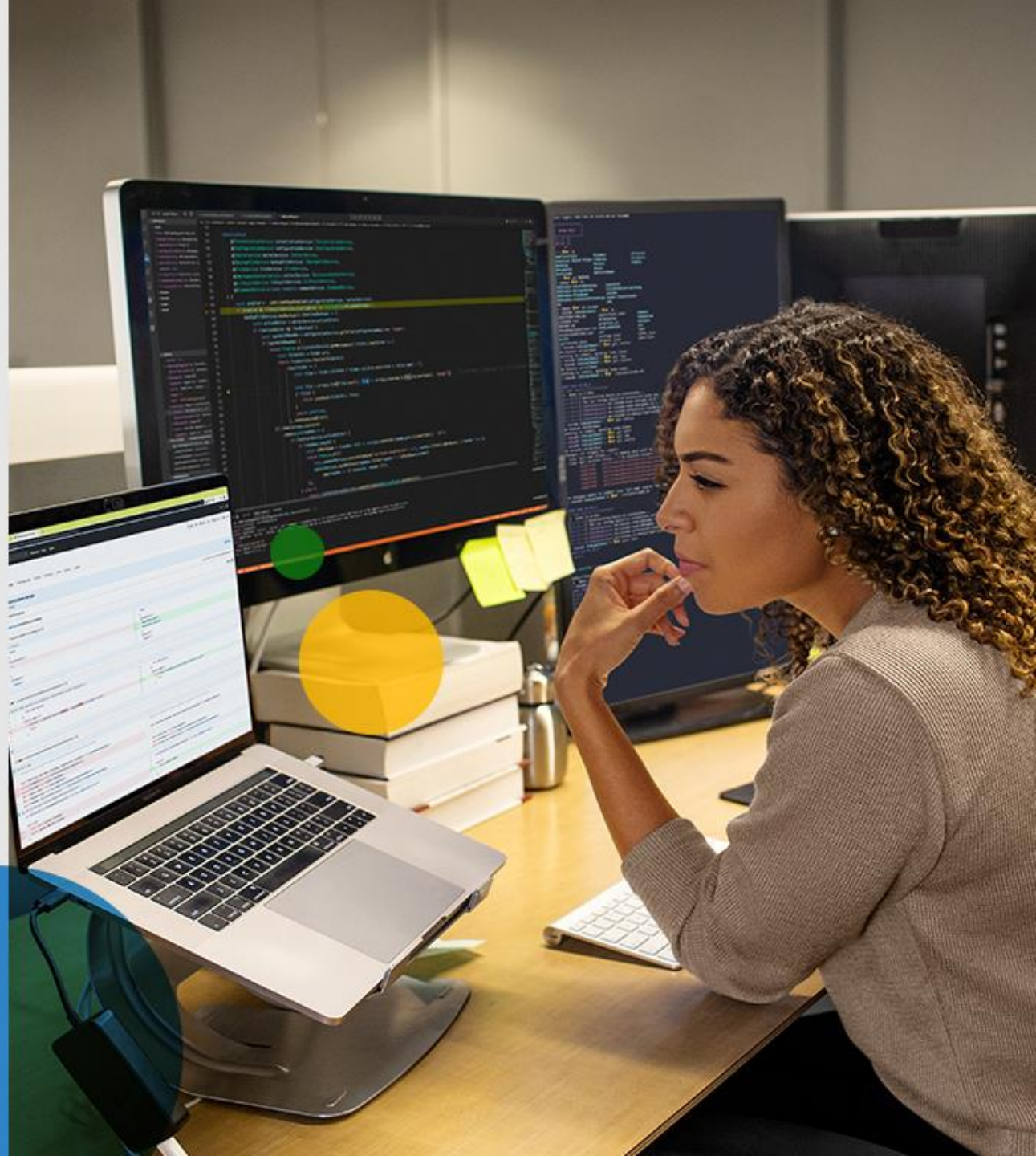
Microsoft Security

Security Tech Frontier Series: Strengthening Security, Compliance and Identity Management

9 – 10 June 2021



Agenda

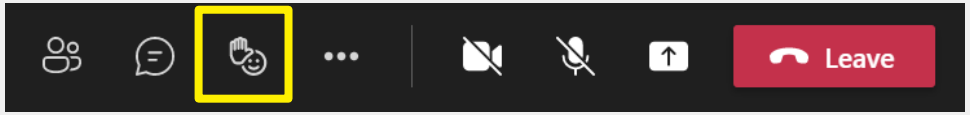
Day 1: 9 June 2021

Time (GMT +8)	Topic	Speaker
09:00am - 10:00am	**Security Hour:** Threat Hunting and SimuLand	Ashish Kumar
10:00am - 10:10am	*Break*	
10:10am - 11:10am	**Identity Hour:** Verifiable Credentials	Phil Whipps Matthijs Hoekstra
11:10am - 11:20am	*Break*	
11:20am - 12:20pm	**Compliance Hour:** Insider risks in today every digitized world - engineering update	Sravan Mera Sankalp Maraan Rohit Gupta

Tips to optimize today's experience

1) Questions & Answers

If you have any questions, send it through here at any time or raise a hand. Our team will answer them as soon as possible.



2) Switch off your camera

To optimize the bandwidth, please switch off your video camera on Teams.

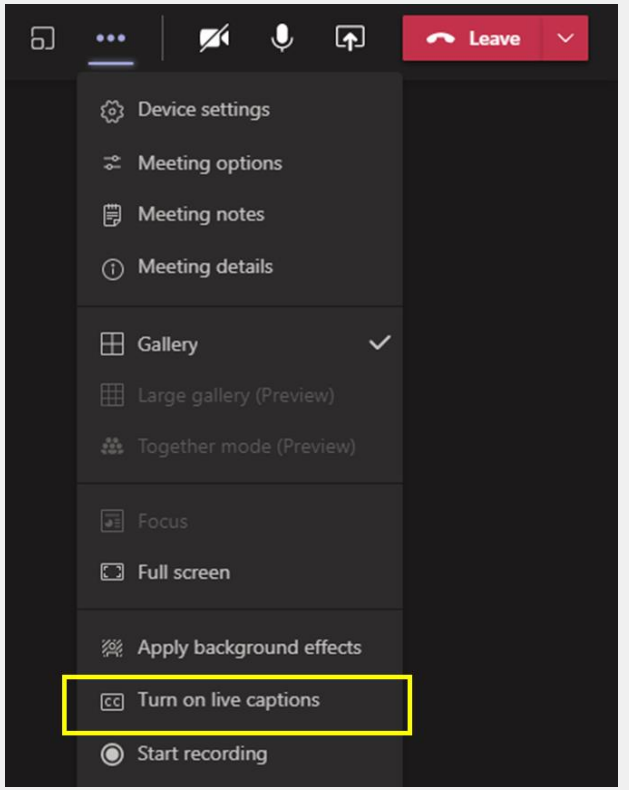
3) No recording

For privacy reasons, this session will not be recorded, and we will be putting everyone on mute. If you have a question or comment, please send it through the chat window.

4) Turn on live captioning

If you enable this on Teams, the live captions will appear at the bottom of the video.

Here's where to find the Live Captioning feature:



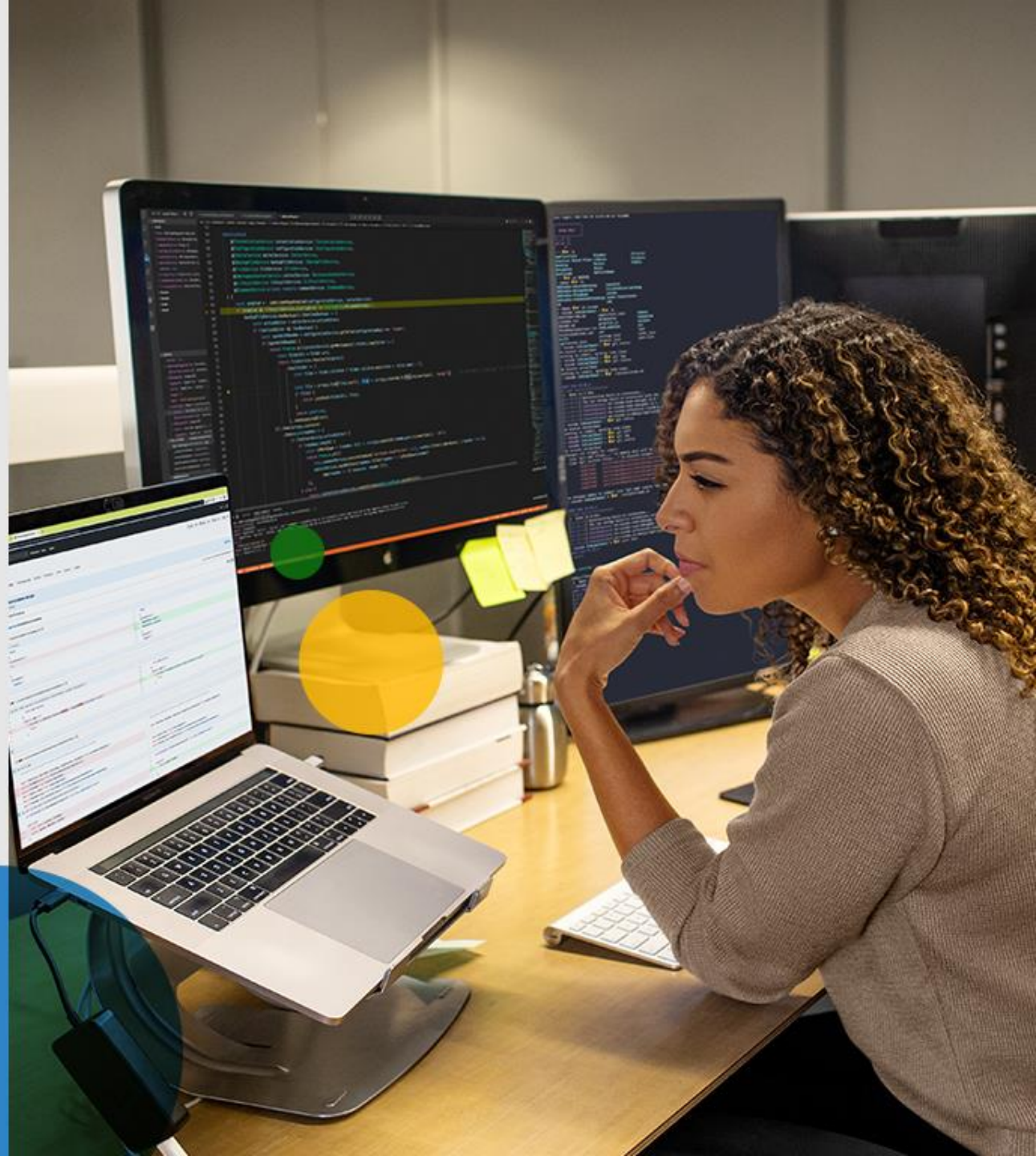
© Microsoft Corporation

Microsoft Security

Security Tech Frontier Series

Security Hour: Threat Hunting and SimuLand

Ashish Kumar



Threat Hunting & Cyberbattle Sim

Ashish K Adhikari
Principal Program Manager, M365 S+C Engineering

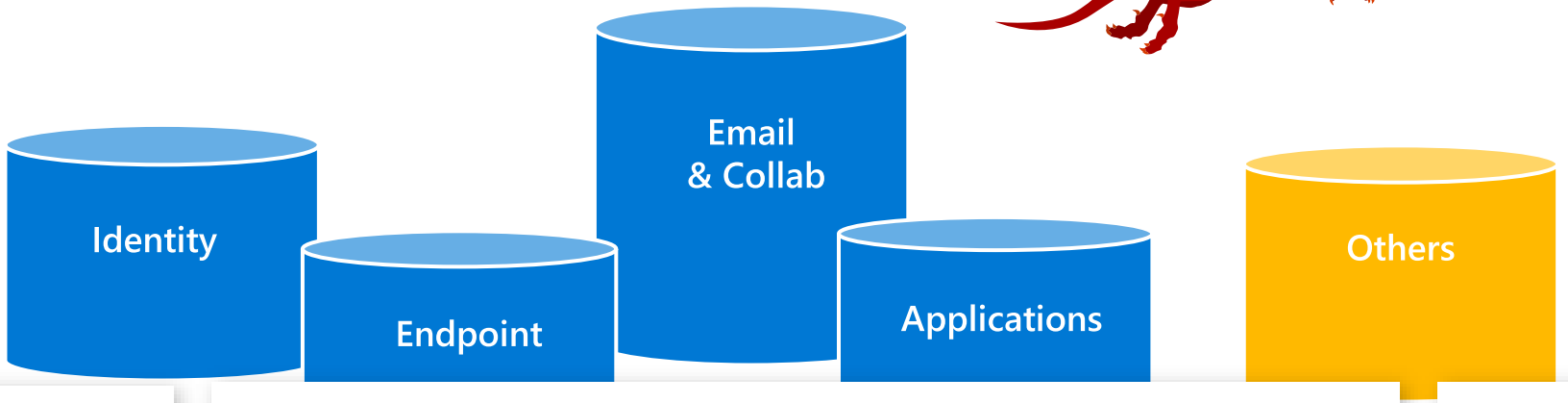
Agenda

- Attacker win probability
- Threat Hunting – what does it means ?
  - MITRE framework
- Running Marathon – needs practice
  - Simuland
  - CyberBattle SIM

Attacker Win probability

Defender Silos make chasing them difficult (even in single SIEM)

Attackers traverse rapidly across the enterprise



MAPPING CHALLENGES

Tools Pivot on Different Attributes

- Network IP address
- Computer Name
- Documents
- Device ID
- Email
- Etc.

DIFFERENT ALERTING APPROACHES

Identity ⟷ Endpoint

Reports only quality alerts Vendors

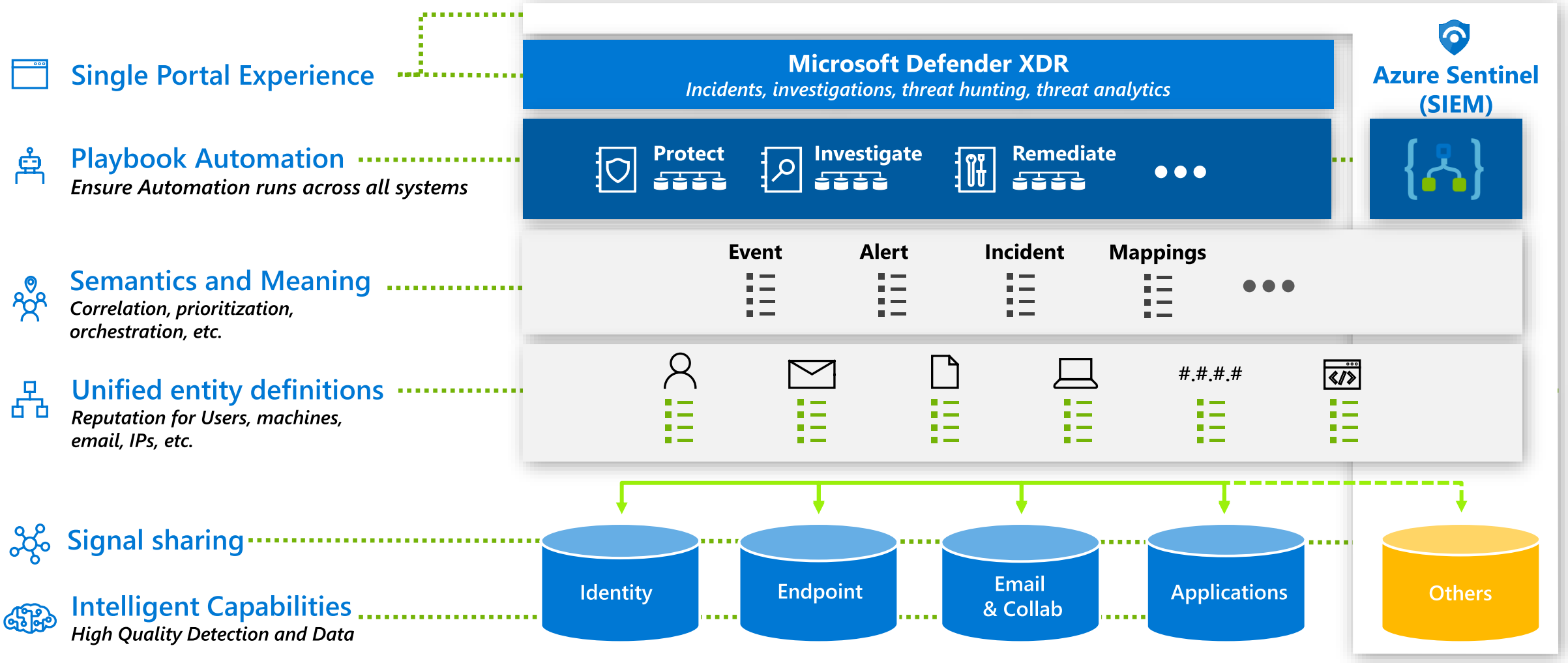
Verbose/ Detailed alert reporting

...

