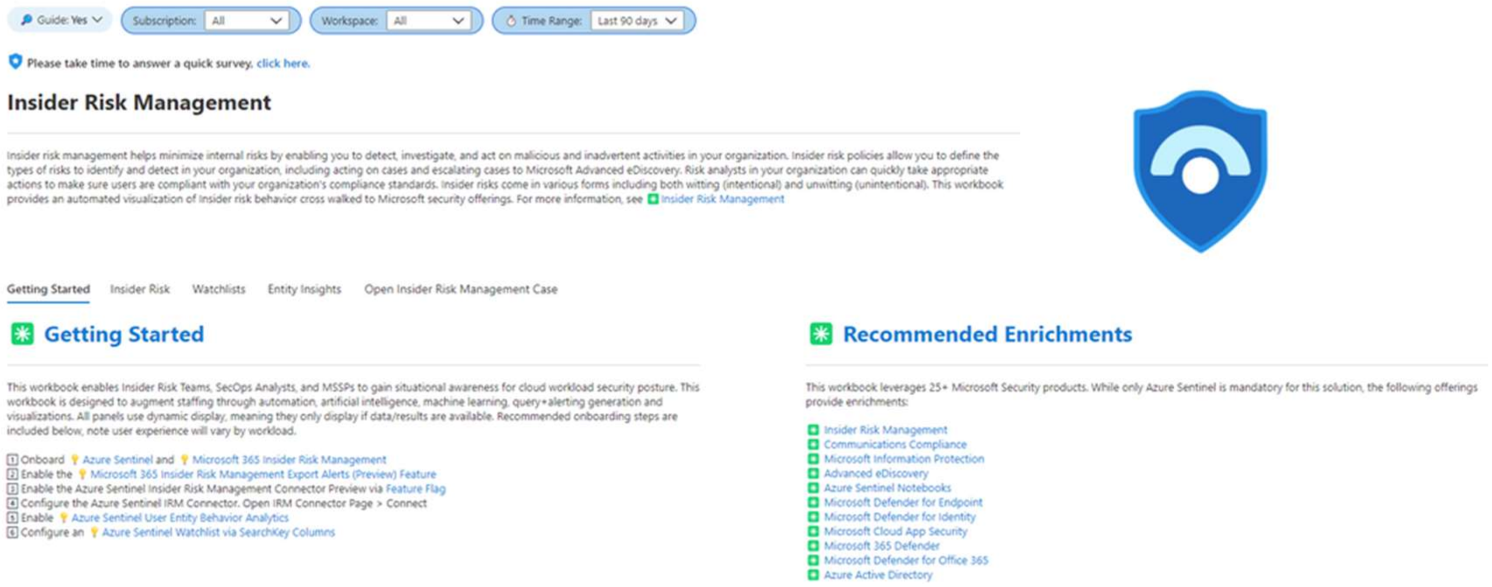
Happened (UTC): **2/5/2021-10/4/2021**

Activity: **Any**

Preview

Integration with Microsoft Sentinel

- This native connector allows for seamless import of alerts
- Single pane of glass to review alerts for insider risk in a broader organizational context
- Workbook integrates telemetry from 25+ Microsoft security products to provide actionable insights into Insider Risk Management
- “Better together” story between Microsoft 365 Insider Risk Management and Microsoft Sentinel



Please take time to answer a quick survey, click here.

Insider Risk Management

Insider risk management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Insider risk policies allow you to define the types of risks to identify and detect in your organization, including acting on cases and escalating cases to Microsoft Advanced eDiscovery. Risk analysts in your organization can quickly take appropriate actions to make sure users are compliant with your organization's compliance standards. Insider risks come in various forms including both witting (intentional) and unwitting (unintentional). This workbook provides an automated visualization of Insider risk behavior cross walked to Microsoft security offerings. For more information, see Insider Risk Management

Getting Started

This workbook enables Insider Risk Teams, SecOps Analysts, and MSSPs to gain situational awareness for cloud workload security posture. This workbook is designed to augment staffing through automation, artificial intelligence, machine learning, query+alerting generation and visualizations. All panels use dynamic display, meaning they only display if data/results are available. Recommended onboarding steps are included below, note user experience will vary by workload.

1. Onboard Azure Sentinel and Microsoft 365 Insider Risk Management
2. Enable the Microsoft 365 Insider Risk Management Export Alerts (Preview) Feature
3. Enable the Azure Sentinel Insider Risk Management Connector Preview via Feature Flag
4. Configure the Azure Sentinel IRM Connector. Open IRM Connector Page > Connect
5. Enable Azure Sentinel User Entity Behavior Analytics
6. Configure an Azure Sentinel Watchlist via SearchKey Columns

Recommended Enrichments

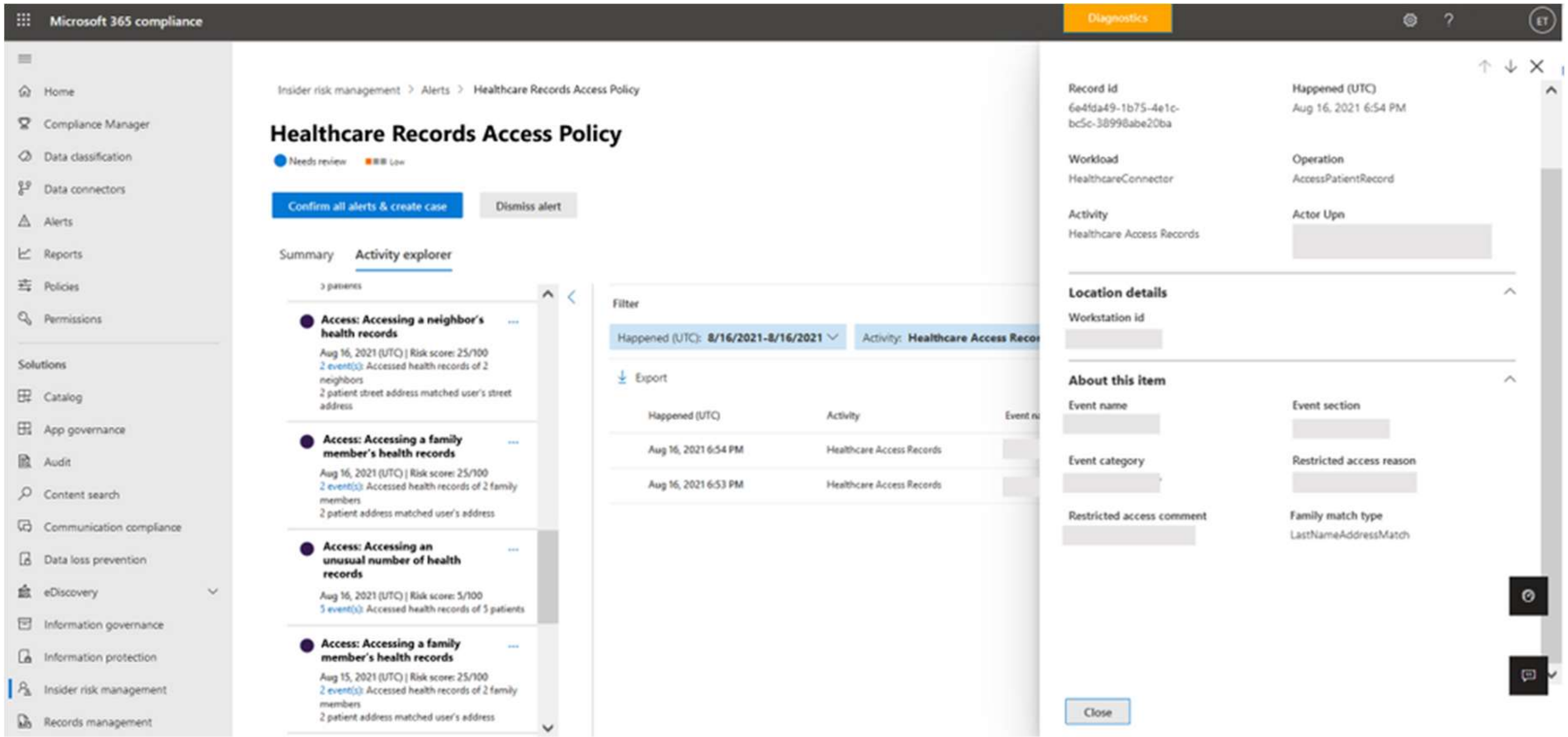
This workbook leverages 25+ Microsoft Security products. While only Azure Sentinel is mandatory for this solution, the following offerings provide enrichments:

- Insider Risk Management
- Communications Compliance
- Microsoft Information Protection
- Advanced eDiscovery
- Azure Sentinel Notebooks
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Cloud App Security
- Microsoft 365 Defender
- Microsoft Defender for Office 365
- Azure Active Directory

Healthcare Policy Template and Indicators

Preview

Healthcare policy template and indicators to help reduce insider risks in the healthcare industry such as patient data misuse



Insider risk management > Alerts > Healthcare Records Access Policy

Healthcare Records Access Policy

● Needs review ■■■ Low

5 patients

Access: Accessing a neighbor's health records
Aug 16, 2021 (UTC) | Risk score: 25/100
2 event(s): Accessed health records of 2 neighbors
2 patient street address matched user's street address

Access: Accessing a family member's health records
Aug 16, 2021 (UTC) | Risk score: 25/100
2 event(s): Accessed health records of 2 family members
2 patient address matched user's address

Access: Accessing an unusual number of health records
Aug 16, 2021 (UTC) | Risk score: 5/100
5 event(s): Accessed health records of 5 patients

Access: Accessing a family member's health records
Aug 15, 2021 (UTC) | Risk score: 25/100
2 event(s): Accessed health records of 2 family members
2 patient address matched user's address

Happened (UTC): **8/16/2021-8/16/2021**   Activity: **Healthcare Access Recor**

Happened (UTC)	Activity	Event na
Aug 16, 2021 6:54 PM	Healthcare Access Records	
Aug 16, 2021 6:53 PM	Healthcare Access Records	

Record id
6e4fda49-1b75-4e1c-bc5c-38998abe20ba

Happened (UTC)
Aug 16, 2021 6:54 PM

Workload
HealthcareConnector

Operation
AccessPatientRecord

Activity
Healthcare Access Records

Actor Upn

Location details

Workstation id

About this item

Event name

Event section

Event category

Restricted access reason

Restricted access comment

Family match type
LastNameAddressMatch

GA Announcements

- Browser file exfiltration detection across Edge and Chrome
- Device indicators
- Policy health
- Export alerts
- View activity in the insider risk audit log
- Configure allowed, unallowed, and third-party domains
- Analytics
- Enhancements to content explorer experience
- Policy customization
- AAD Leaver signals and triggers

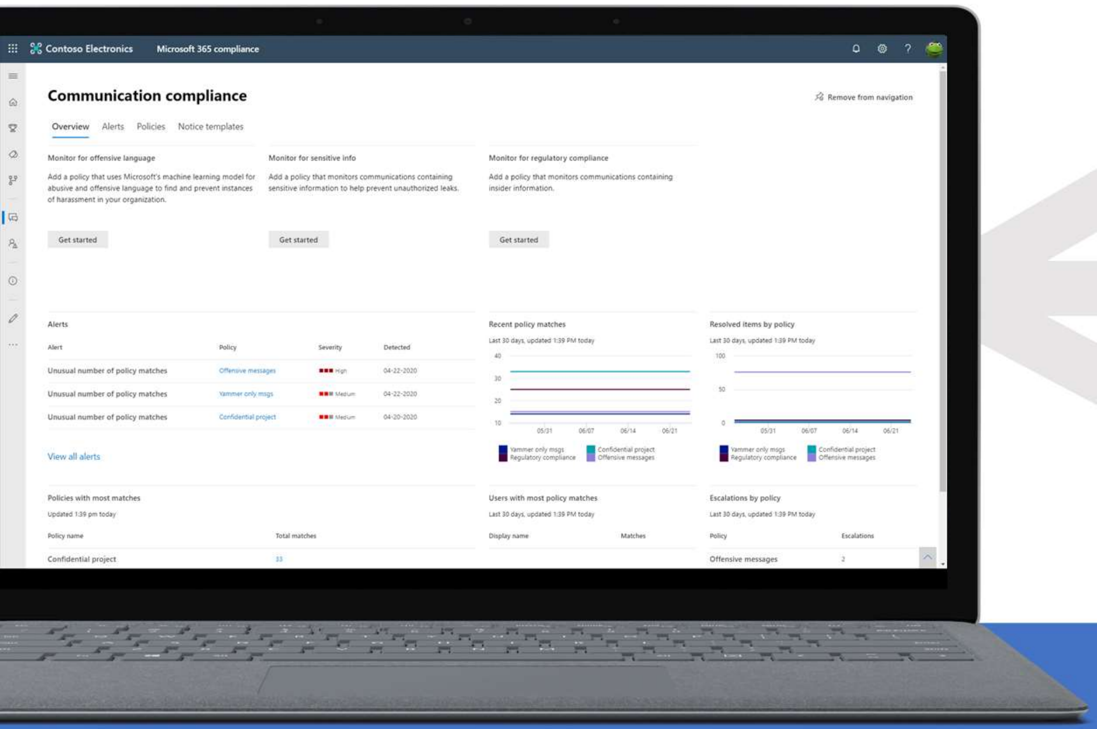
Aka.ms/InsiderRiskBlog

Microsoft

Communication Compliance

Communication Compliance

Quickly identify and act on code-of-conduct policy violations



Communication compliance

Monitor for offensive language

Add a policy that uses Microsoft's machine learning model for abusive and offensive language to find and prevent instances of harassment in your organization.

Monitor for sensitive info

Add a policy that monitors communications containing sensitive information to help prevent unauthorized leaks.

Monitor for regulatory compliance

Add a policy that monitors communications containing insider information.

Alerts

Alert	Policy	Severity	Detected
Unusual number of policy matches	Offensive messages	High	04-22-2020
Unusual number of policy matches	Yammer only msgs	Medium	04-22-2020
Unusual number of policy matches	Confidential project	Medium	04-20-2020

Recent policy matches

Last 30 days, updated 1:39 PM today

Resolved items by policy

Last 30 days, updated 1:39 PM today

Policies with most matches

Updated 1:39 pm today

Policy name	Total matches
Confidential project	33

Users with most policy matches

Last 30 days, updated 1:39 PM today

Display name	Matches

Escalations by policy

Last 30 days, updated 1:39 PM today

Policy	Escalations
Offensive messages	2

Intelligent customizable playbooks

Leverage machine learning to detect violations across Teams, Exchange, and 3rd-party content.

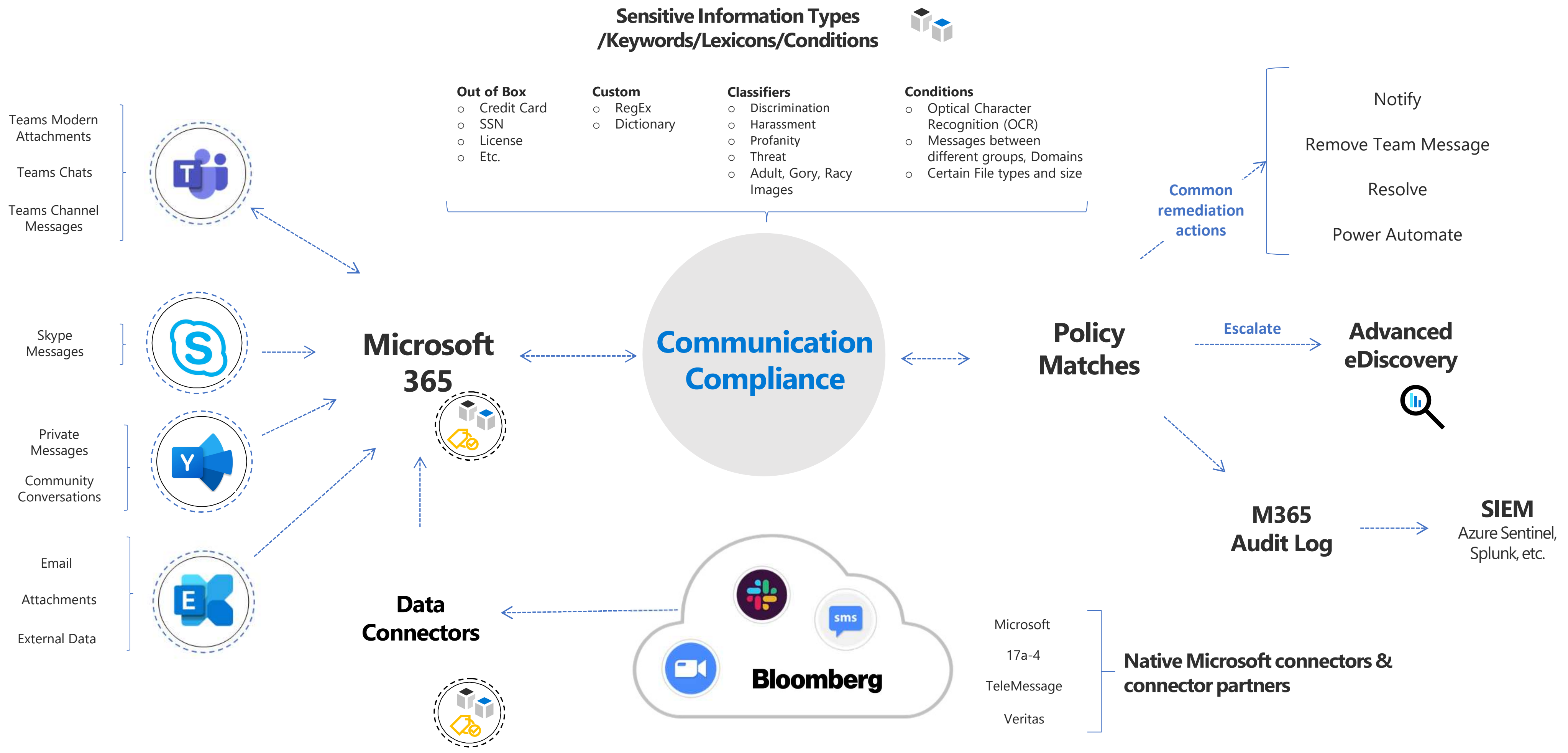
Flexible remediation workflows

Remediation workflows to quickly act on violations and remove incriminating messages on Teams.

Privacy, built in

Identify and investigate communications risks while maintaining end-user privacy.

Communication Compliance Overview



Sensitive Information Types /Keywords/Lexicons/Conditions

Out of Box
- Credit Card
- SSN
- License
- Etc.

Custom
- RegEx
- Dictionary

Classifiers
- Discrimination
- Harassment
- Profanity
- Threat
- Adult, Gory, Racy Images

Conditions
- Optical Character Recognition (OCR)
- Messages between different groups, Domains
- Certain File types and size

Teams Modern Attachments

Teams Chats

Teams Channel Messages

Skype Messages

Private Messages

Community Conversations

Email

Attachments

External Data

Microsoft 365

Communication Compliance

Policy Matches

Common remediation actions

Notify

Remove Team Message

Resolve

Power Automate

Escalate

Advanced eDiscovery

M365 Audit Log

SIEM

Azure Sentinel, Splunk, etc.

Data Connectors

Bloomberg

Microsoft

17a-4

TeleMessage

Veritas

Native Microsoft connectors & connector partners

Microsoft

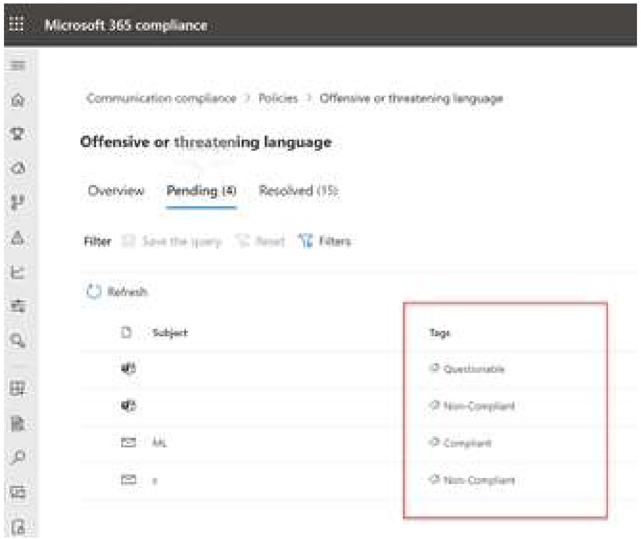
Communication Compliance – What's New

Aka.ms/ccignite2021

Platform Improvements

New capabilities	Product availability
Communication Compliance tagging improvements	GA - October
Communication Compliance cross-tenant classifier feedback	GA - November
Communication Compliance discrimination classifier	Preview – July
DLP Policy Recommendation	Preview - October
Day Zero Insights	Preview - November
Additional Classifier language support	Preview - November
Review Activity Summary	Preview - December
In product getting started videos	Coming Soon
Analyze content of Modern Attachments - Teams	Coming Soon

Communication Compliance Tagging Improvements

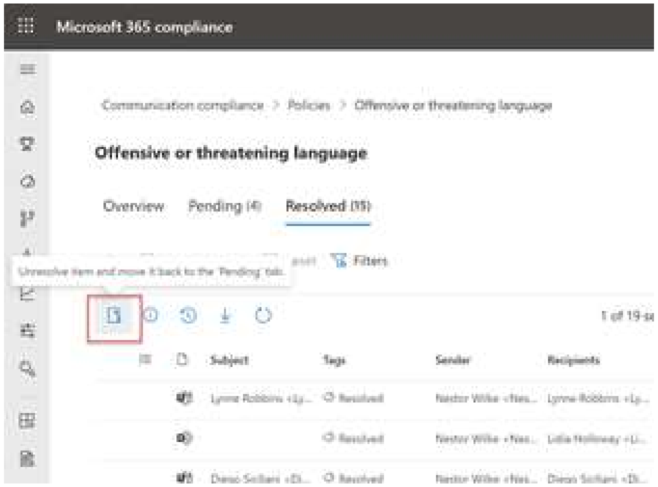


Microsoft 365 compliance
Communication compliance > Policies > Offensive or threatening language

Offensive or threatening language

Subject	Tags
	Questionable
	Non-Compliant
AL	Compliant
x	Non-Compliant

Added column that will display the current tag applied



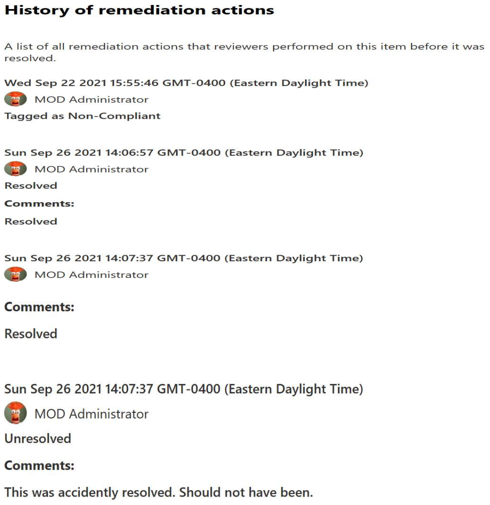
Microsoft 365 compliance
Communication compliance > Policies > Offensive or threatening language

Offensive or threatening language

Overview
Pending (4)
Resolved (15)
Filters
Unresolve item and move it back to the 'Pending' tab.
1 of 19 s

Subject	Tags	Sender	Recipients
Lynne Robbins <Ly...	Resolved	Nestor Wilke <Nes...	Lynne Robbins <Ly...
	Resolved	Nestor Wilke <Nes...	Lidia Holloway <Li...
Diego Siciliani <Di...	Resolved	Nestor Wilke <Nes...	Diego Siciliani <Di...