Silos must be integrated to provide high quality alerts and correlation

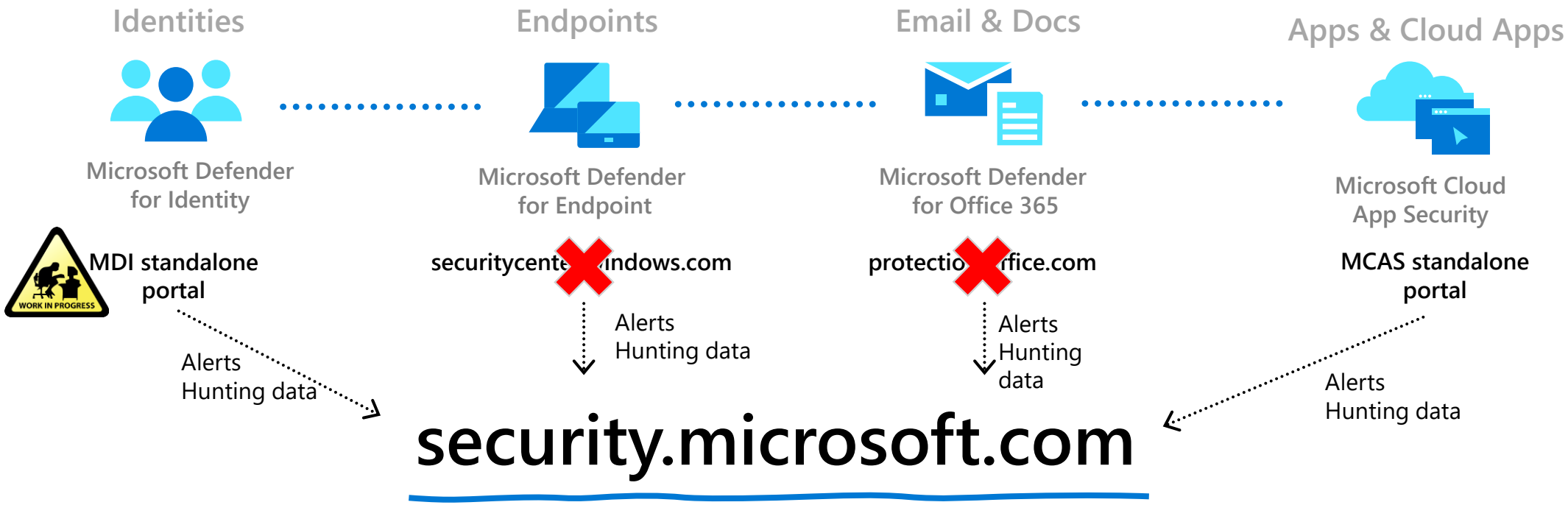
Converging Tools & Data

Engineering a single seamless system with automation



The unified Microsoft 365 Defender portal:

A journey from multiple to a single portal

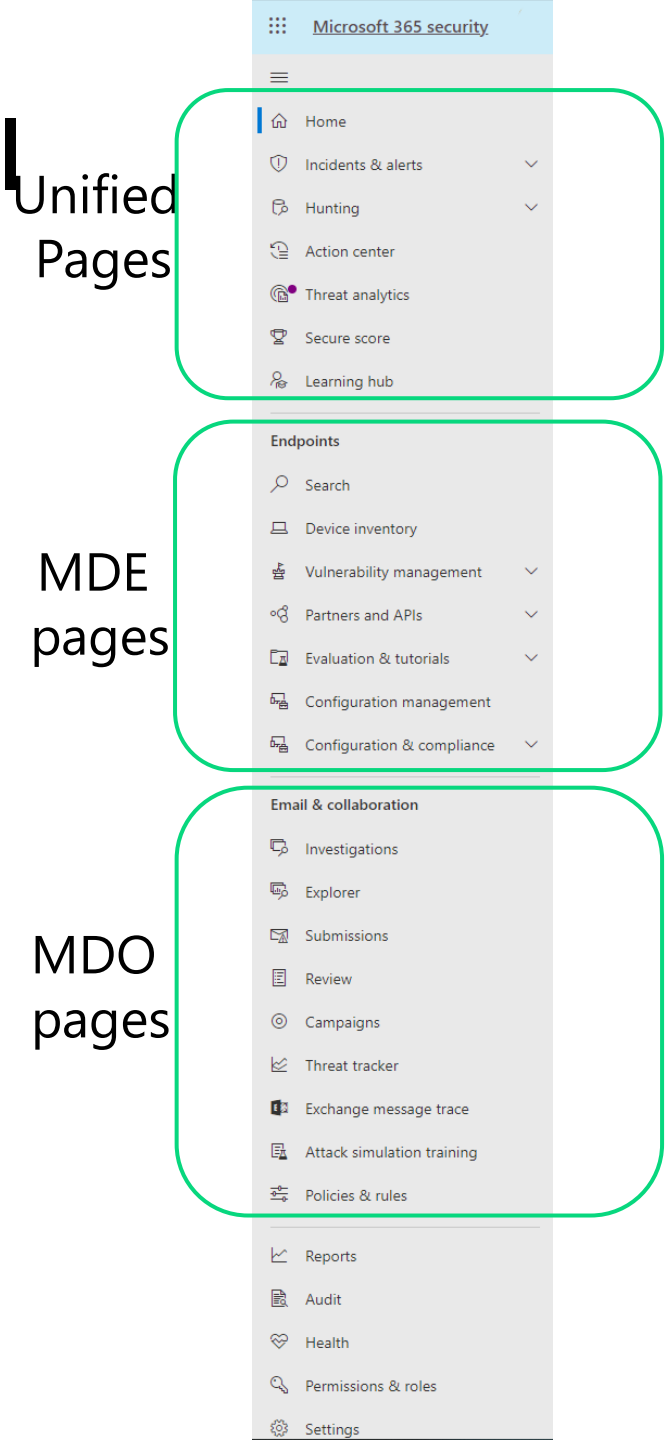


Journey to Converged portal

New Unified Experiences:
- Unified alerts queue
- Unified alerts page
- Email entity page
- Hunting

Not changed:
- Investigations (queue)
- Explorer
- Submissions
- Review
- Campaigns
- Policies

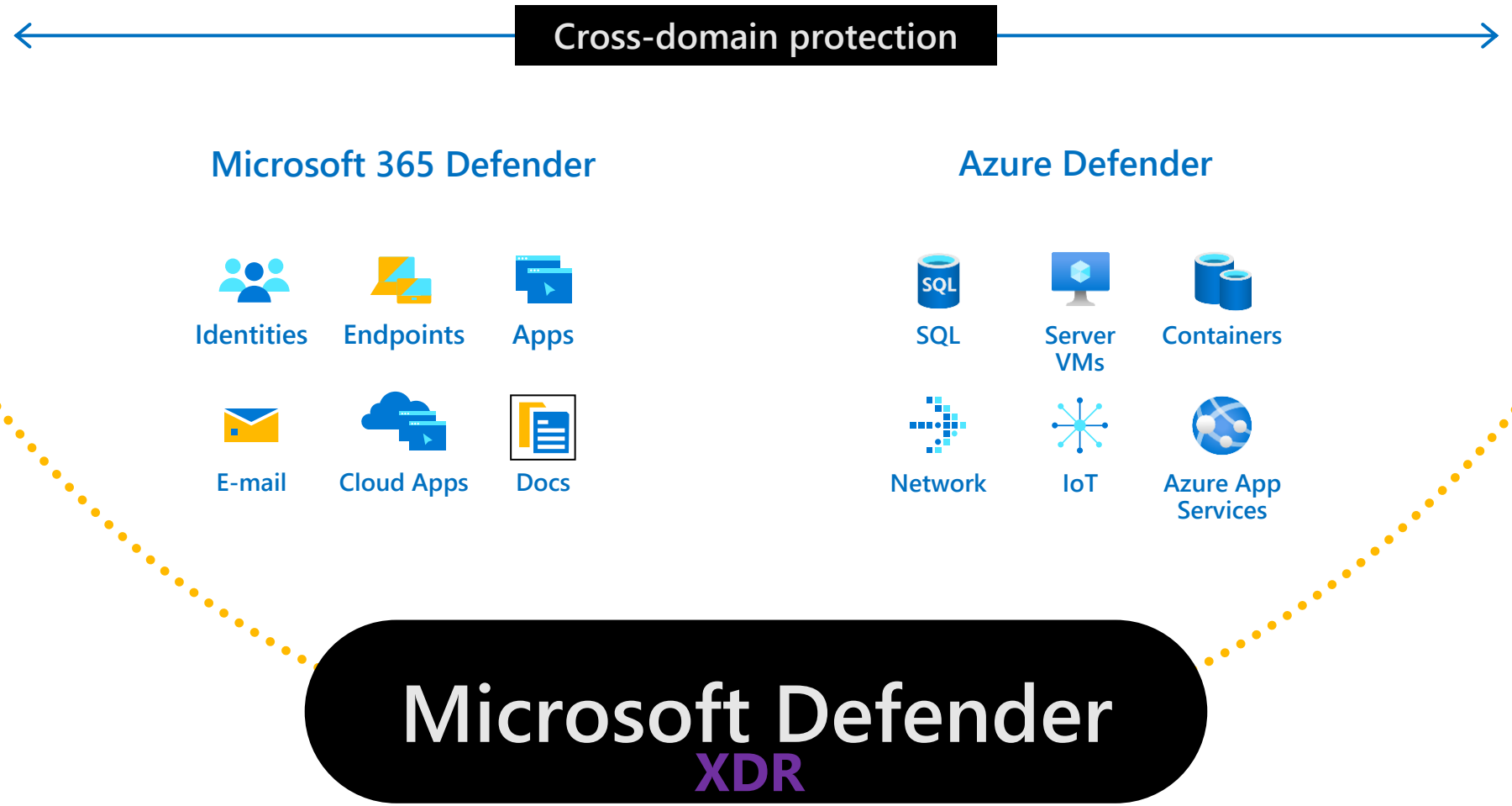
Aggregated:
- Reports
- Settings



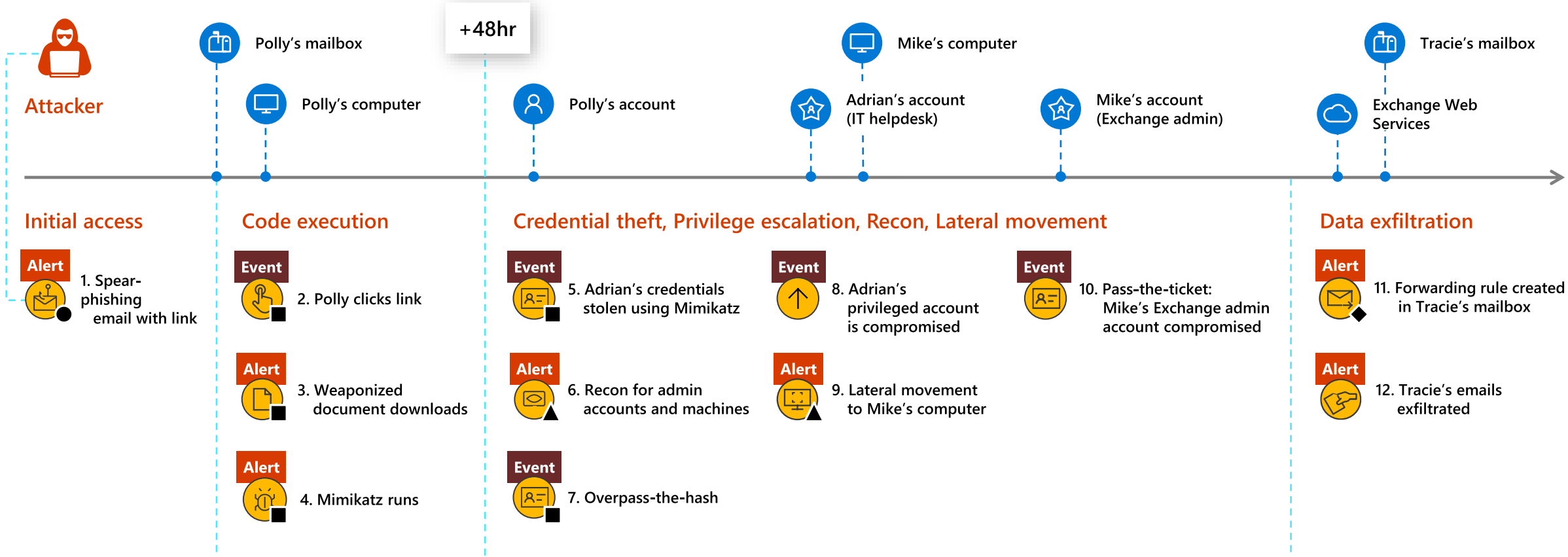
Microsoft Confidential

Unified Security Portal

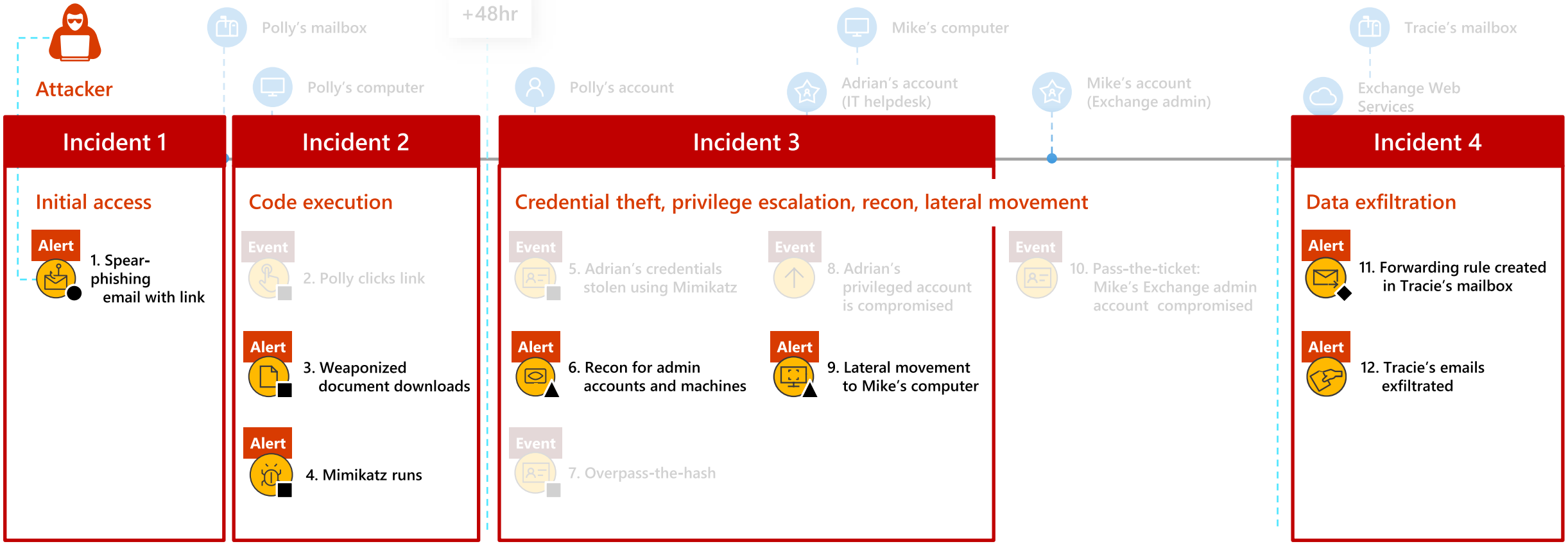
https://security.microsoft.com/


Cross-domain protection
Microsoft 365 Defender
Identities
Endpoints
Apps
E-mail
Cloud Apps
Docs
Azure Defender
SQL
Server VMs
Containers
Network
IoT
Azure App Services
Microsoft Defender
XDR

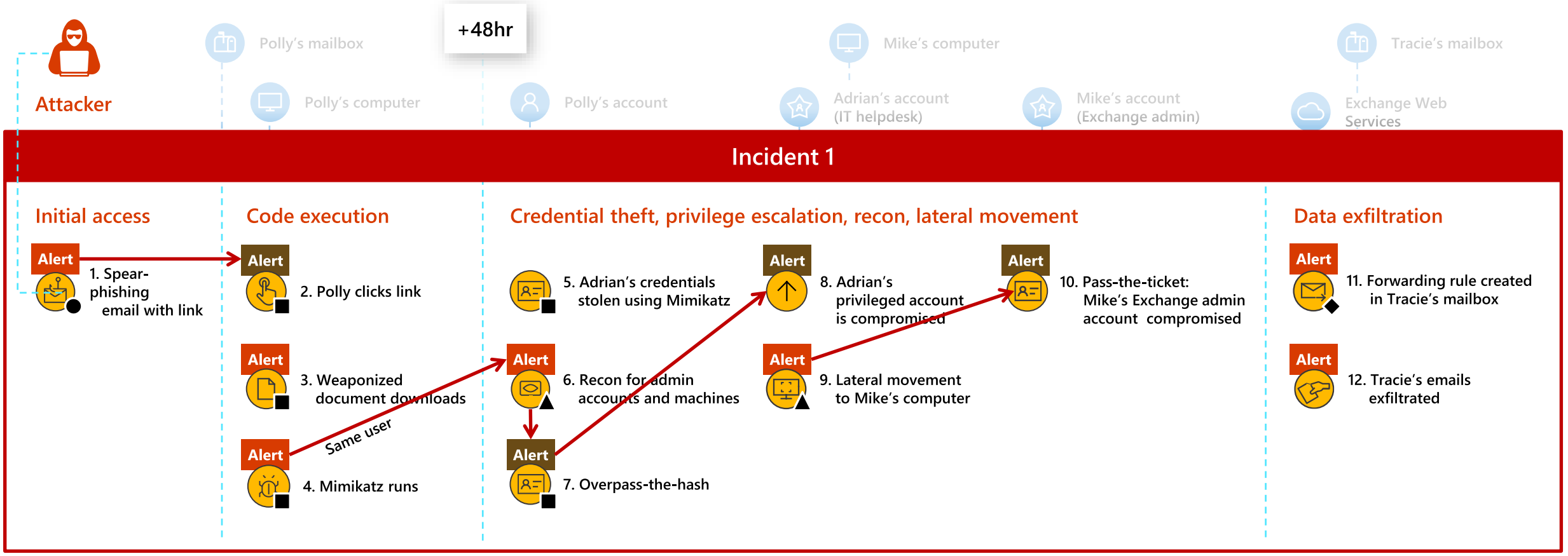
Why is it challenging



Why is it challenging – generic tools logic

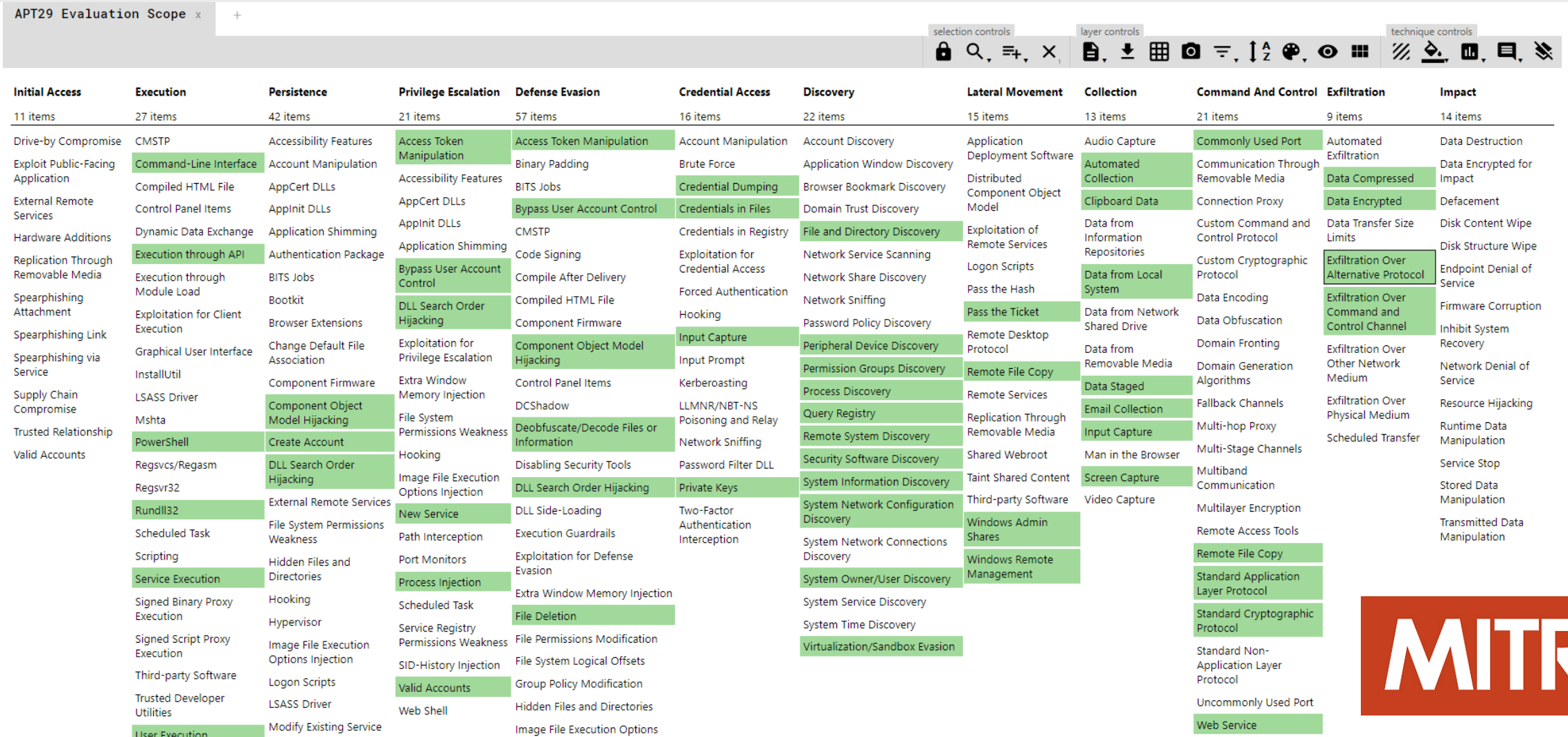


Microsoft Defender XDR Approach – with proper logic



Case study: MITRE APT29

Wide and complex attack across the kill chain



- **Microsoft Threat Experts**

Microsoft Threat Experts

Microsoft brings deep knowledge and proactive threat hunting to your Security Operations Center

Threat monitoring and analysis

Hunter-trained artificial intelligence

Proactive Notification service

Full context of breach

Experts on demand

Microsoft Threat Experts

Targeted attack notifications

Threat experts provide special insights and analysis that help ensure that the most critical threats are identified and responded to quickly and accurately.