Ability to unresolve a message



History of remediation actions

A list of all remediation actions that reviewers performed on this item before it was resolved.

Wed Sep 22 2021 15:55:46 GMT-0400 (Eastern Daylight Time)
MOD Administrator
Tagged as Non-Compliant

Sun Sep 26 2021 14:06:57 GMT-0400 (Eastern Daylight Time)
MOD Administrator
Resolved
Comments:
Resolved

Sun Sep 26 2021 14:07:37 GMT-0400 (Eastern Daylight Time)
MOD Administrator

Comments:

Resolved

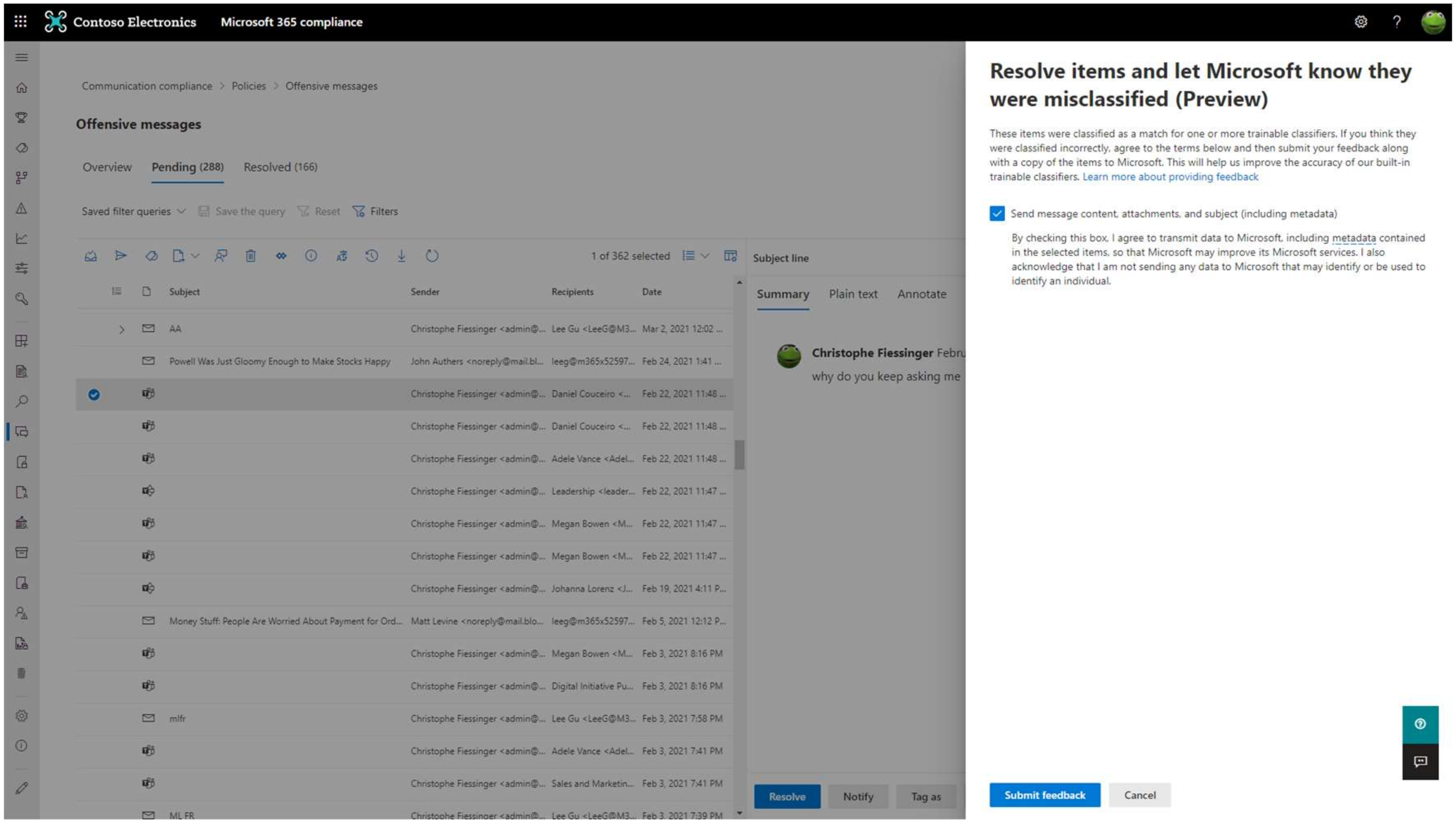
Sun Sep 26 2021 14:07:37 GMT-0400 (Eastern Daylight Time)
MOD Administrator
Unresolved
Comments:
This was accidently resolved. Should not have been.

All while being audited

Global Feedback Loop

Allows investigators to submit feedback directly to Microsoft on misclassified policy matches

Effectively retrains and improves the detection algorithm



Offensive messages

Subject	Sender	Recipients	Date
AA	Christophe Fiessinger <admin@...	Lee Gu <LeeG@M3...	Mar 2, 2021 12:02 ...
Powell Was Just Gloomy Enough to Make Stocks Happy	John Authers <noreply@mail.bl...	leeg@m365x52597...	Feb 24, 2021 1:41 ...
	Christophe Fiessinger <admin@...	Daniel Couceiro <...	Feb 22, 2021 11:48 ...
	Christophe Fiessinger <admin@...	Daniel Couceiro <...	Feb 22, 2021 11:48 ...
	Christophe Fiessinger <admin@...	Adele Vance <Adel...	Feb 22, 2021 11:48 ...
	Christophe Fiessinger <admin@...	Leadership <leader...	Feb 22, 2021 11:47 ...
	Christophe Fiessinger <admin@...	Megan Bowen <M...	Feb 22, 2021 11:47 ...
	Christophe Fiessinger <admin@...	Megan Bowen <M...	Feb 22, 2021 11:47 ...
	Christophe Fiessinger <admin@...	Johanna Lorenz <J...	Feb 19, 2021 4:11 P...
Money Stuff: People Are Worried About Payment for Ord...	Matt Levine <noreply@mail.blo...	leeg@m365x52597...	Feb 5, 2021 12:12 P...
	Christophe Fiessinger <admin@...	Megan Bowen <M...	Feb 3, 2021 8:16 PM
	Christophe Fiessinger <admin@...	Digital Initiative Pu...	Feb 3, 2021 8:16 PM
mlfr	Christophe Fiessinger <admin@...	Lee Gu <LeeG@M3...	Feb 3, 2021 7:58 PM
	Christophe Fiessinger <admin@...	Adele Vance <Adel...	Feb 3, 2021 7:41 PM
	Christophe Fiessinger <admin@...	Sales and Marketin...	Feb 3, 2021 7:41 PM
ML FR	Christophe Fiessinger <admin@...	Lee Gu <LeeG@M3...	Feb 3, 2021 7:39 PM

Christophe Fiessinger Febru

why do you keep asking me

Resolve items and let Microsoft know they were misclassified (Preview)

These items were classified as a match for one or more trainable classifiers. If you think they were classified incorrectly, agree to the terms below and then submit your feedback along with a copy of the items to Microsoft. This will help us improve the accuracy of our built-in trainable classifiers. Learn more about providing feedback