Experts on demand

Threat experts from Microsoft provide technical consultation on relevant detections and adversaries.

Microsoft

Microsoft Threat Experts

Microsoft brings deep knowledge and proactive hunting to the Security Operations Center

THREAT MONITORING AND ANALYSIS

Reduce attacker dwell time and risk to business

HUNTER-TRAINED ARTIFICIAL INTELLIGENCE

Discover and prioritize attacks both known and unknown

PROACTIVE NOTIFICATION SERVICE

Expert hunters look deeper to expose human adversaries and advanced threats

FULL CONTEXT OF BREACH

Improve SOC response with specific info about scope and methods of entry

EXPERTS ON DEMAND

Partner with world-class security experts to better understand threats and alerts

Alerts > **Detection of activity linked to adversary with s...**

Microsoft Threat Experts | BARIUM | Detection of activity linked to adversary with supply chain attacks

This alert is part of incident (4)

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Execution
Detection source: Microsoft Threat Experts

Alert context

barbaram-pc
mtpdemos\barbara.moreland

First activity: 10.28.2019 | 23:02:28
Last activity: 10.28.2019 | 23:03:13

Description

Executive summary

This alert provides additional context for an alert you have received, 'Pynamer' malware was detected . We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action here. While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

Timeline of observed events

Date/Time	Notes
2019-10-28T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-10-28T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-10-28T21:19:52.563Z	Network connection to IP address 131.107.147.82

Impacted machines

Machine Id	Notes
c5fab76bb18b987a79bf53965aa39d18ff0ae185	Impacted machine 1

Recommended actions

Recommendation summary

1. Fully investigate the machine in questio
2. Practice the principle of least-privilege a
   Restricting local administrative privileges
3. Enforce strong, randomized local admini
4. If you have any questions about this aler
   right of the portal and select 'Consult a t
5. If you need immediate help from Micros
6. Examine the Indicators of Compromise (
   investigation.

Indicators of Compromise

IOC
Install (2).exe [explore]
InstallConfig.exe [explore]
InstallLauncher.exe [explore]
881ba9b12040d4576b5e09de73e5eb33de2e [explore]
ab16cd1b09e5157791a568456a12659aae92 [explore]
131.107.147.82 [explore]

Microsoft Threat Experts - Trial

Your Experts on Demand trial version expires in 84 days from your Microsoft Threat Experts enrolment. Contact your Microsoft representative to get a full subscription.

Learn more about Microsoft Threat Experts – Experts on Demand

Consult a threat expert

Get Microsoft Threat Experts advice and insights about suspicious activities in your organization.

Ensure that the portal page for the alert or machine in question is in view while providing information for this inquiry.

Note: This and other relevant information will be shared with Microsoft Threat Experts to enable the best response to your inquiry.

Inquiry topic *

https://securitycenter.windows.com/alert/da637081759681505242_958338753

Can you help me understand if I still have this threat in my environment and why I may have been targeted by this adversary?

Email *

Enter the email address you'd like Microsoft Threat Experts to send their reply

secops@MTPDemos.net

Submit

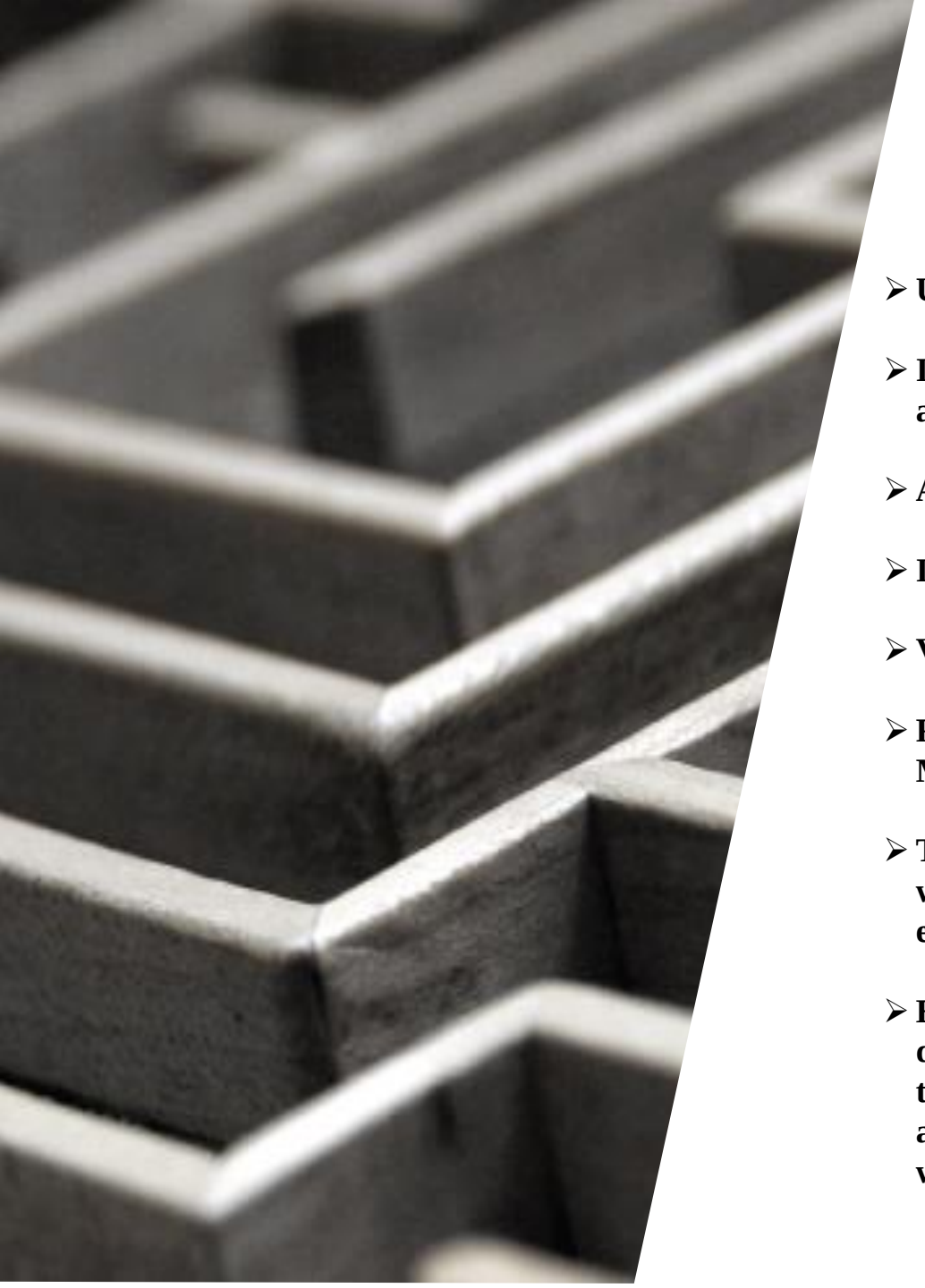
Privacy statement.

What is SimuLand ?

- **Open-source project which aims to help security teams reproduce known attack scenarios - and test just how good Microsoft's core security products are.**

- **Verify the effectiveness of related Microsoft 365 Defender, Azure Defender, and Azure Sentinel detections.**

.



FEATURES OF SIMULAND

- **Understand the underlying behavior and functionality of adverse trading techniques.**
- **Identify attacker pathways and mitigations by documenting preconditions for each attacker action.**
- **Accelerate the design and deployment of threat research lab environments.**
- **Identify, document and share relevant data sources to model and detect adverse actions.**
- **Validate and tune detection capabilities.**
- **Replicate different types of environments (hybrid, cloud) and includes Azure Resource Manager (ARM) templates.**
- **The structure of the project is very simple and broken down in a modular way so that we can re-use and test a few combinations of attacker actions with different lab environment designs.**
- **Every simulation plan provided through this project is research-based and broken down into attacker actions mapped to the MITRE ATT&CK framework. The goal of the simulate and detect component is to also summarize the main steps used by a threat actor to accomplish a specific object and allow security researchers to get familiarized with the attacker behavior at a high level.**

CURRENT SCENARIOS

- **Currently, the only lab environment available for deployment allows researchers to test and improve their defenses against Golden SAML attacks that allow threat actors to forge authentication to cloud apps.**

- **Currently there is only one lab released by Microsoft.**

FUTURE PLANS

Future improvements to the project include:

- **A data model to document the simulation steps in a more organized and standardized way.**
- **A CI/CD pipeline with Azure DevOps to deploy and maintain infrastructure.**
- **Automation of attack actions in the cloud via Azure Functions.**
- **Capabilities to export and share telemetry generated with the InfoSec community.**
- **Microsoft Defender evaluation labs integration.**

Cyberbattle sim

An experimentation and research platform to investigate the interaction of automated agents in an abstract simulated network environments.

What is it ?

- By open sourcing it we hope to encourage the research community to investigate how cyber-agents interact and evolve in such network environments.
- The simulation we provide is admittedly simplistic to avoid misuse.
- Focus is on building preventing AI technologies

Environment

State = network
Single-agent
Partially observable
Deterministic
Static
Discrete
Post-breach

Action space

Local attack
Remote attack
Authenticated connection

Observation space

Discovered nodes
Owned nodes
Discovered credentials
Escalation levels
Available attacks

Reward

Intrinsic node value
(SQL server > test machine)

How simulation works ?

Let us go through a toy example and introduce how simulation works using RL terminology.

Our network environment is given by a directed annotated graph where nodes represent computers and edges represent knowledge of other nodes or communication taking place between nodes.

There is a **single agent**: the attacker.

Initially, one node is infected (post-breach assumption)

Its **goal** is to maximize reward by discovering and 'owning' nodes in the network.

The environment is **partially observable**: the agent does not get to see all the nodes and edges of the network graph in advance.

Instead the attacker takes actions to gradually observe the environment. There are **three kinds of actions** offering a mix of exploitation and exploration capabilities to the agent:

• Perform a local attack,

• Perform a remote attack,

• Connect to other nodes.

The **reward** is a float represents the intrinsic value of a node (e.g., a SQL server has greater value than a test machine).

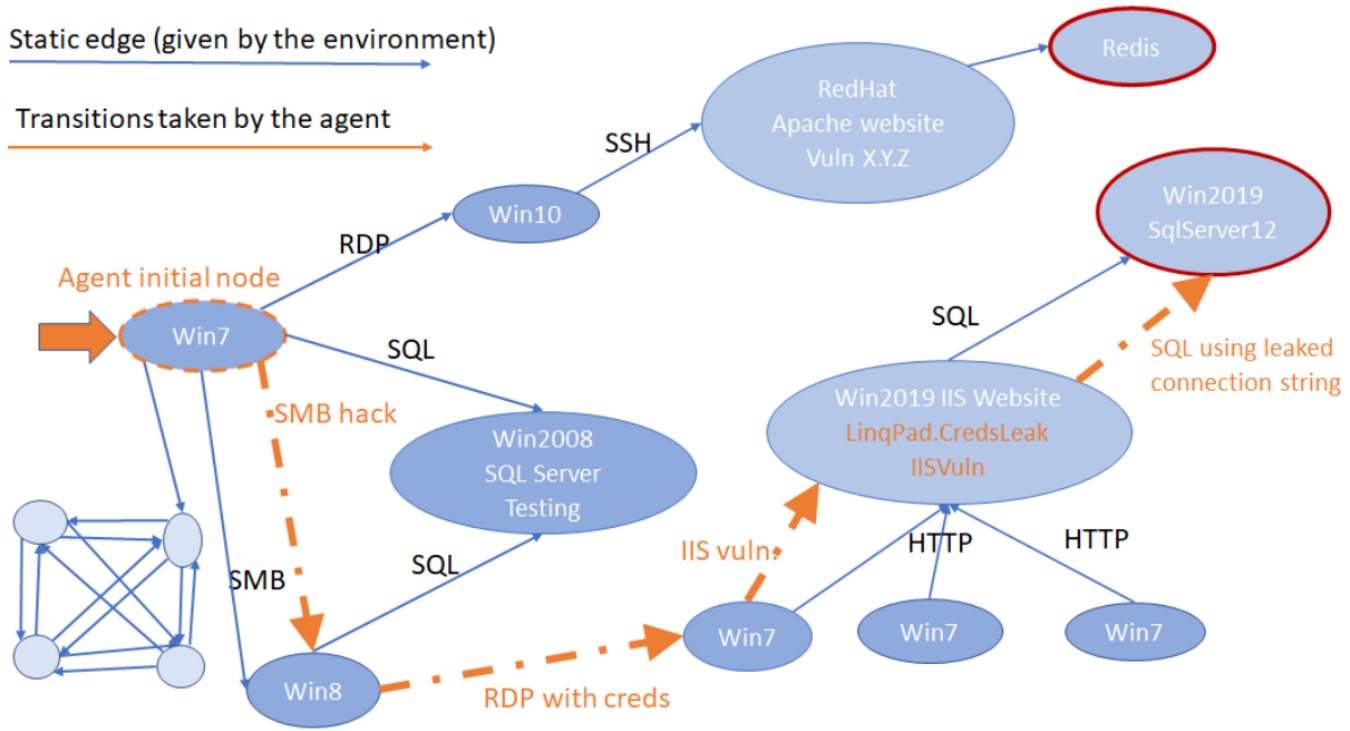
The attacker breaches into the network from the Win7 node on the left pointed by the fat orange arrow,

• Then proceeds with a lateral move to the Win8 node by exploiting a vulnerability in SMB,

• Then uses some cached credential to log into a Win7 machine,

• Exploits an IIS remote vulnerability to own the IIS server,

• Leaked connection strings to get to the SQL DB.



Vulnerability outcomes

- Each vulnerability has a pre-defined outcome which may include:
- * A leaked set of credentials
- * A leaked reference to another node in the network
- * Leaked information about a node
- * Ownership to a node
- * Privilege escalation on the node.
- Example of remote vulnerabilities include:
- *A SharePoint site exposing ssh credentials (but not necessarily the ID of the remote machine);
- *An ssh vulnerability granting access to the machine;
- *A github project leaking credentials in commit history;
- *A SharePoint site with file containing SAS token to storage account;
- Examples of *local* vulnerabilities:
- *Extracting authentication token or credentials from a system cache;
- *Escalating to SYSTEM privileges;
- *Escalating to Administrator privileges.

- Once we set up the CyberBattleSim. There are various activities for us to do. All of them are present in the Jupyter notebooks. They are →

- 'Capture The Flag' toy environment notebooks:
  - Random agent
  - Interactive session for a human player
  - Interactive session - fully solved
- Chain environment notebooks:
  - Random agent
- Other environments:
  - Interactive session with a randomly generated environment
  - Random agent playing on randomly generated networks

- Lets see the “Toy example” in capture the flag.

Thanks for being part of our journey!

Threat Hunting & Cyberbattle Sim

Ashish K Adhikari
Principal Program Manager, M365 S+C Engineering

We’re having a short break.

Next session starts at 10.10am (GMT+8)

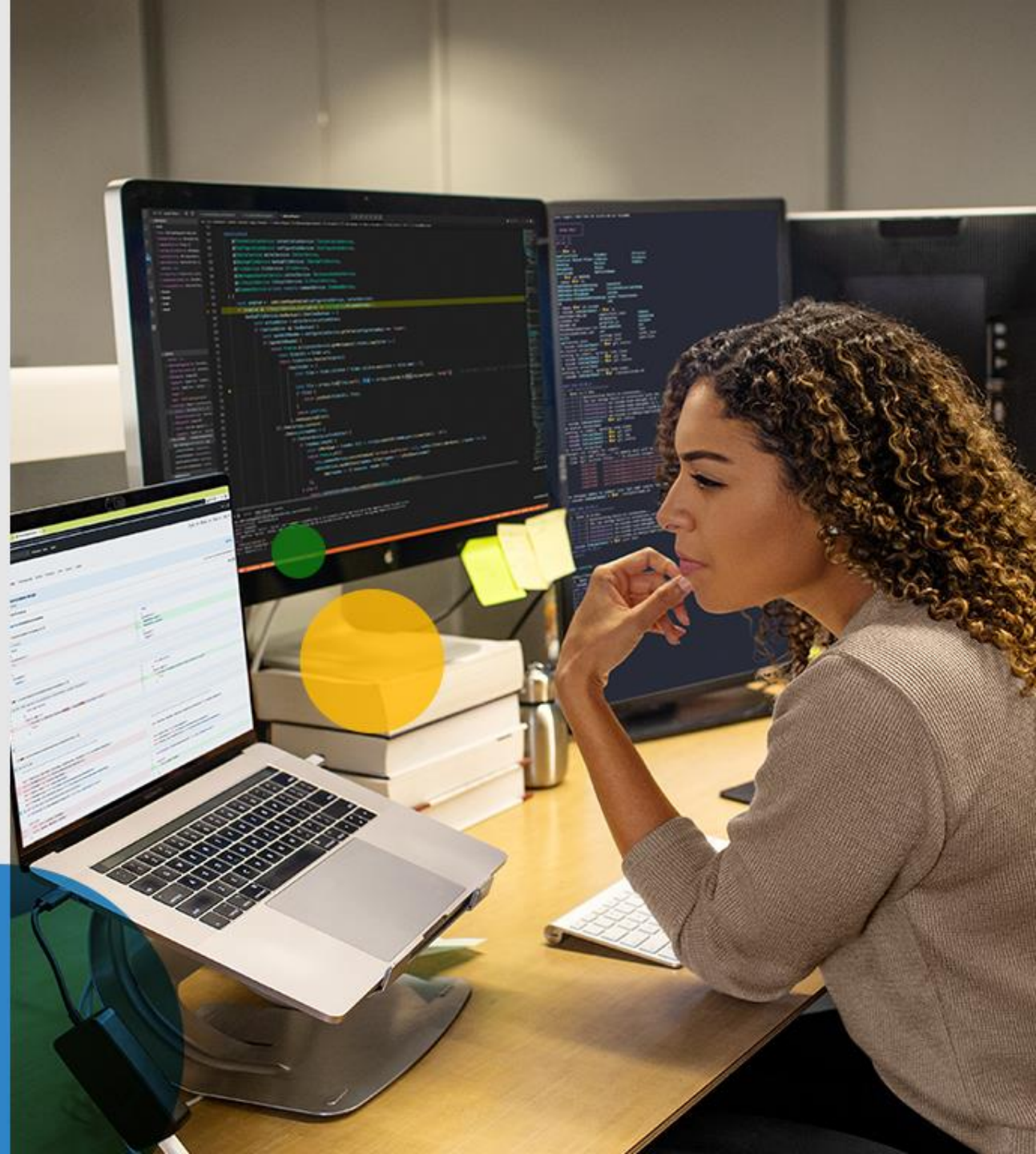
In the meantime, speakers will be answering questions in the chat window, so ask away!

Microsoft Security

Security Tech Frontier Series

Identity Hour: Verifiable Credentials

Phil Whipps
Matthijs Hoekstra



Microsoft Security

Azure AD Verifiable Credentials

- Verify once, use everywhere

Microsoft Security

92%

of organizations perform identity verification today

Source Microsoft, survey of 3000 US-based companies, greater than 500 users

Onboarding for employees, contractors, customers

Access to high-value apps and resources

Self-service account recovery

82% of organizations wish there was a better way

More protection against breaches
Credentials verified by reliable parties
Meeting regulatory requirements by default

Safer

No custom integration
No need to store users PII
No wait times for id verification

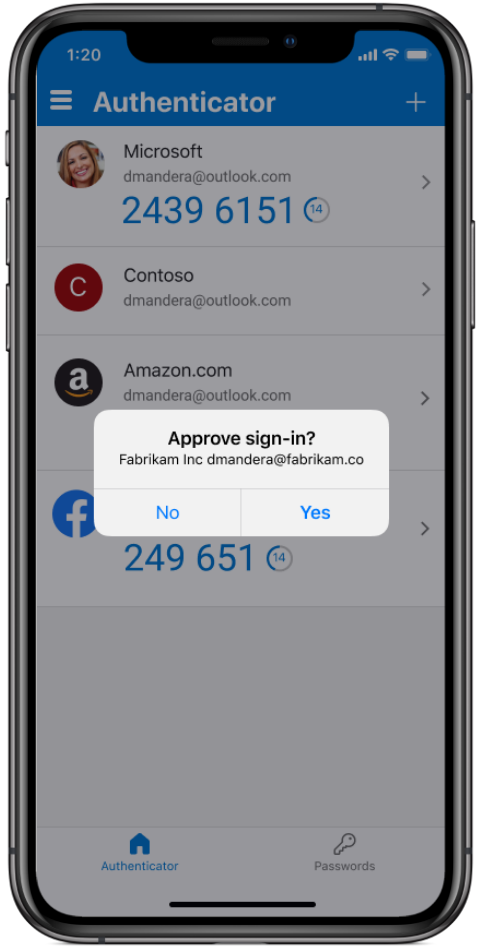
Faster

Lower cost
As easy using digital cards
Verify once, use everywhere

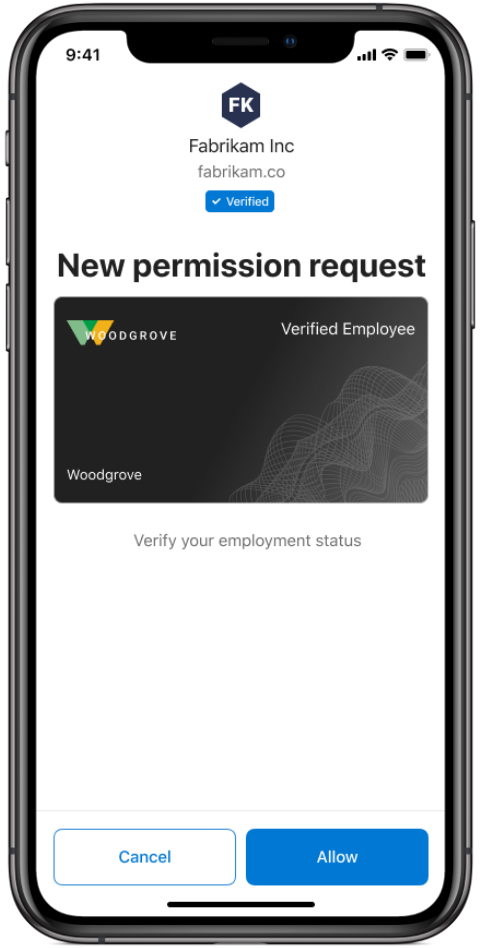
Easier

Demonstration:
ID verification based on open standards

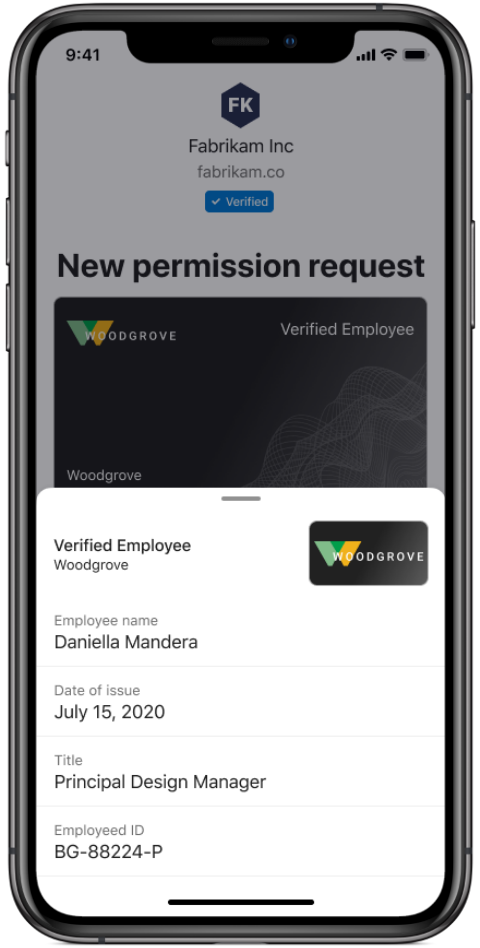
Azure AD verifiable credentials - a better way to verify



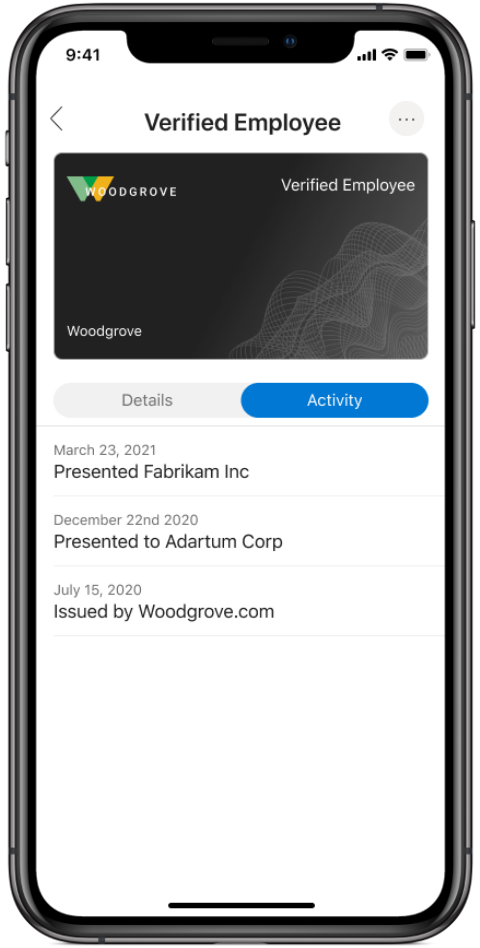
easy to use and secure



verifiable

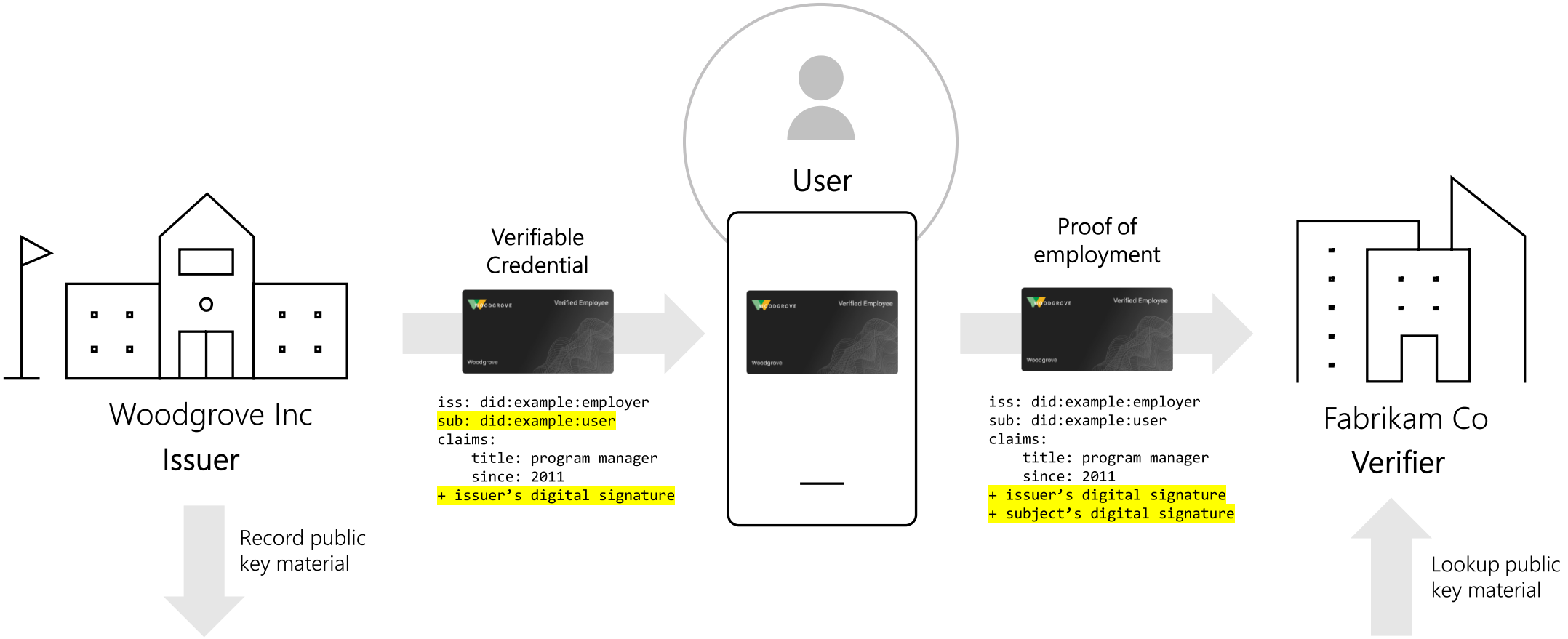


transparent



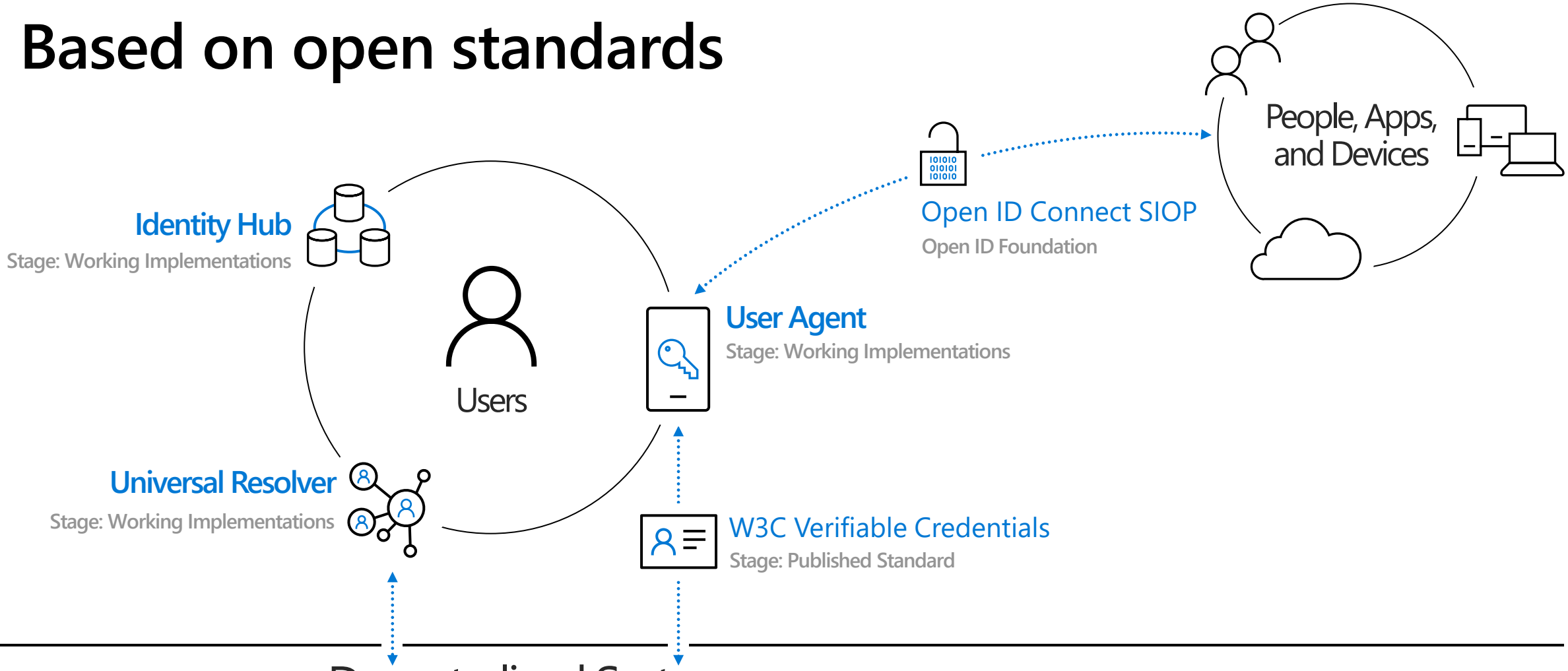
convenient

How does this work?

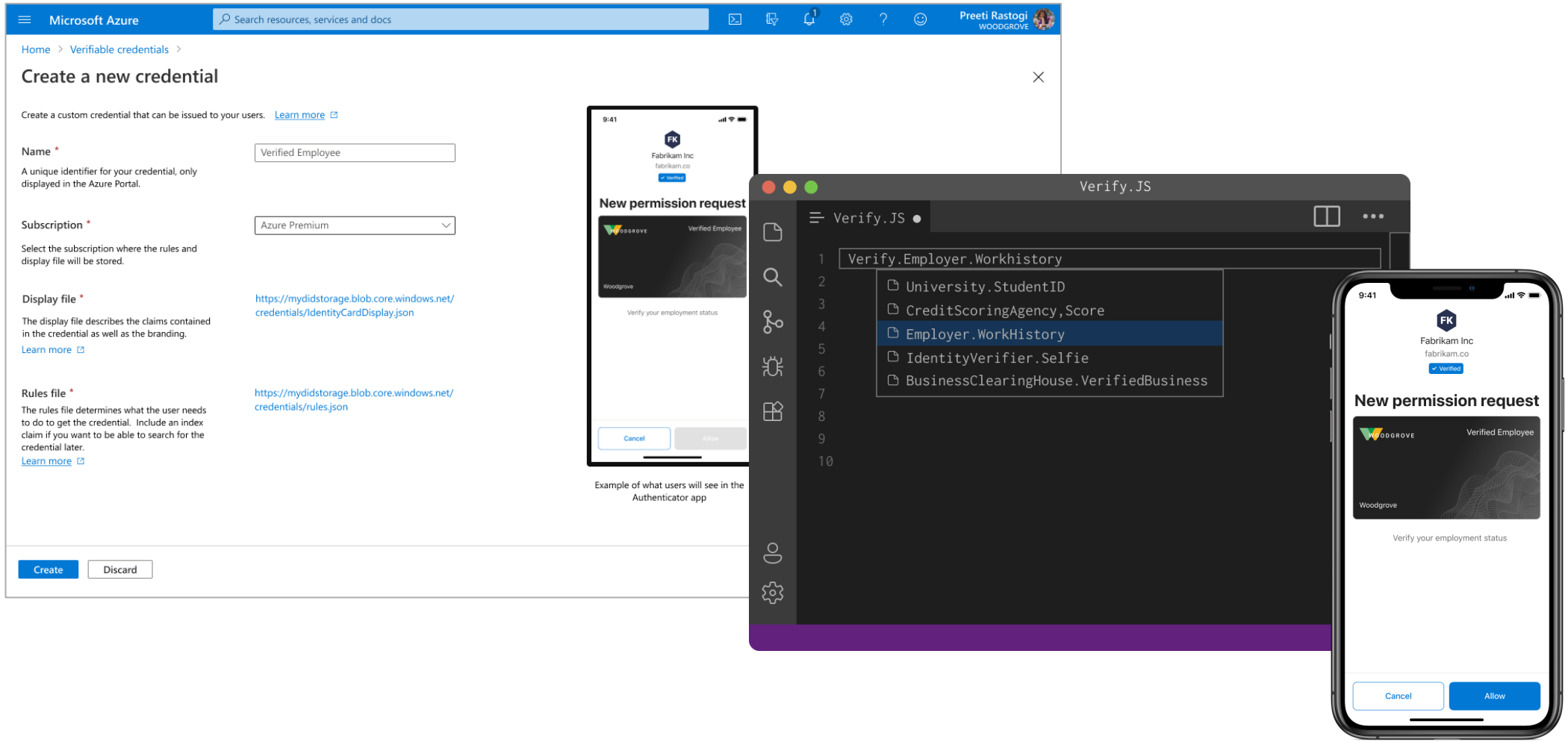


Microsoft

Based on open standards



Decentralized Identity Platform by Microsoft



Issuer interface
(Azure AD)

Developer tools
(SDK + API)

End user wallet
(Microsoft Authenticator)

Accelerate with trusted technology partners

In partnership with Identity verification leaders

Acuant

Au10tix

Jumio

Idemia

Lexis Nexis

Onfido

Socure

VU Security

Accelerate adoption with partner solutions

AffinitiQuest/ Avaleris

Condatis

192 Countries

6000 Identification documents

1000's Organizational attributes

Millions Individual ID attributes

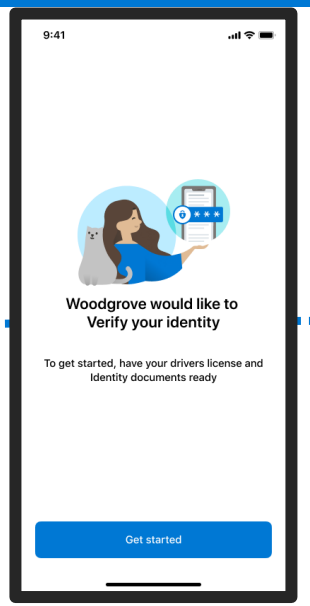
Decades of experience to go from idea to implementation in hours