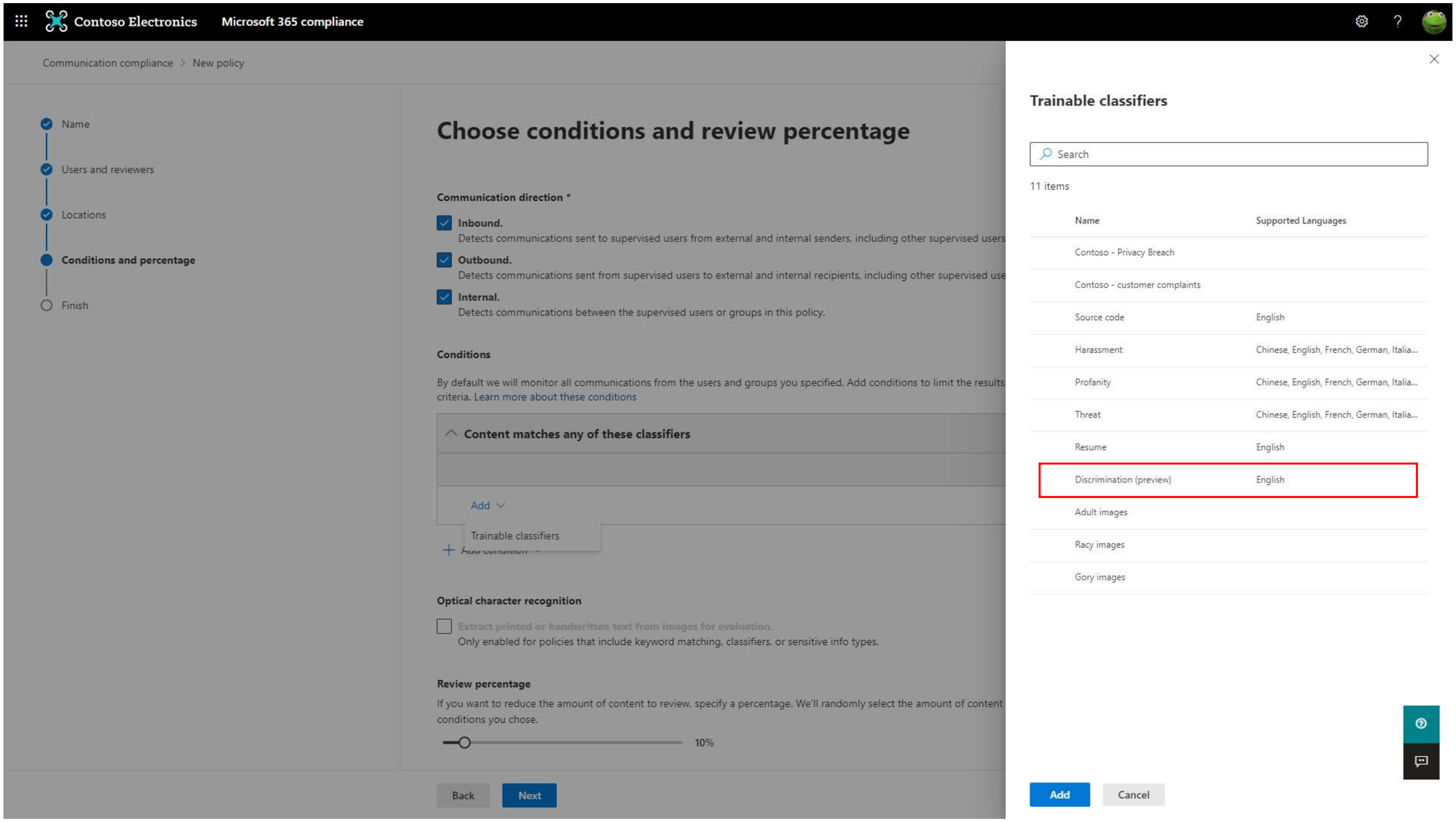
☑ Send message content, attachments, and subject (including metadata)

By checking this box, I agree to transmit data to Microsoft, including metadata contained in the selected items, so that Microsoft may improve its Microsoft services. I also acknowledge that I am not sending any data to Microsoft that may identify or be used to identify an individual.

Discrimination Classifier

Preview

Aims to detect and triage explicit discriminatory language



Communication compliance > New policy

- ● Name
- ● Users and reviewers
- ● Locations
- ● **Conditions and percentage**
- ○ Finish

Choose conditions and review percentage

Communication direction *

☑ **Inbound.**
Detects communications sent to supervised users from external and internal senders, including other supervised users

☑ **Outbound.**
Detects communications sent from supervised users to external and internal recipients, including other supervised use

☑ **Internal.**
Detects communications between the supervised users or groups in this policy.

Conditions

By default we will monitor all communications from the users and groups you specified. Add conditions to limit the results criteria. Learn more about these conditions

Content matches any of these classifiers

Optical character recognition

□ Extract printed or handwritten text from images for evaluation.
Only enabled for policies that include keyword matching, classifiers, or sensitive info types.

Review percentage

If you want to reduce the amount of content to review, specify a percentage. We'll randomly select the amount of content conditions you chose.

10%

Trainable classifiers

11 items

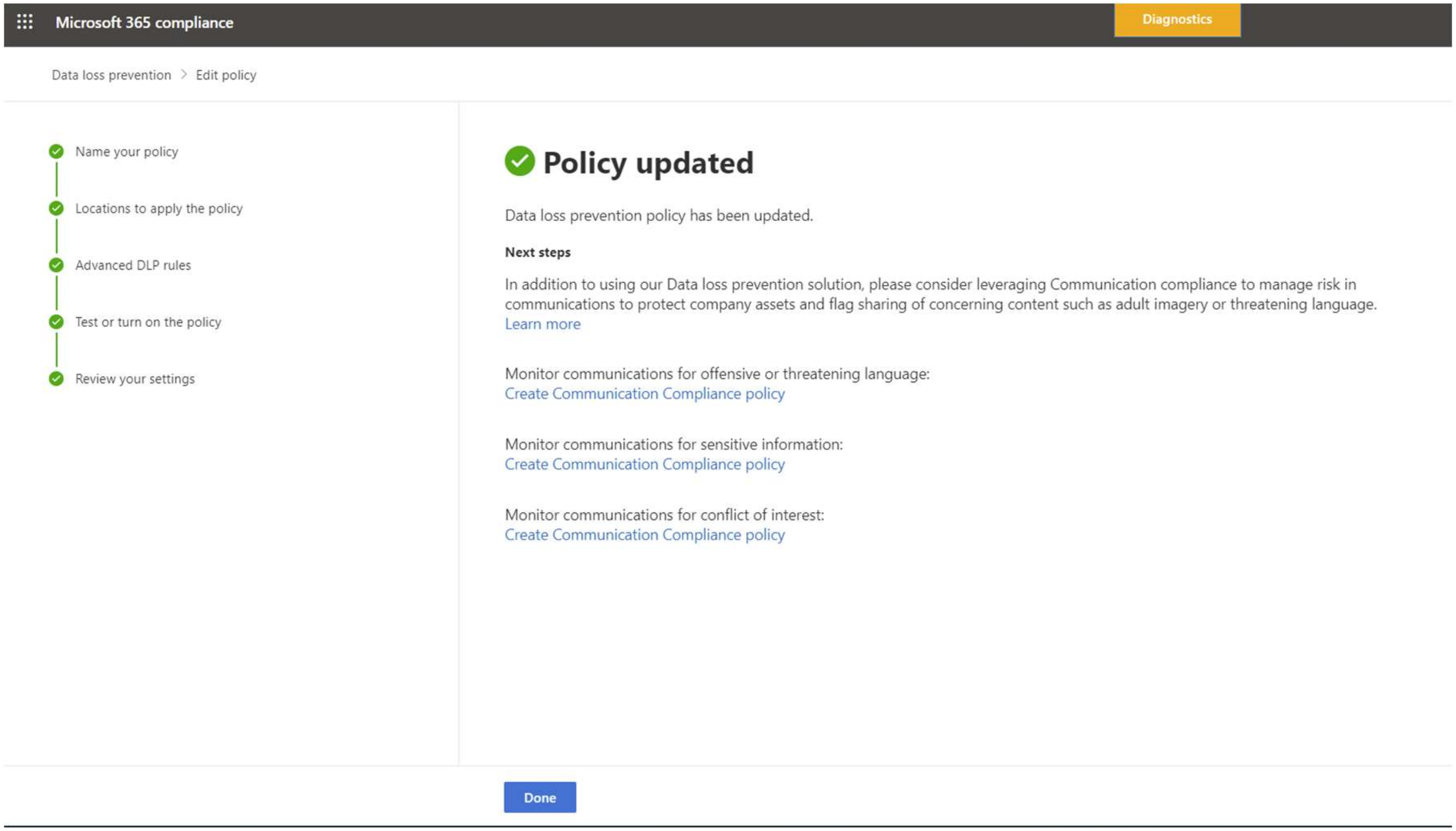
Name	Supported Languages
Contoso - Privacy Breach	
Contoso - customer complaints	
Source code	English
Harassment	Chinese, English, French, German, Italia...
Profanity	Chinese, English, French, German, Italia...
Threat	Chinese, English, French, German, Italia...
Resume	English
Discrimination (preview)	English
Adult images	
Racy images	
Gory images	