Key scenarios

- Onboard
- Access
- Recover

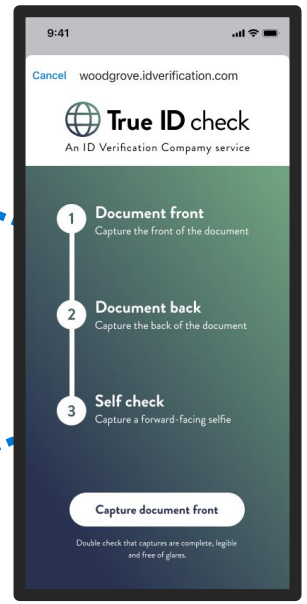
Onboard new employees, partners and customers

Start

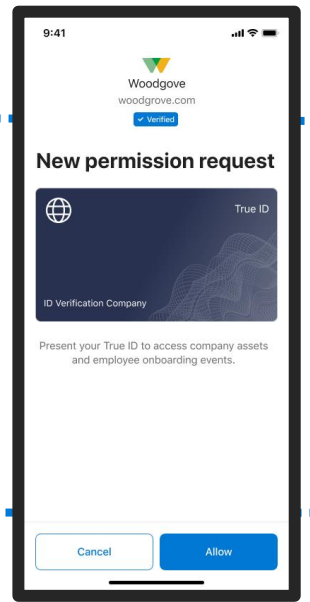


Invitation
User is invited to onboard using employer website

Request
Verify just-in-time



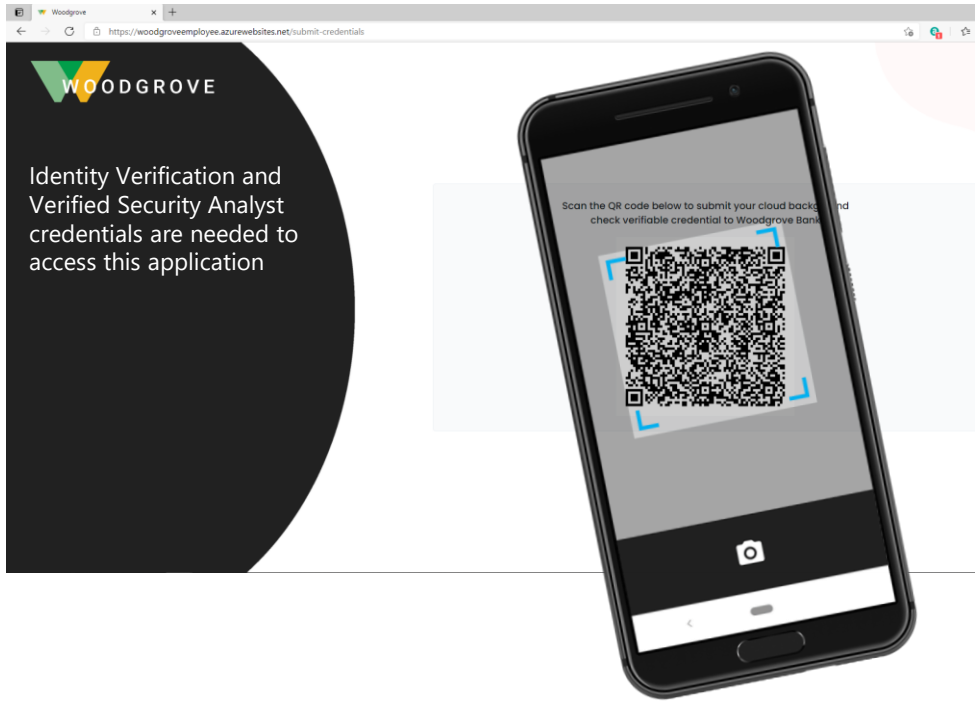
Upload
Scan docs and take selfie

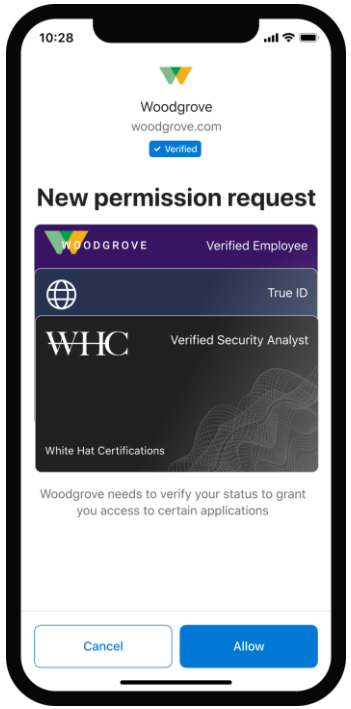


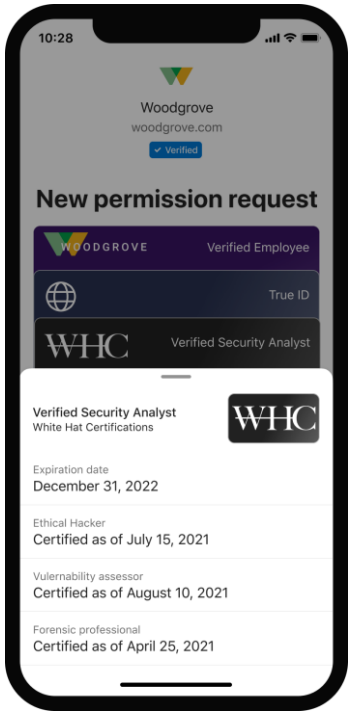
Issuance
Verification company issues a credential

Presentation
User presents verified identity to employer

Secure access to applications







Start

Sign in

Presentation

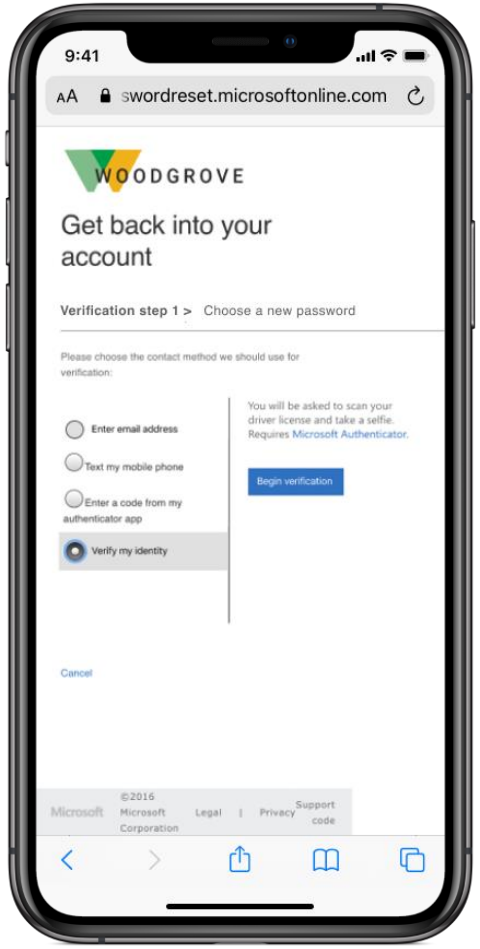
User shares the requested verifiable credentials

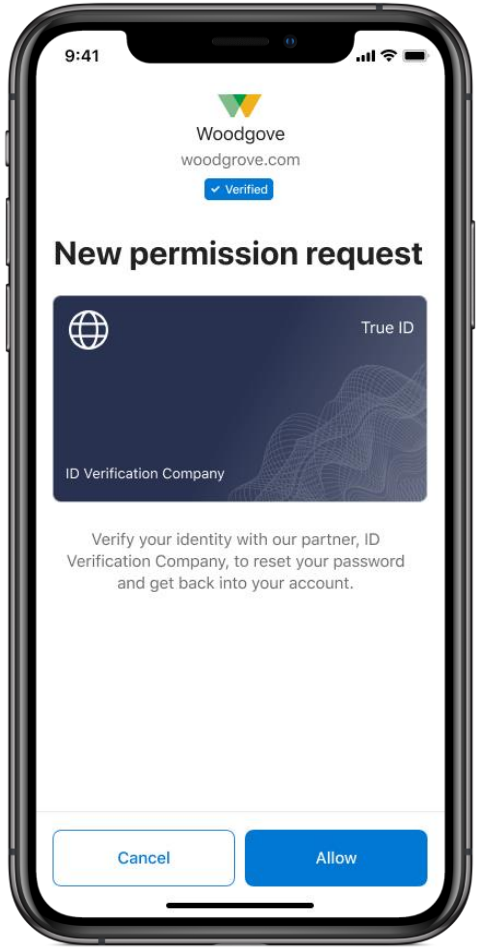
Detailed view

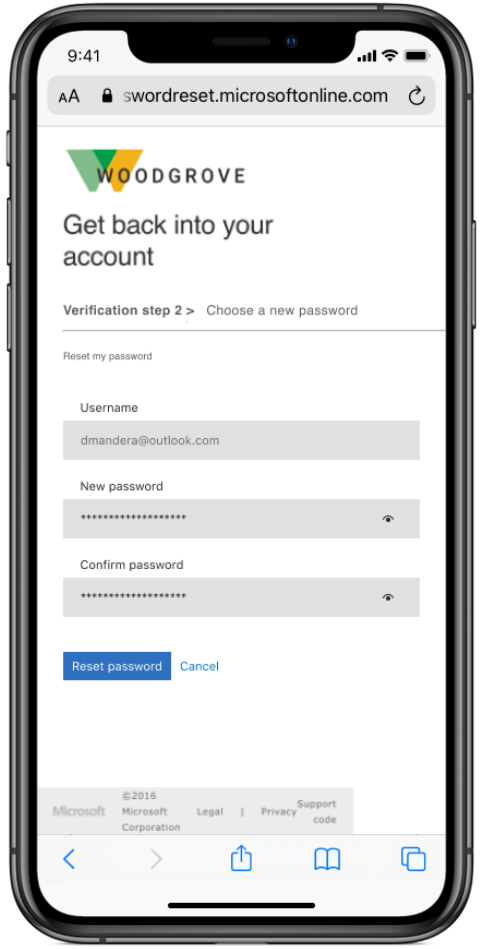
User confirms which claims are being shared

Recovery

Reduce support phone calls and security questions with a simpler, more secure process to verify identity.







Trustworthy, faster, cheaper way to verify

Onboard employees, partners, customers

Trustworthy self-service enrollment and faster onboarding by digitally validating information with industry leading ID verification providers.

Access to high-value apps and resources

Quickly verify credentials and get access to sensitive resources that have advanced security requirements

Self-service account recovery

Reduce support phone calls and security questions with a simpler, more secure process to verify identity.

Customer stories

Keio
University

National
Health Service

Government
of Flanders

and many more...

Resources

http://identity.foundation
Industry working group for all things Decentralized ID (DID)

http://aka.ms/didwhitepaper
White paper by Microsoft: approach for DID + Verifiable Credentials

http://aka.ms/didexplained
Quick overview

https://youtu.be/Whc9Im-U0Wg
Overview for developers: scenario walk-through and how-to

http://aka.ms/didfordevs
Developer documentation

http://aka.ms/azureadblog/did
Blogs (including scale and performance and self-owned key recovery)

We’re having a short break.

Next session starts at 11.20am (GMT+8)

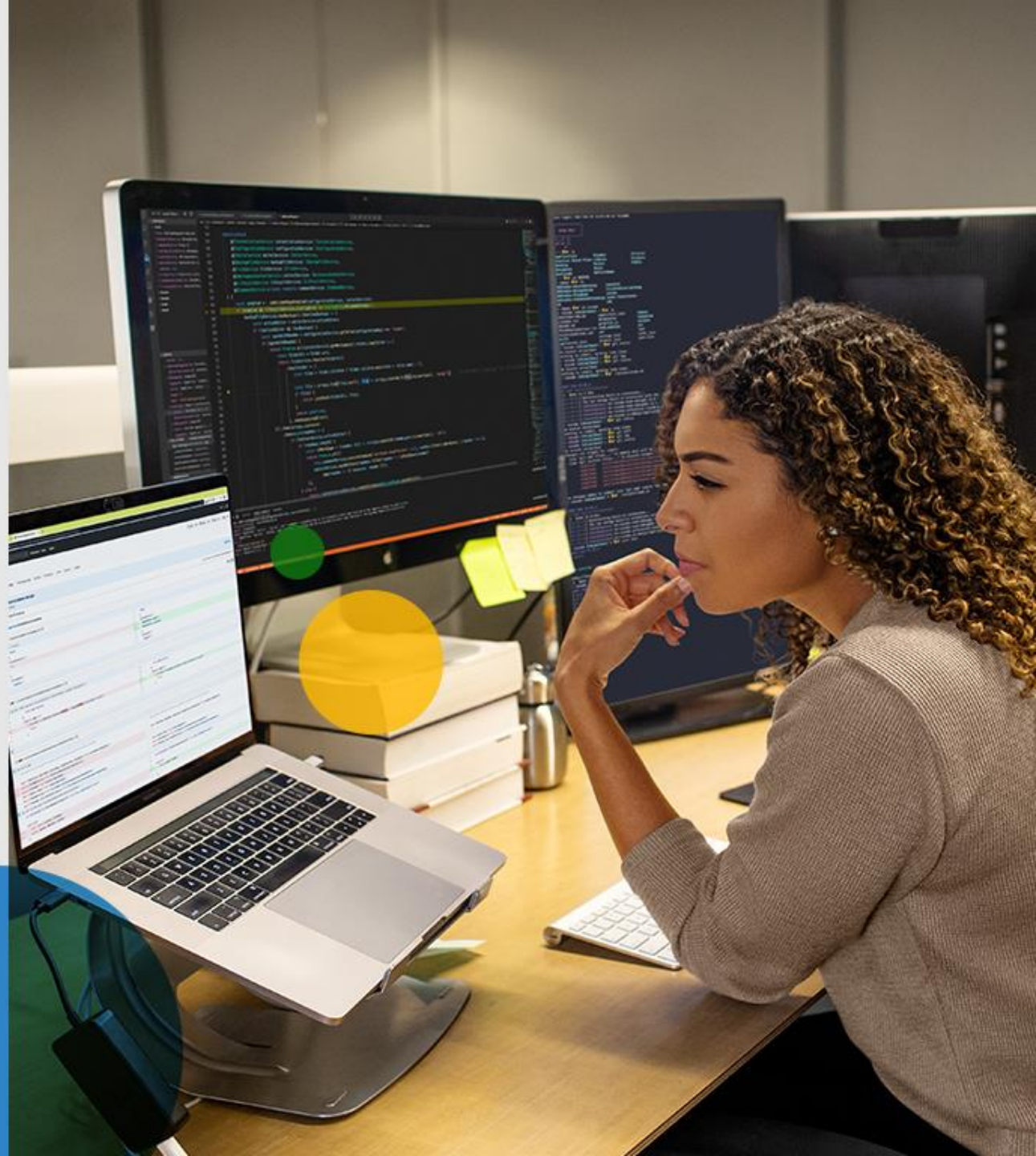
In the meantime, speakers will be answering questions in the chat window, so ask away!

Microsoft Security

Security Tech Frontier Series

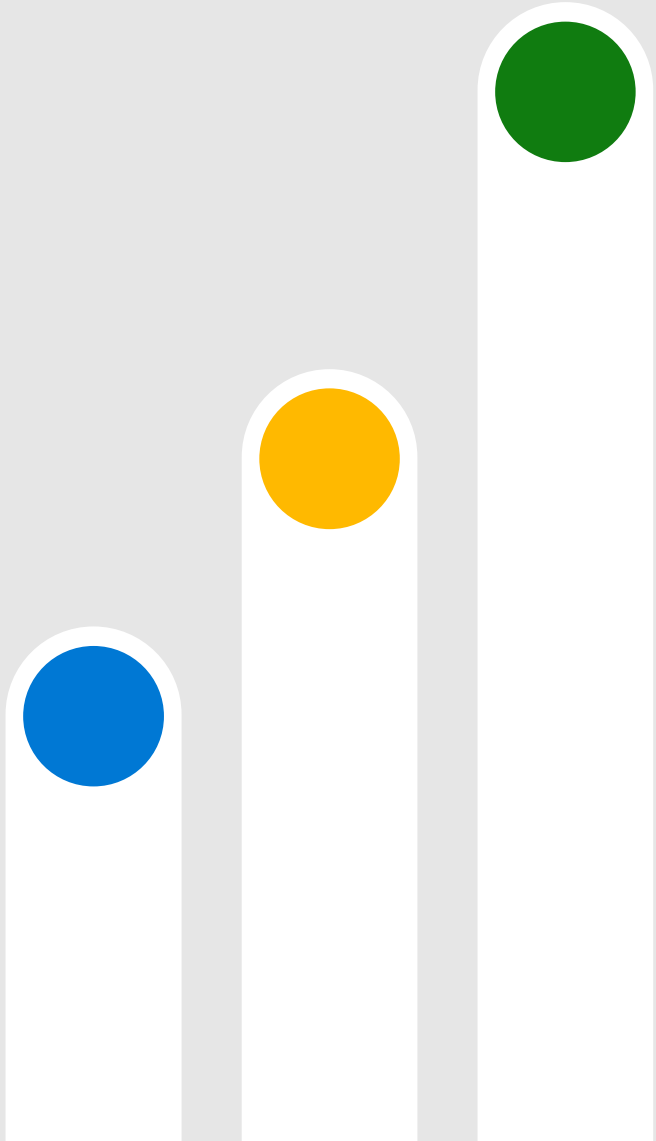
Compliance Hour: Insider risks in today every digitized world - engineering update

Sravan Mera
Sankalp Madaan
Rohit Gupta



Agenda

- Insider risk – Scenario overview
- M365 IRM – Latest features
- Communication compliance - Demo
- Data connectors

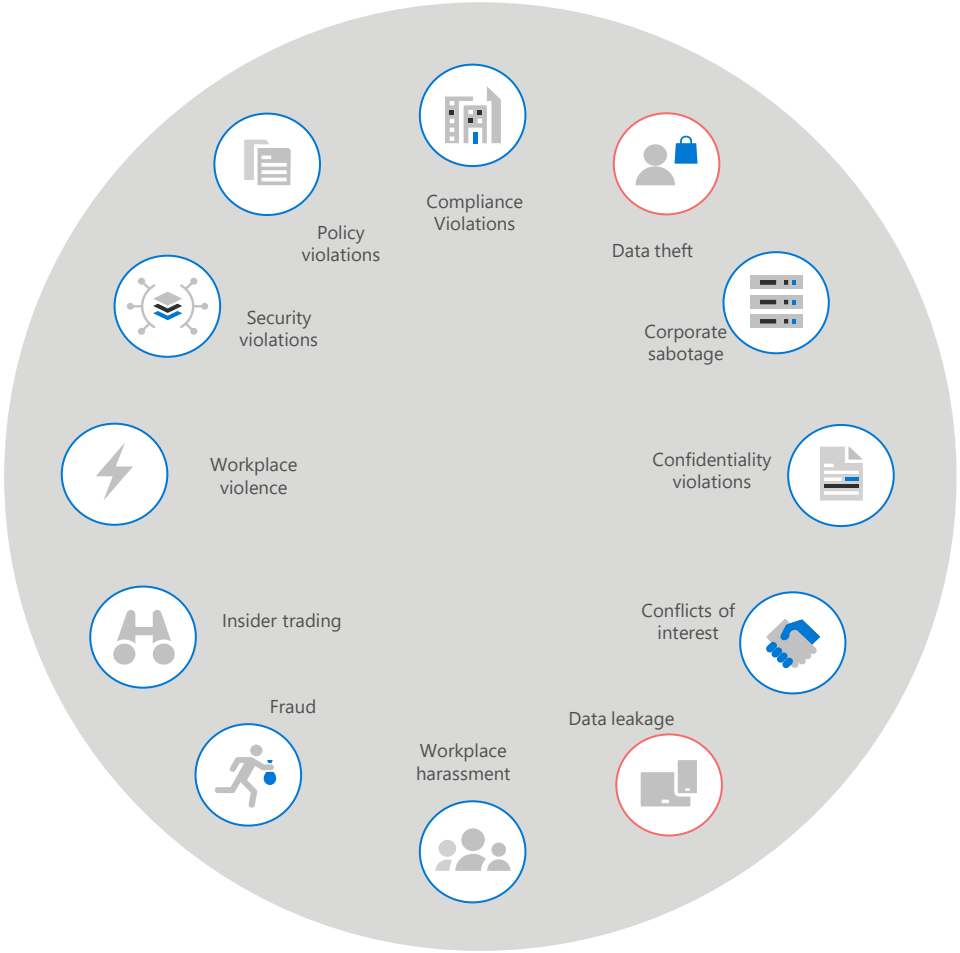


Microsoft

Insider Risk Management

Intelligently investigate and take action on insider risks

While organizations face a broad range of risks from insiders…



Certain risks are more prevalent with significant negative impacts

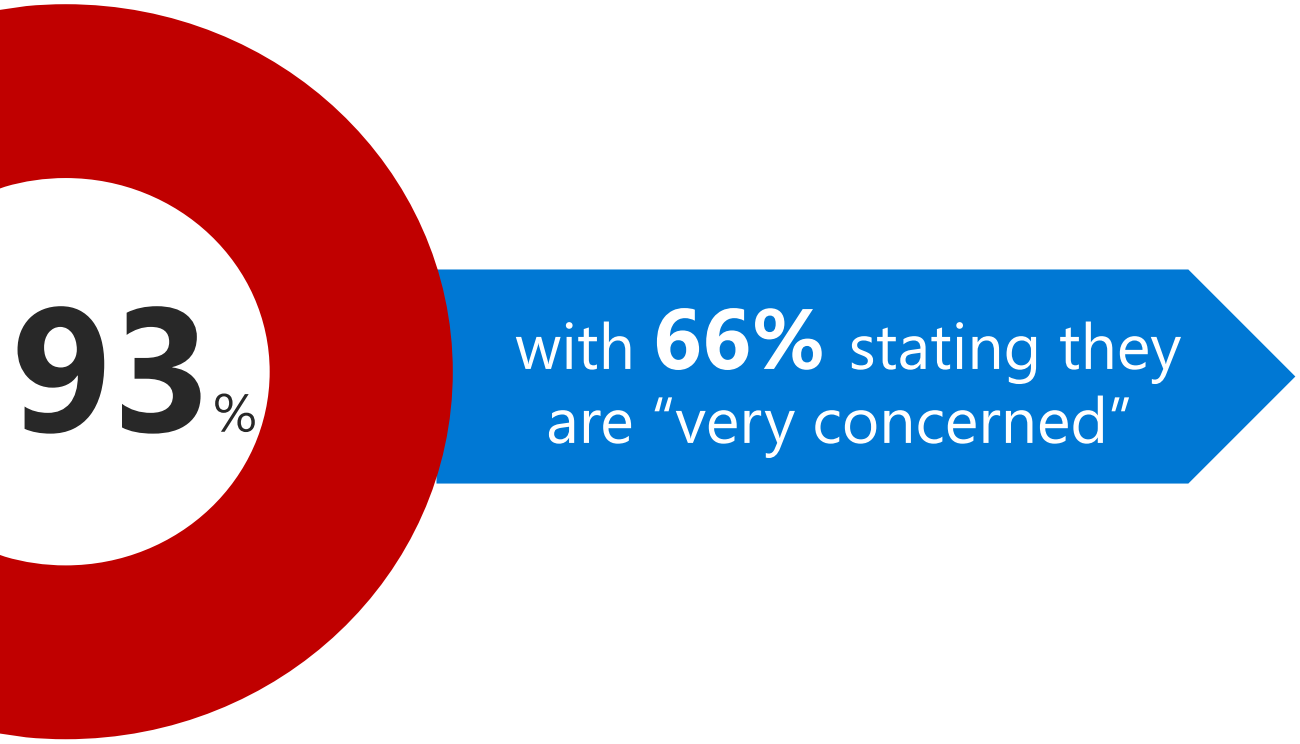
Data theft by departing employees

Data leakage, both malicious and inadvertent

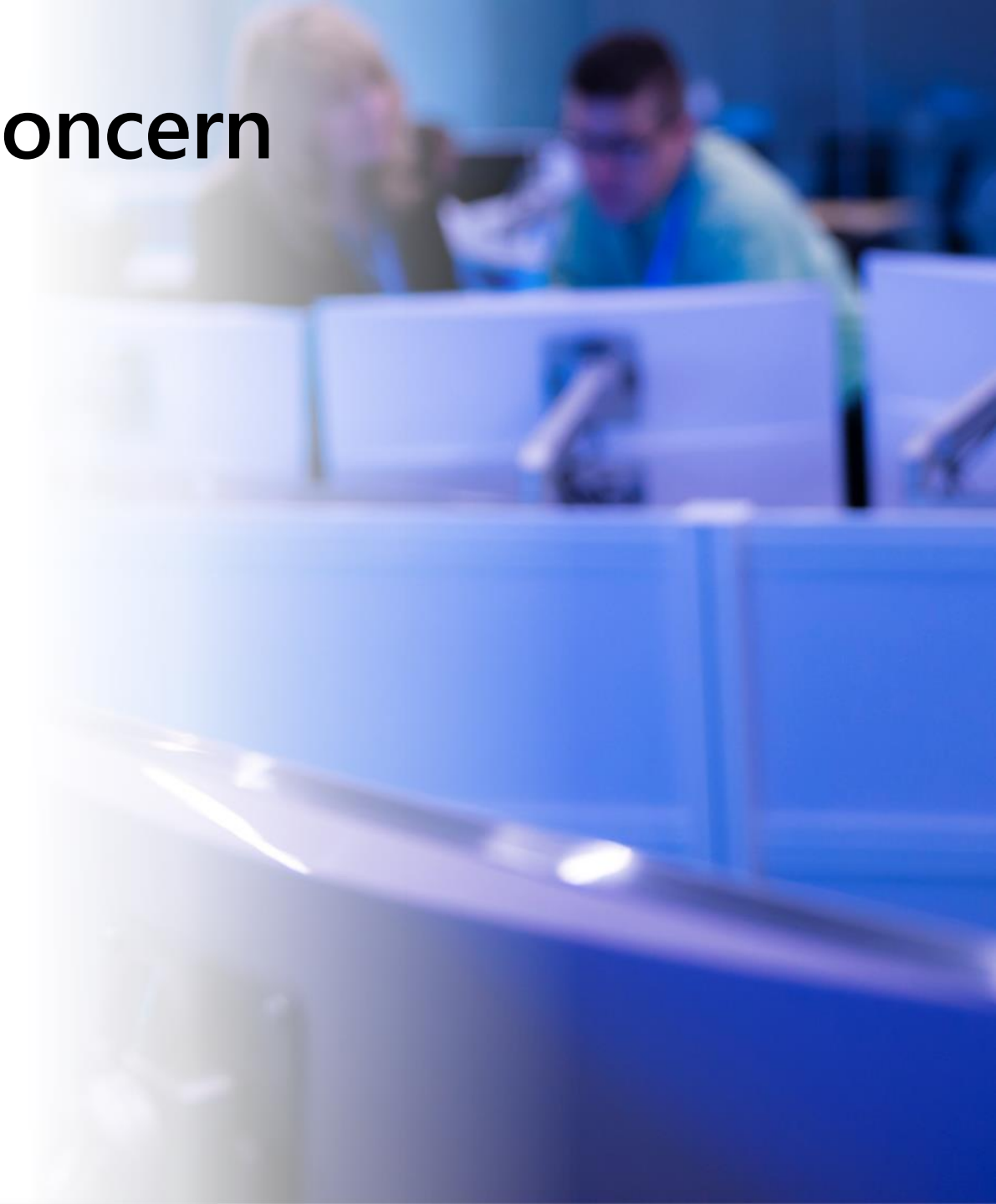
MICROSOFT CONFIDENTIAL

Insider risks are a universal concern

How concerned is your business about insider risks?



with **66%** stating they are “very concerned”



Insider Risk Management Microsoft Market Research January 2021

Insider Risk Management

Quickly identify and take-action on insider risks with integrated end-to-end approach

Rich insights

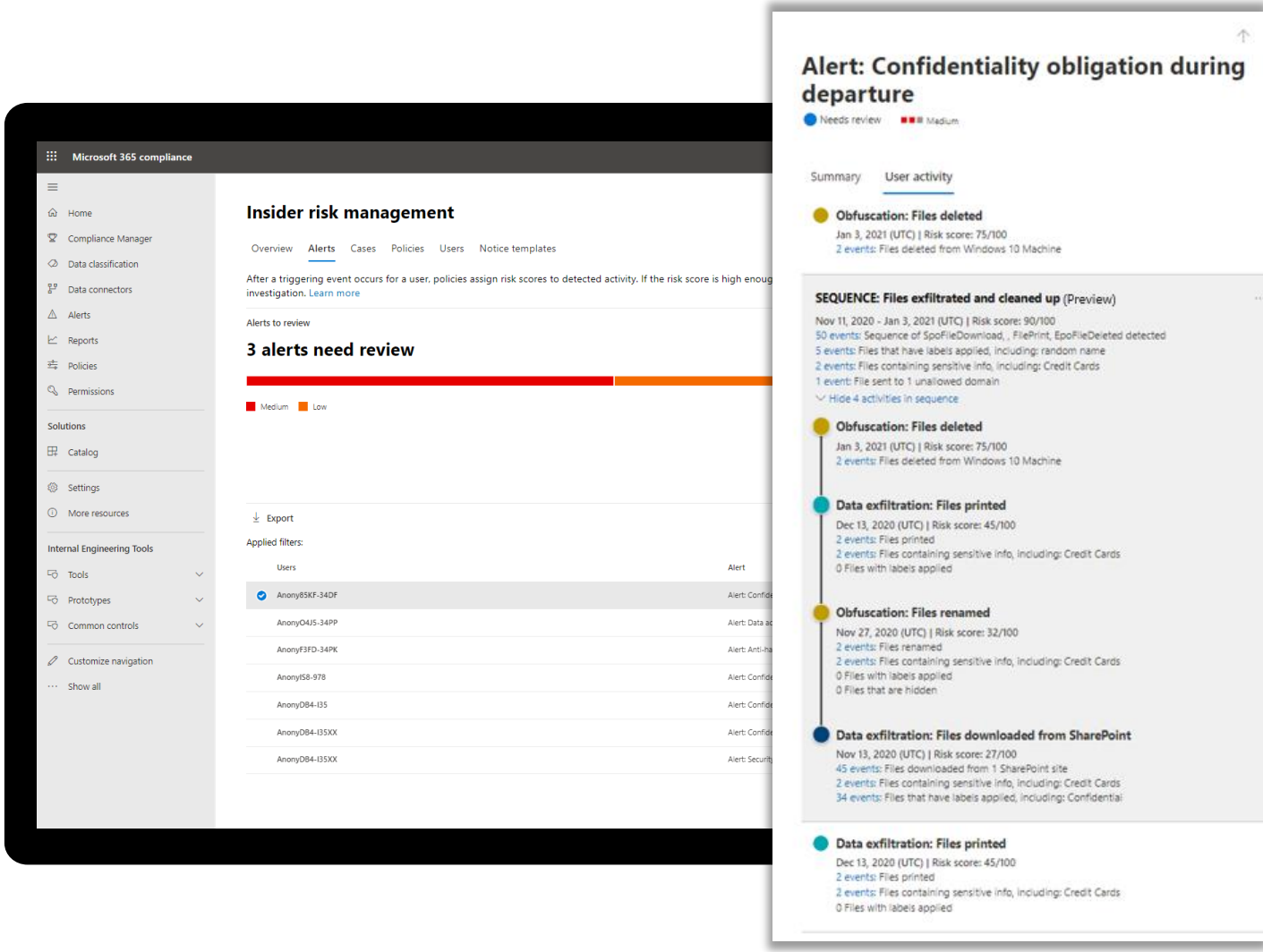
Identify hidden risks with customizable ML templates requiring no end-point agents

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



Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Internal Engineering Tools
Tools
Prototypes

Insider risk management

Insider risk settings | Show in navigation

Overview | Alerts | Cases | Policies | Users | Notice templates

Detect risky activity across your organization to help you quickly identify, investigate, and take action on insider risks and threats. Learn more

Users included in insider risk management policies must have a Microsoft 365 E5 Compliance license or be included in a Microsoft 365 E5 subscription. This feature is subject to the Online Service Terms.

Here are some steps to get you up and running (0/2) complete

Initial Setup - Step 1

Scan for insider risks in your organization (Preview)

Optional step

The risk scan will show data-driven insights on risky activities happening in your organization with recommendations on how to mitigate them. Learn more

Run Scan

Initial Setup - Step 2

Create your first policy

Required step

Insider risk policies are based on pre-defined templates that define the risk activities you want to detect and investigate, such as data theft or data leaks. Learn more

Create policy

Configure insider risk management settings

Before creating policies, you'll need to choose user privacy settings and decide what activities you want your policies to detect.

Get started

Alerts to review

Policy matches	Alert severity	User	Time detected

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog
Audit
Content search
Communication compliance
Data investigations
Data loss prevention
Data subject requests
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Here are the risks we found in your tenant's user activity (Preview)

This report is generated by scanning the activities of users in your organization. All insights are aggregated and anonymized. Learn more about our privacy assurances. If you no longer wish to receive data-driven policy recommendations, you can disable this scan from Insider risk settings

Insights from September 15 - September 28

Data Leaks insight

1.3% of employees are showing data exfiltration patterns

Based on the activity of 23K employees scanned

Recommendation: Monitor leakage of sensitive data with General data leaks policy

General data leaks policy template evaluates the activities of employees activities to detect and alert you on potential data leakage risks.

View details

1.1% of employees have done activities involving sensitive content
0.8% of employees downloaded SPO files
0.7% of employees shared SPO sites externally

Data Theft insight

5.9% of employees with a resignation date are showing exfiltration patterns

Based on the activity of 219 recently departed employees scanned

Recommendation: Monitor leakage of sensitive data with a data theft policy

Departing employee data theft policy template evaluates the activities of employees leaving your organization to detect and alert you on potential data theft risks.

View details

4.9% of employees with a resignation date have done activities involving sensitive content
3.1% of employees with a resignation date downloaded SPO files
2.8% of employees with a resignation date shared SPO sites externally

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data investigations
Data loss prevention
Data subject requests
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Here are the risks we found in your tenant's user activity

This report is generated by scanning the activities of users in your organization. All insights are aggregated and anonymized. Learn more about our privacy assurances. If you no longer wish to receive data-driven policy recommendations, you can disable this scan from Insider risk settings

Insights from September 15 - September 28

Data Leaks insight

1.3% of employees are showing data exfiltration patterns

Based on the activity of 23K employees scanned

1.1% of employees have done activities involvi
content
0.8% of employees downloaded SPO files
0.7% of employees shared SPO sites externally

Recommendation: Monitor leakage of sensitive data with General data leaks policy

General data leaks policy template evaluates the activities of employees activities to detect and alert you on potential data leakage risks.

View details

Data Theft insight

5.9% of employees with a resignation date are showing exfiltration patterns

Based on the activity of 219 recently departed employees scanned

4.9% of employees with a resignation date hav
activities involving sensitive content
3.1% of employees with a resignation date dov
files
2.8% of employees with a resignation date sha
externally

Recommendation: Monitor leakage of sensitive data with a data theft policy

Departing employee data theft policy template evaluates the activities of employees leaving your organization to detect and alert you on potential data theft risks.

View details

Data leak insights

Data leaks can range from accidental oversharing of information outside your organization to data theft with malicious intent.

What we detected

We scanned the activities of 23K employees and found some potentially risky behaviors.

1.3% of employees are showing data exfiltration patterns

- 1.1% of employees have done activities involving sensitive content
- 0.8% of employees downloaded SPO files
- 0.7% of employees shared SPO sites externally
- 0.5% of employees shared SPO folders externally
- 0.5% of employees shared SPO files externally
- 0.4% of employees copied sensitive content to personal cloud
- 0.4% of employees shared files across network
- 0.3% of employees emailed externally
- 0.2% of employees copied content to USB
- 0.1% of employees printed large quantity of files

Mitigate this risk with a policy

Setting up a IRM policy will alert you to any potential risks detected in your organization.

Create policy Close

- Policy template
- Name and description
- Users and groups
- Content to prioritize
- Indicators and triggering event
- Finish

Choose a policy template

These templates are made up of conditions and indicators that define the risk activities you want to detect and investigate. All templates rely on a triggering event to occur before the policy will begin assigning risk scores to user activity. Triggering events are different depending on the template you choose, and prerequisites are required for some policies to work. Learn more about templates

To bypass triggering event requirements, you can temporarily add a user to this policy after it's created. Learn how to do this

Categories

- Data theft
- Security policy violations (pre...
- Data leaks

Templates

- General data leaks
- Data leaks by disgruntled use...
- Data leaks by priority users (...

General data leaks

Detects data leaks by any user included in this policy. Data leaks can range from accidental oversharing of information outside your organization to data theft with malicious intent.
Learn more about this template

Prerequisites

- (Optional) Data loss prevention (DLP) policy configured to generate high severity alerts.
- (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:

- Exfiltration activity. Scores assigned when user performs specific exfiltration activities that exceed certain thresholds.
- DLP policy match. Scores assigned when user performs an activity matching specified DLP policy.

Detected activities include

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

Next

Cancel

Policy template
Name and description
Users and groups
Content to prioritize
Indicators and triggering event
Finish

Indicators and triggering event for this policy

The following triggering event and indicators are used to generate alerts for the activity detected by the policy template you selected. 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 performs an exfiltration activity (Preview)

Policy will start assigning risk scores when specific thresholds are detected for activity relating to the following indicators:

- Files downloaded from SharePoint
- Send email to recipients outside the organization

These indicators will only be used as the triggering event. They won't be used to score related activity unless they're turned on below or on the 'Policy indicators' page in insider risk settings.

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.