Communication Compliance within the DLP workflow

Preview

Ability to apply DLP policy insights to your insider risk practice to better identify user behavior and intent

Now you will be directed to configure a relevant policy in Communication Compliance at the end of the Data Loss Prevention policy configuration flow



Policy updated

Data loss prevention policy has been updated.

Next steps

In addition to using our Data loss prevention solution, please consider leveraging Communication compliance to manage risk in communications to protect company assets and flag sharing of concerning content such as adult imagery or threatening language.
Learn more

Monitor communications for offensive or threatening language:
Create Communication Compliance policy

Monitor communications for sensitive information:
Create Communication Compliance policy

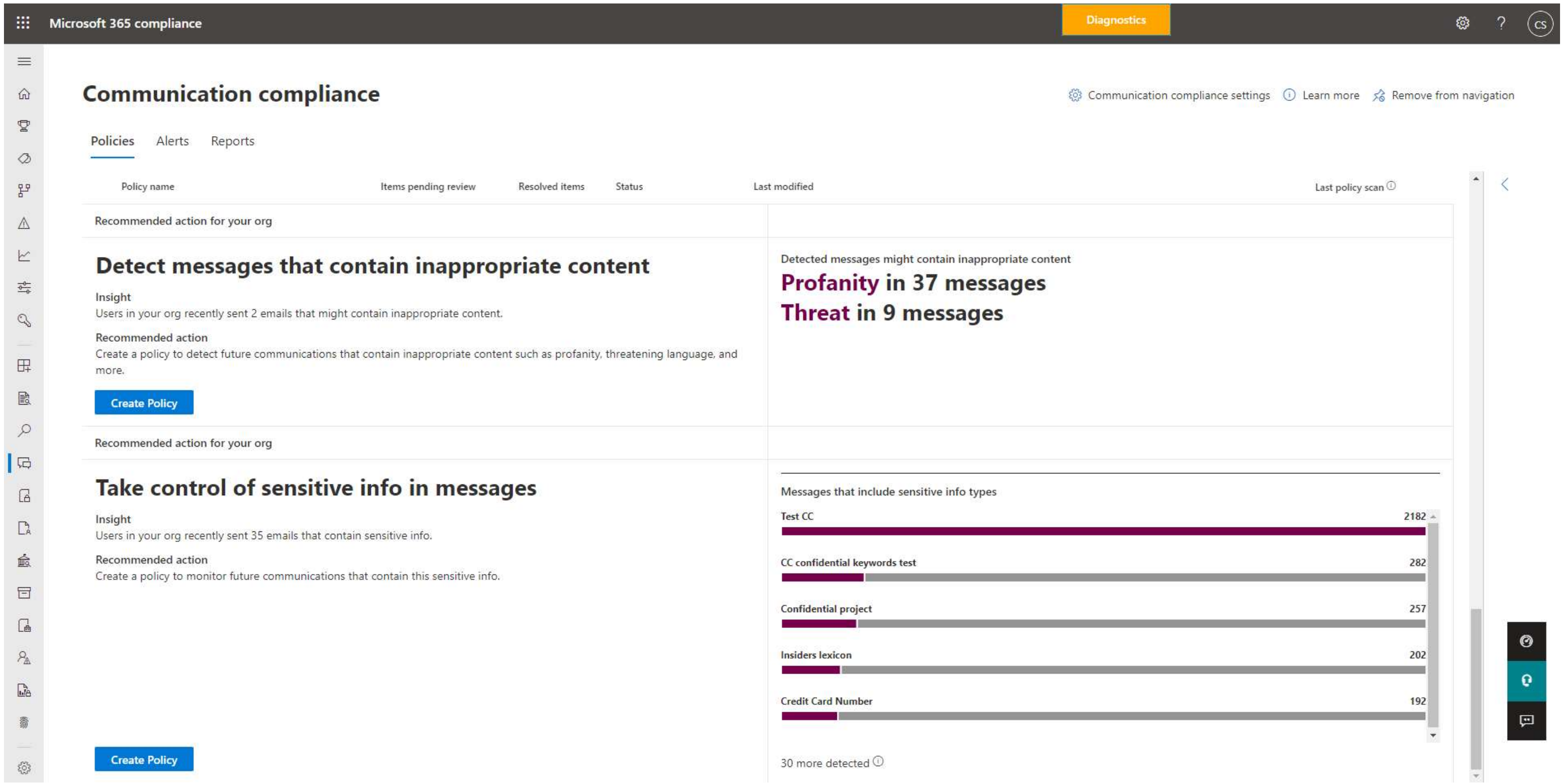
Monitor communications for conflict of interest:
Create Communication Compliance policy

Zero Day Insights

Preview

Discover risks you may not be aware of

Displays the aggregate number of matches per classification type, with none of the insights containing any personally identifiable information



Communication compliance

Policy name	Items pending review	Resolved items	Status	Last modified	Last policy scan ⓘ

Recommended action for your org

Detect messages that contain inappropriate content

Insight
Users in your org recently sent 2 emails that might contain inappropriate content.

Recommended action
Create a policy to detect future communications that contain inappropriate content such as profanity, threatening language, and more.

Create Policy

Detected messages might contain inappropriate content

Profanity in 37 messages

Threat in 9 messages

Recommended action for your org

Take control of sensitive info in messages

Insight
Users in your org recently sent 35 emails that contain sensitive info.

Recommended action
Create a policy to monitor future communications that contain this sensitive info.

Create Policy

Messages that include sensitive info types

Sensitive info type	Messages
Test CC	2182
CC confidential keywords test	282
Confidential project	257
Insiders lexicon	202
Credit Card Number	192

30 more detected ⓘ

Preview

Additional language support

Four additional language support for Threat, Harassment and Profanity classifiers:

- Arabic
- Dutch
- Korean
- Chinese Traditional

Existing languages supported: English, French, Spanish, German, Portuguese, Italian, Japanese, and Chinese.