Policy indicators

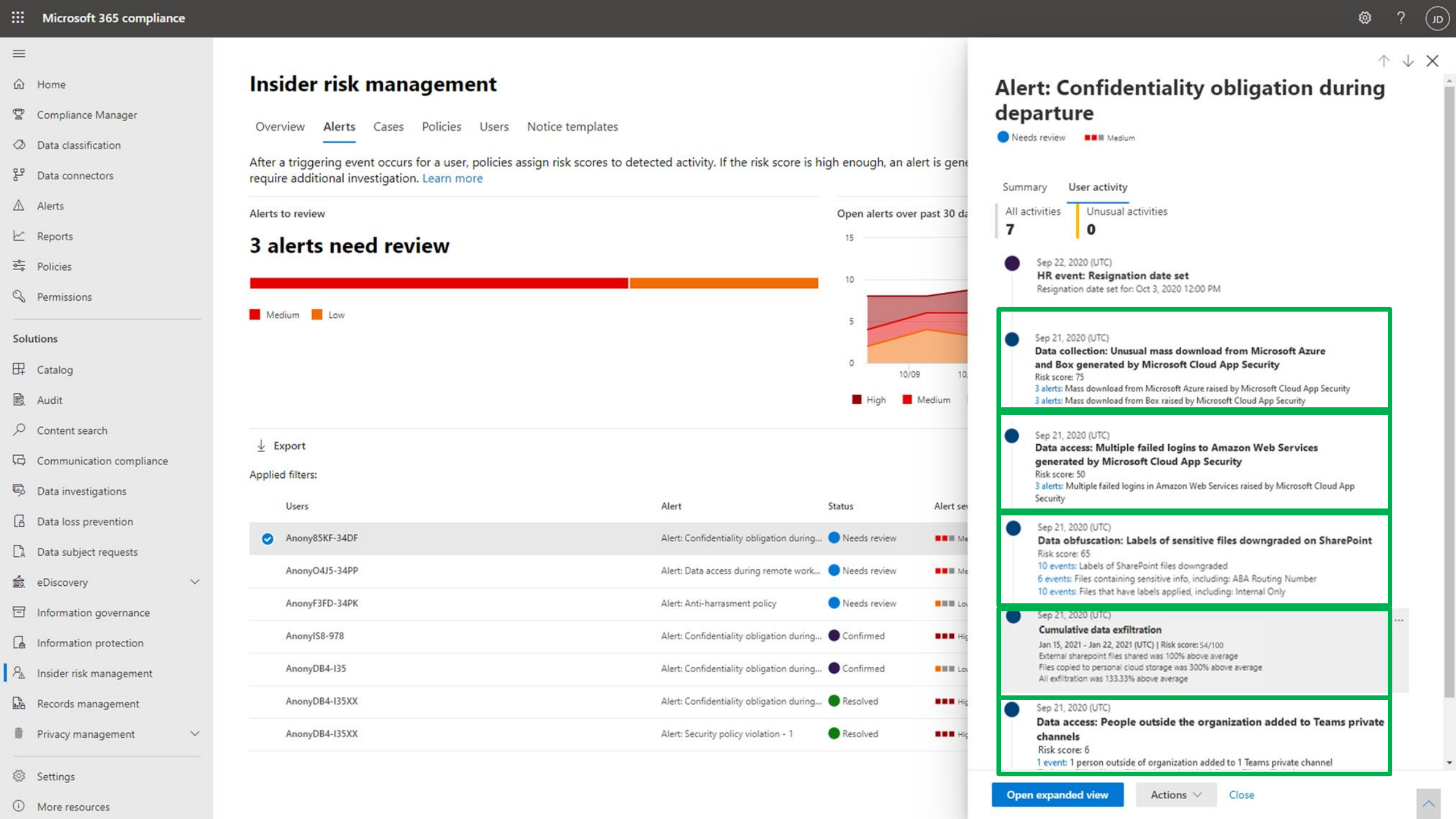
This policy will use the selected indicators below to detect user activity.

If an indicator isn't selected below, you won't receive any alerts for that activity.

Office indicators

- [x] Select all
- [x] Sharing SharePoint files with people outside the organization
- [x] Sharing SharePoint folders with people outside the organization
- [x] Sharing SharePoint sites with people outside the organization
- [x] Downloading content from SharePoint
- [x] Adding people outside organization to SharePoint sites (Preview)
- [x] Downgrading sensitivity labels of SharePoint files (Preview)
- [x] Removing sensitivity labels of SharePoint files (Preview)
- [x] Removing sensitivity labels of SharePoint sites (Preview)
- [x] Accessing sensitive or priority SharePoint files

Back Next Cancel


Microsoft 365 compliance
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Audit
Content search
Communication compliance
Data investigations
Data loss prevention
Data subject requests
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management
Settings
More resources
Insider risk management
Overview
Alerts
Cases
Policies
Users
Notice templates
After a triggering event occurs for a user, policies assign risk scores to detected activity. If the risk score is high enough, an alert is gene
require additional investigation. Learn more
Alerts to review
3 alerts need review
Medium
Low
Open alerts over past 30 da
15
10
5
0
10/09
High
Medium
Export
Applied filters:
Users
Alert
Status
Alert se
Anony85KF-34DF
Alert: Confidentiality obligation during...
Needs review
AnonyO4J5-34PP
Alert: Data access during remote work...
Needs review
AnonyF3FD-34PK
Alert: Anti-harrasment policy
Needs review
AnonyIS8-978
Alert: Confidentiality obligation during...
Confirmed
AnonyDB4-I35
Alert: Confidentiality obligation during...
Confirmed
AnonyDB4-I35XX
Alert: Confidentiality obligation during...
Resolved
AnonyDB4-I35XX
Alert: Security policy violation - 1
Resolved
Alert: Confidentiality obligation during departure
Needs review
Medium
Summary
User activity
All activities
7
Unusual activities
0
Sep 22, 2020 (UTC)
HR event: Resignation date set
Resignation date set for: Oct 3, 2020 12:00 PM
Sep 21, 2020 (UTC)
Data collection: Unusual mass download from Microsoft Azure and Box generated by Microsoft Cloud App Security
Risk score: 75
3 alerts: Mass download from Microsoft Azure raised by Microsoft Cloud App Security
3 alerts: Mass download from Box raised by Microsoft Cloud App Security
Sep 21, 2020 (UTC)
Data access: Multiple failed logins to Amazon Web Services generated by Microsoft Cloud App Security
Risk score: 50
3 alerts: Multiple failed logins in Amazon Web Services raised by Microsoft Cloud App Security
Sep 21, 2020 (UTC)
Data obfuscation: Labels of sensitive files downgraded on SharePoint
Risk score: 65
10 events: Labels of SharePoint files downgraded
6 events: Files containing sensitive info, including: ABA Routing Number
10 events: Files that have labels applied, including: Internal Only
Sep 21, 2020 (UTC)
Cumulative data exfiltration
Jan 15, 2021 - Jan 22, 2021 (UTC) | Risk score: 54/100
External sharepoint files shared was 100% above average
Files copied to personal cloud storage was 300% above average
All exfiltration was 133.33% above average
Sep 21, 2020 (UTC)
Data access: People outside the organization added to Teams private channels
Risk score: 6
1 event: 1 person outside of organization added to 1 Teams private channel
Open expanded view
Actions
Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog

Settings
More resources

Internal Engineering Tools
Tools
Prototypes
Common controls

Customize navigation
Show all

Insider risk management

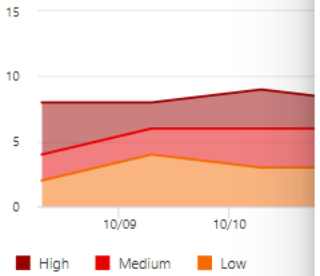
Overview | Alerts | Cases | Policies | Users | Notice templates

After a triggering event occurs for a user, policies assign risk scores to detected activity. If the risk score is high enough, an alert is generated. Confirm alerts if you wa
investigation. Learn more

Alerts to review

3 alerts need review

Open alerts over past 30 days



Export

Applied filters:

Users	Alert	Status	Alert se
Anony85KF-34DF	Alert: Confidentiality obligation during...	Needs review	Me
AnonyO4J5-34PP	Alert: Data access during remote work...	Needs review	Me
AnonyF3FD-34PK	Alert: Anti-harassment policy	Needs review	Lo
AnonyIS8-978	Alert: Confidentiality obligation during...	Confirmed	Hig
AnonyDB4-I35	Alert: Confidentiality obligation during...	Confirmed	Lo
AnonyDB4-I35XX	Alert: Confidentiality obligation during...	Resolved	Hig
AnonyDB4-I35XX	Alert: Security policy violation - 1	Resolved	Hig

Alert: Confidentiality obligation during departure

Needs review Medium

Summary | User activity

Obfuscation: Files deleted
Jan 3, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

SEQUENCE: Files exfiltrated and cleaned up (Preview)
Nov 11, 2020 - Jan 3, 2021 (UTC) | Risk score: 90/100
50 events: Sequence of SpoFileDownload, , FilePrint, EpoFileDeleted detected
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
Show 4 activities in sequence

Data 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

Data exfiltration: Emails with attachments sent outside the organization
Dec 3, 2020 (UTC) | Risk score: 67/100
5 events: Emails sent outside the organization
0 events: Emails sent to 0 unallowed domains
2 events: Files containing sensitive info, including: Credit Cards

Data exfiltration: Emails with attachments sent outside the organization
Dec 1, 2020 (UTC) | Risk score: 23/100
5 events: Emails sent outside the organization
0 events: Emails sent to 0 unallowed domains
0 Emails that contain sensitive info

Obfuscation: Files renamed
Nov 27, 2020 (UTC) | Risk score: 32/100
2 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
0 Files with labels applied
0 Files that are hidden

Data exfiltration: Files downloaded from SharePoint
Nov 21, 2020 (UTC) | Risk score: 24/100
13 events: Files downloaded from 1 SharePoint site
0 Files that contain sensitive info

Open expanded view | Actions | Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog

Settings
More resources

Internal Engineering Tools
Tools
Prototypes
Common controls

Customize navigation
Show all

Insider risk management

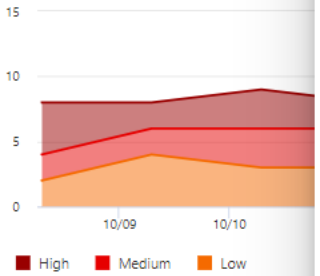
Overview | Alerts | Cases | Policies | Users | Notice templates

After a triggering event occurs for a user, policies assign risk scores to detected activity. If the risk score is high enough, an alert is generated. Confirm alerts if you wa
investigation. Learn more

Alerts to review

3 alerts need review

Open alerts over past 30 days



Export

Applied filters:

Users	Alert	Status	Alert se
Anony85KF-34DF	Alert: Confidentiality obligation during...	Needs review	Me
AnonyO4J5-34PP	Alert: Data access during remote work...	Needs review	Me
AnonyF3FD-34PK	Alert: Anti-harassment policy	Needs review	Lo
AnonyIS8-978	Alert: Confidentiality obligation during...	Confirmed	Hig
AnonyDB4-I35	Alert: Confidentiality obligation during...	Confirmed	Lo
AnonyDB4-I35XX	Alert: Confidentiality obligation during...	Resolved	Hig
AnonyDB4-I35XX	Alert: Security policy violation - 1	Resolved	Hig

Alert: Confidentiality obligation during departure

Needs review Medium

Summary | User activity

Obfuscation: Files deleted
Jan 3, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

SEQUENCE: Files exfiltrated and cleaned up (Preview)
Nov 11, 2020 - Jan 3, 2021 (UTC) | Risk score: 90/100
50 events: Sequence of SpoFileDownload, , FilePrint, EpoFileDeleted detected
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
Hide 4 activities in sequence

Obfuscation: Files deleted
Jan 3, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

Data 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

Obfuscation: Files renamed
Nov 27, 2020 (UTC) | Risk score: 32/100
2 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
0 Files with labels applied
0 Files that are hidden

Data exfiltration: Files downloaded from SharePoint
Nov 13, 2020 (UTC) | Risk score: 27/100
45 events: Files downloaded from 1 SharePoint site
2 events: Files containing sensitive info, including: Credit Cards
34 events: Files that have labels applied, including: Confidential

Data 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

Open expanded view | Actions | Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Risk Type Show by

Obfuscation: Files deleted
Jan 3, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

SEQUENCE: Files exfiltrated and cleaned up
Nov 11, 2020 - Jan 3, 2021 (UTC) | Risk score: 90/100
50 events: Sequence of SpoFileDownload, , FilePrint, EpoFileDeleted detected (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)
Show 4 activities in sequence

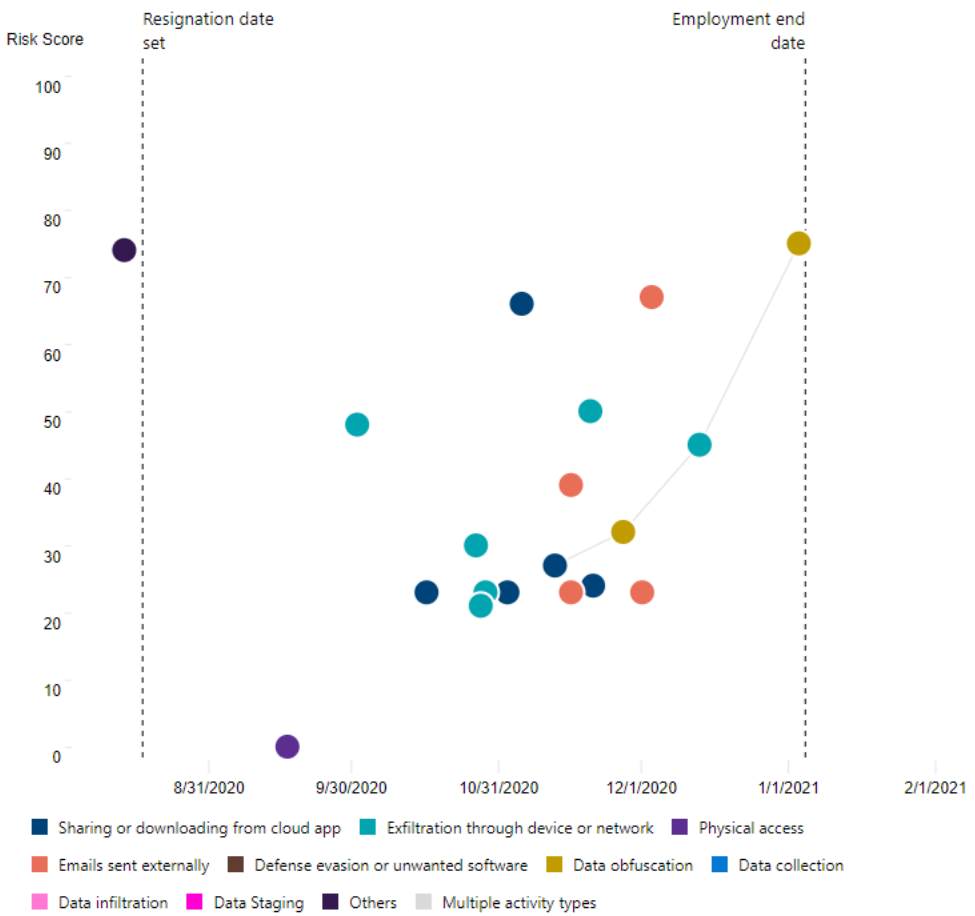
Data exfiltration: Files printed
Dec 13, 2020 (UTC) | Risk score: 45/100
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards
0 Files with labels applied

Data 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

Data exfiltration: Emails with attachments sent outside the organization
Dec 1, 2020 (UTC) | Risk score: 23/100
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

Obfuscation: Files renamed

6 Months 3 Months 1 Month



Case details User details

User profile
Pseudonymize On

Name and title
A Anony85KF-34DF

User email

Alias

Organization or department

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Data subject requests
eDiscovery
Information governance
Information protection
Insider risk management
Records management
Privacy management

Settings
More resources

Risk Type Show by

Obfuscation: Files deleted
Jan 3, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

SEQUENCE: Files exfiltrated and cleaned up
Nov 11, 2020 - Jan 3, 2021 (UTC) | Risk score: 90/100
50 events: Sequence of SpoFileDownload, , FilePrint, EpoFileDeleted detected (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)
Hide 4 activities in sequence

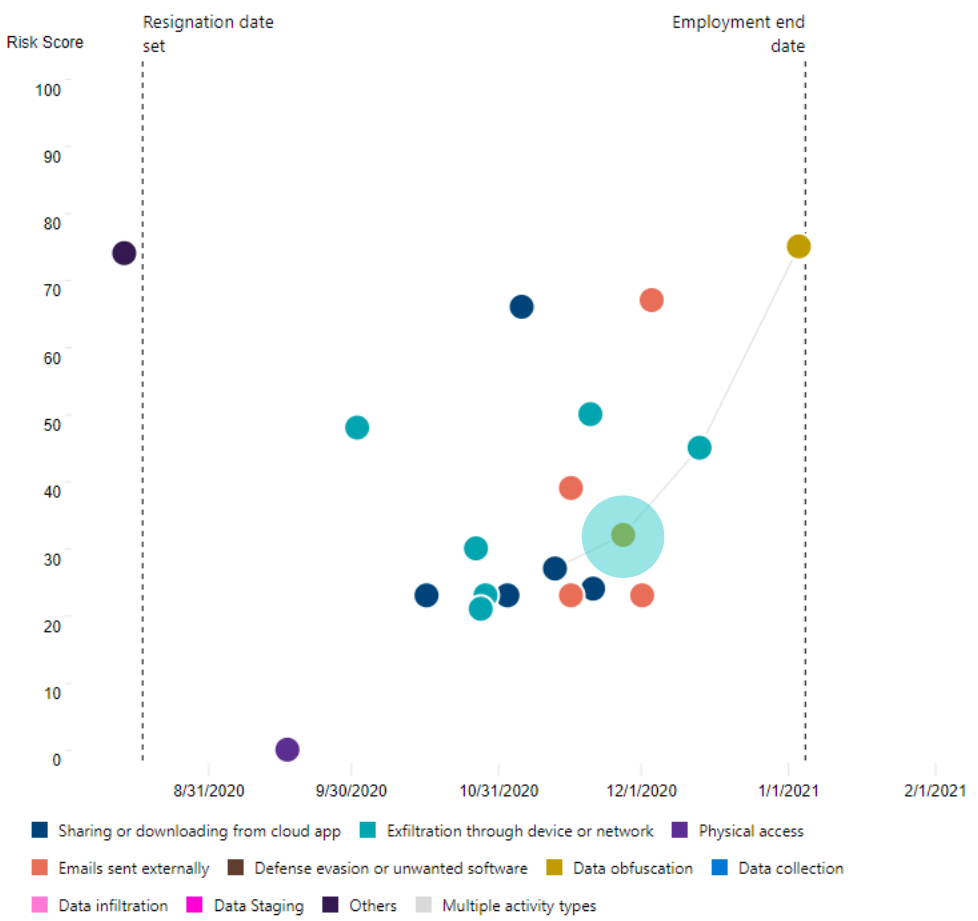
Obfuscation: Files deleted
Jan 3, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

Data 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

Obfuscation: Files renamed
Nov 27, 2020 (UTC) | Risk score: 32/100
2 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
0 Files with labels applied
0 Files that are hidden