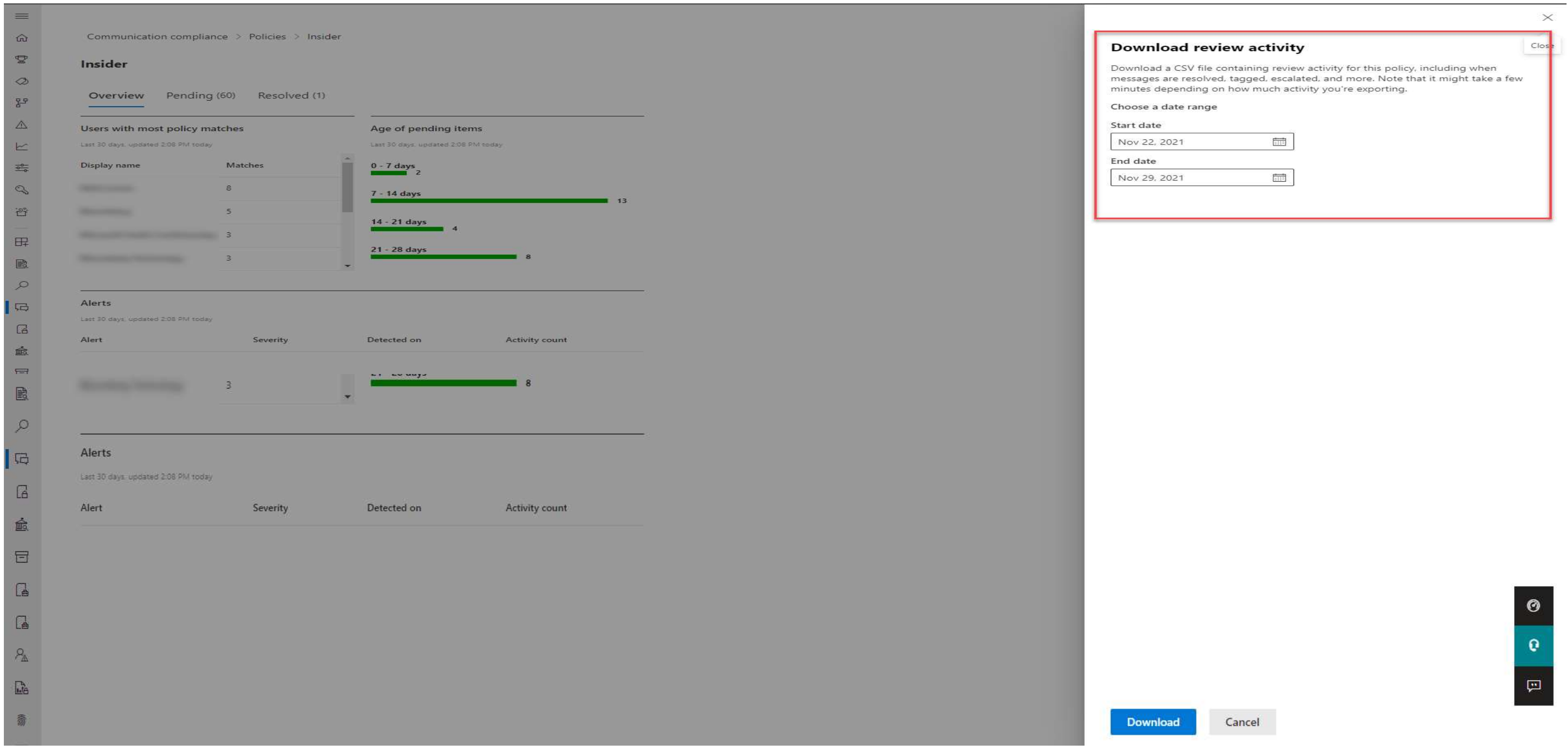
Review Activity Summary

Preview

Provides comprehensive summary of all activities and actions that have occurred against a policy, such as:

- Date sent
- Date flagged
- Reviewed by
- Message reconciliation

Can help fulfill regulatory compliance obligations and can help organizations better track the status and progress for unresolved policy violations



Communication compliance > Policies > Insider

Insider

Users with most policy matches

Last 30 days, updated 2:08 PM today

Display name	Matches
[redacted]	8
[redacted]	5
[redacted]	3
[redacted]	3

Age of pending items

Last 30 days, updated 2:08 PM today

Age	Items
0 - 7 days	2
7 - 14 days	13
14 - 21 days	4
21 - 28 days	8

Alerts

Last 30 days, updated 2:08 PM today

Alert	Severity	Detected on	Activity count

Alerts

Last 30 days, updated 2:08 PM today

Alert	Severity	Detected on	Activity count

Download review activity

Download a CSV file containing review activity for this policy, including when messages are resolved, tagged, escalated, and more. Note that it might take a few minutes depending on how much activity you're exporting.

Choose a date range

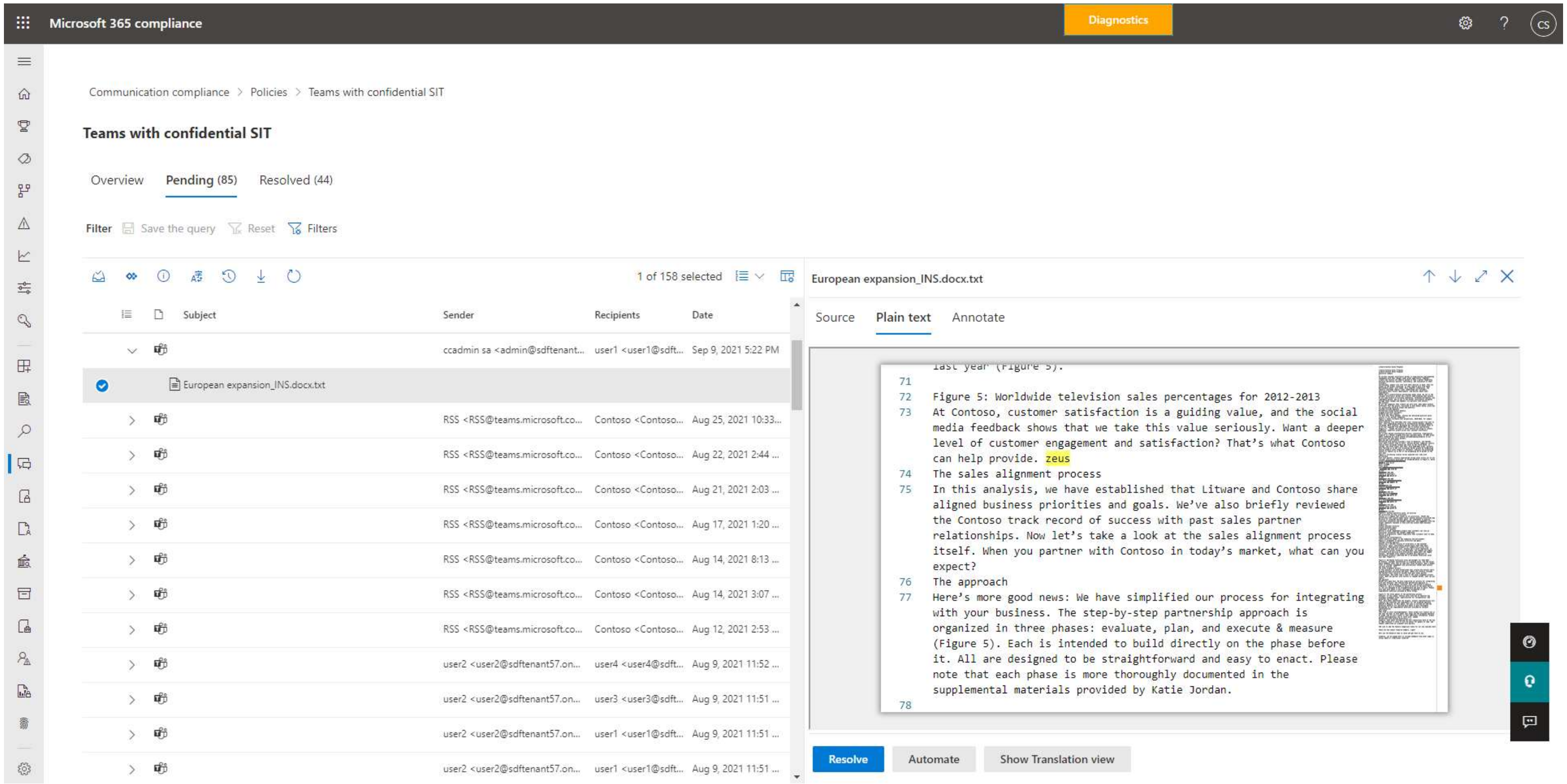
Start date: Nov 22, 2021

End date: Nov 29, 2021

Coming Soon

Deeper Microsoft Teams Integration

Analyze Team Modern Attachments



Communication compliance > Policies > Teams with confidential SIT

Teams with confidential SIT

Subject	Sender	Recipients	Date
	ccadmin sa <admin@sdftenant...	user1 <user1@sdft...	Sep 9, 2021 5:22 PM
European expansion_INS.docx.txt			
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 25, 2021 10:33...
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 22, 2021 2:44 ...
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 21, 2021 2:03 ...
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 17, 2021 1:20 ...
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 14, 2021 8:13 ...
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 14, 2021 3:07 ...
	RSS <RSS@teams.microsoft.co...	Contoso <Contoso...	Aug 12, 2021 2:53 ...
	user2 <user2@sdftenant57.on...	user4 <user4@sdft...	Aug 9, 2021 11:52 ...
	user2 <user2@sdftenant57.on...	user3 <user3@sdft...	Aug 9, 2021 11:51 ...
	user2 <user2@sdftenant57.on...	user1 <user1@sdft...	Aug 9, 2021 11:51 ...
	user2 <user2@sdftenant57.on...	user1 <user1@sdft...	Aug 9, 2021 11:51 ...

European expansion_INS.docx.txt

```
last year (Figure 5).

Figure 5: Worldwide television sales percentages for 2012-2013
At Contoso, customer satisfaction is a guiding value, and the social
media feedback shows that we take this value seriously. Want a deeper
level of customer engagement and satisfaction? That’s what Contoso
can help provide. zeus
The sales alignment process
In this analysis, we have established that Litware and Contoso share
aligned business priorities and goals. We’ve also briefly reviewed
the Contoso track record of success with past sales partner
relationships. Now let’s take a look at the sales alignment process
itself. When you partner with Contoso in today’s market, what can you
expect?
The approach
Here’s more good news: We have simplified our process for integrating
with your business. The step-by-step partnership approach is
organized in three phases: evaluate, plan, and execute & measure
(Figure 5). Each is intended to build directly on the phase before
it. All are designed to be straightforward and easy to enact. Please
note that each phase is more thoroughly documented in the
supplemental materials provided by Katie Jordan.
```

New Guides

- Interactive Guide: Interactive guide with step-by-step guidance on how to create policies, investigate policy violations, and escalate compliance issues for remediation.
- SIEM Integration Guide: Learn how to integrate Communication Compliance with SIEM solutions so that you can view Communication Compliance alerts in your SIEM.
- Financial Services Industry Playbook: This guide provides a set of guiding principles and best practice use cases for Communication Compliance to address regulatory compliance obligations.

Stay up to date

aka.ms/m365roadmap

Microsoft

Resources

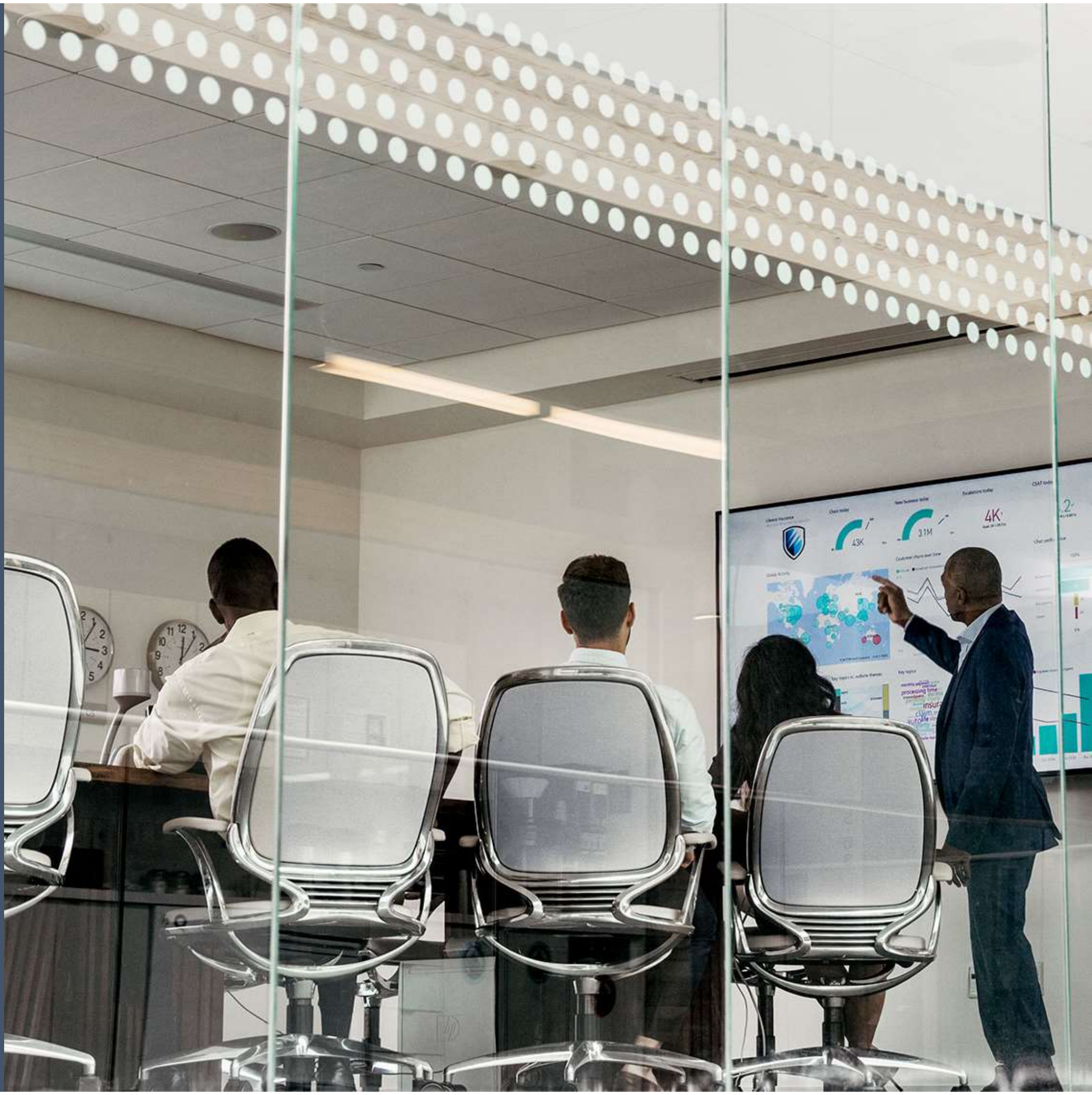
Resources

- OSS – https://aka.ms/mipc/oss
- Insider Risk Guide - https://aka.ms/insiderriskguide
- Insider Risk Blog - https://aka.ms/insiderriskblog
- Communication Compliance Guide - https://aka.ms/CommunicationCompliance
- Communication Compliance Ignite blog – https://aka.ms/ccignite2021

M365 SECURITY & COMPLIANCE
Customer Experience Engineering

Microsoft

Q & A



Microsoft

Thank you!

M365 SECURITY & COMPLIANCE
Customer Experience Engineering