Data exfiltration: Files downloaded from SharePoint
Nov 13, 2020 (UTC) | Risk score: 27/100
45 events: Files downloaded from 1 SharePoint site (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
34 events: Files that have labels applied, including:

6 Months 3 Months 1 Month



Case details User details

User profile
Pseudonymize On

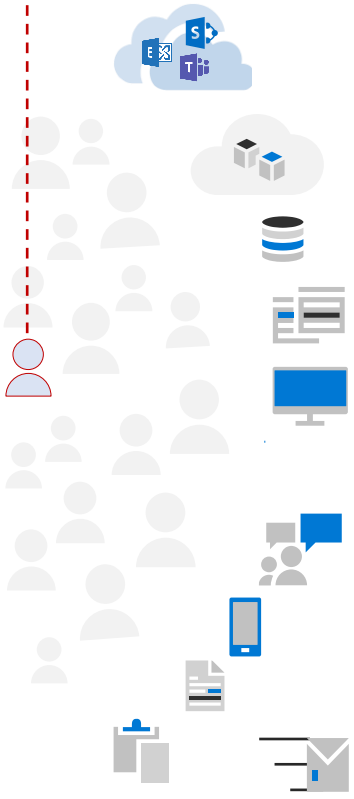
Name and title
A Anony85KF-34DF

User email

Alias

Organization or department

Fractured approach for insider risks



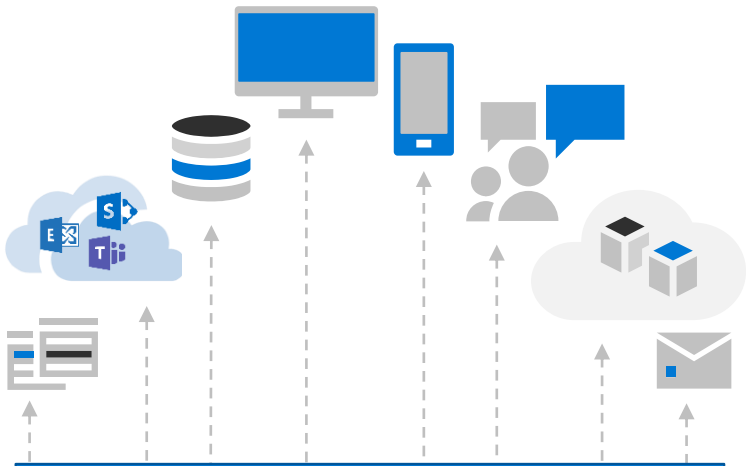
Insider risks are difficult to identify & manage

- Data growing, being accessed and shared across multiple devices and apps
- Visibility into location and movement of sensitive data is poor
- Requires analysis of millions of disparate signals and collaboration (security/HR/legal)

Traditional approaches have limitations

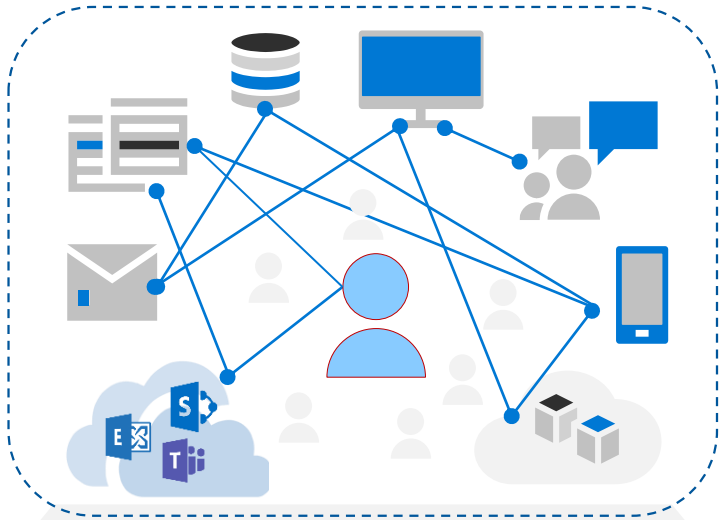
	UEBA (user behavior analytics)	**UAM** (user activity monitoring)	**DLP** (data loss prevention)
Complex setup	• Configuration requires scripting (engineering or managed services) • COGS burden for storage of signals and compute for analytics • Signal curation requires additional solutions (Firewalls, UAM, DLP, EDR) • Events per second are capped • On-prem server-based model	• Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model	• Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model • Some narrowly focused on email communications
Limited enrichment	• Low visibility into content • Low sentiment analysis • Low understanding of content sensitivity	• Low visibility into content • Low sentiment analysis • Limited signal correlation • Low understanding of content sensitivity	• Low visibility into content • Low sentiment analysis • Limited signal correlation • Prone to high-false positive rate
Narrow workflows	• No integrated workflow beyond SOC	• No integrated workflow beyond SOC	• No integrated workflow beyond SOC

Addressing risks to your information



Data Loss Prevention

Enforcing data loss prevention rules across endpoints

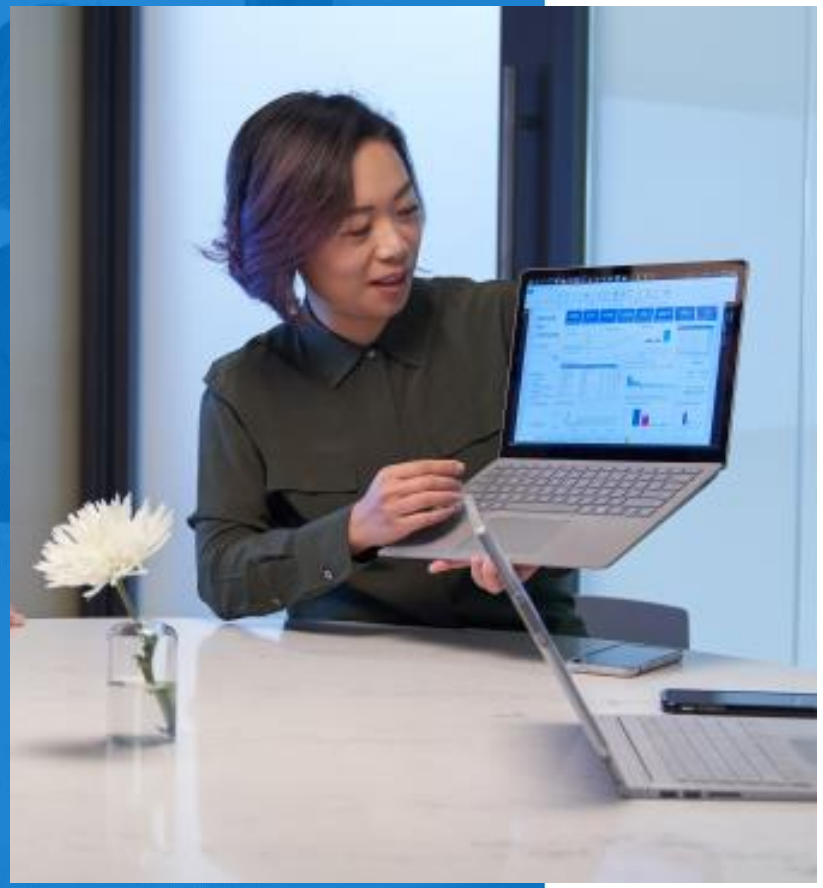


Insider Risk Management

Identify and mitigate risks by a user

	Data Loss Prevention	Insider Risk Management
Pivot	Content	User
Risk identification	Transactional	Correlated
Mitigation of risk	Rule enforcement / User Education	Collaborate across security, HR, legal
Examples	• **Block printing** of Word documents with Credit Cards, • **Audit copying** PDF files with label "Confidential" to USB, • **Warn w/ Override** uploading of Office files with label "Sensitive" to Cloud	• Identify **departing employees who are** taking sensitive documents upon departure • Identify **creative insider threat** by correlating activities (collection> obfuscation>exfiltration) • Identify the **vigilant insider threat** involved in careful low-and-slow leak over days

Getting started



Start using Insider Risk Management today
https://compliance.microsoft.com

Take a quick look at
https://aka.ms/insiderriskguide

Learn more: http://aka.ms/insiderriskblog

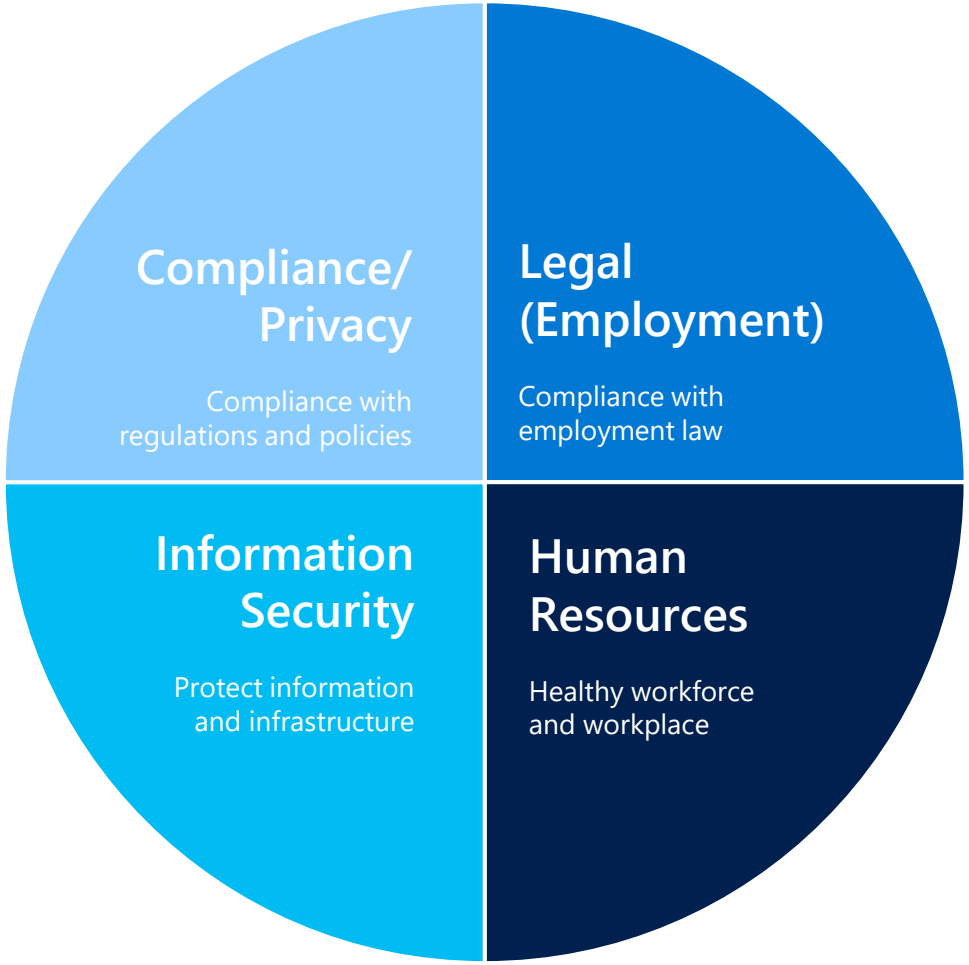
Microsoft

Communication Compliance

Quickly identify and remediate corporate code-of-conduct policy violations

Organizations face a broad range of communication risks

And many stakeholders are involved to address these risks



Communication Compliance

Quickly identify and remediate corporate code-of-conduct policy violations

Intelligent customizable playbooks

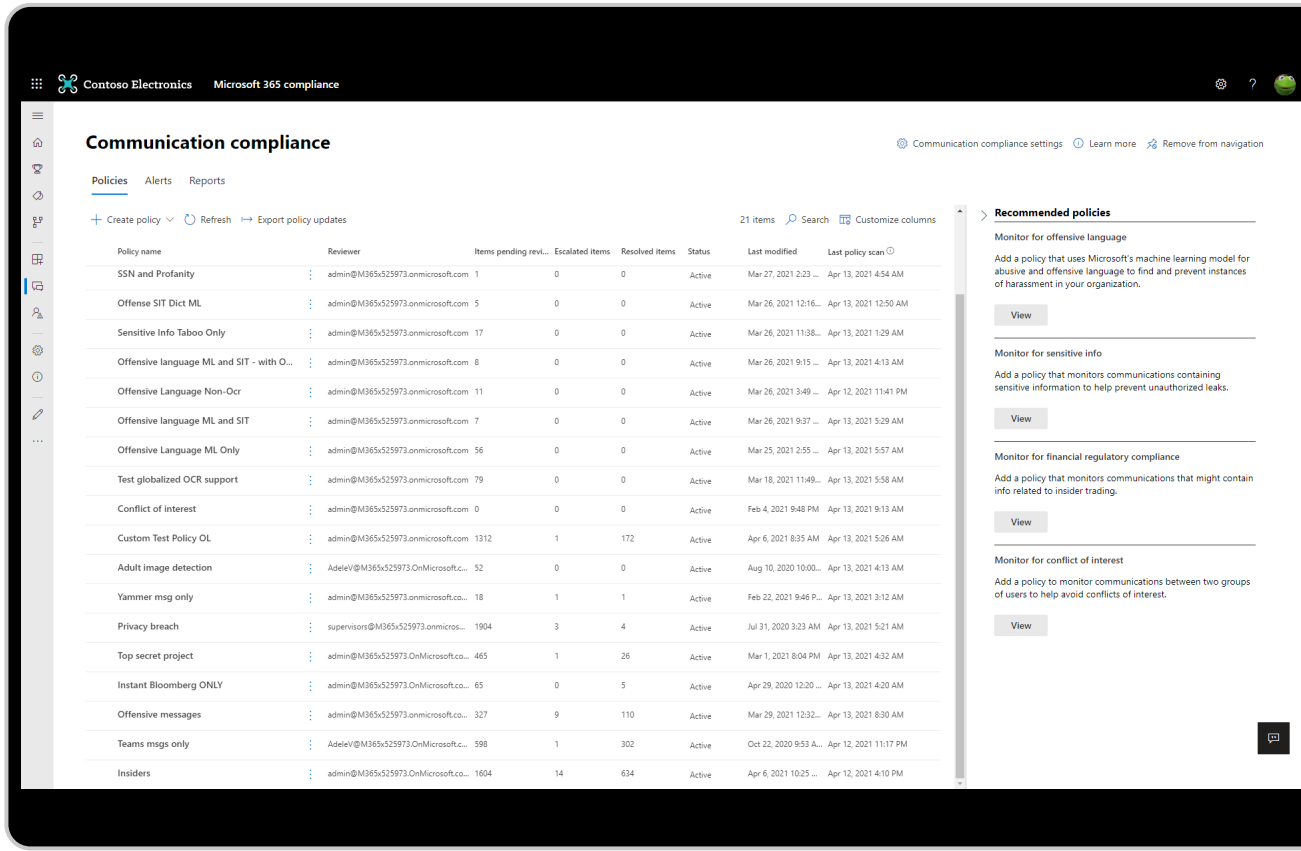
Leverage machine learning to detect violations across Teams, Exchange and 3rd party content

Flexible remediation workflows

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

Built-in privacy by design

Pseudonymization, audit trails and strong controls to appropriately manage data about risks



Tailored policy templates

Detect offensive or threatening language

Detect for distribution of sensitive information

Detect for information related to financial regulatory compliance

Detect potential **conflicts of interest** between 2 groups of users

Learn about our newest feature announcements at aka.ms/ccrsa2021

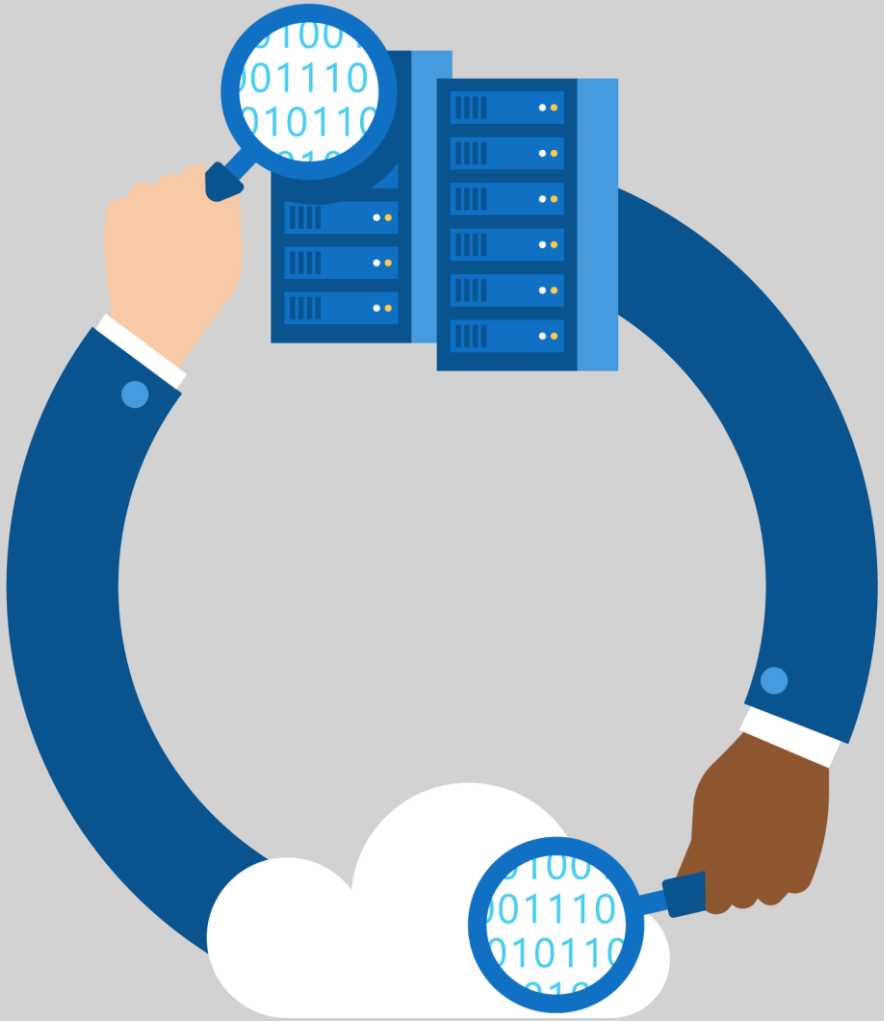
Better Together with Microsoft Teams

	Communication compliance By Microsoft	Competitors
Visibility	Native Teams Shared channels Private channels Adaptive cards	No
Review	Additional Teams context	No
Remediation	Remove Teams message	No
Coming Soon	Modern attachments Report offensive content	No

Microsoft

Communication Compliance

Demo



Demo: Communication Compliance

Home
Compliance Manager
Data classification
Data connectors

Solutions
Catalog
Communication compliance
Insider risk management

Settings
More resources

Customize navigation
Show all

Communication compliance

Communication compliance settings | Learn more | Remove from navigation

Policies | Alerts | Reports

Create policy | Refresh | Export policy updates | 21 items | Search | Customize columns

Policy name	Reviewer	Items pending revi...	Escalated items	Resolved items	Status	Last modified	Last policy scan
Offense SIT Dict ML	admin@M365x525973.onmicrosoft.com	5	0	0	Active	Mar 26, 2021 12:16...	Apr 13, 2021 12:50 AM
Sensitive Info Taboo Only	admin@M365x525973.onmicrosoft.com	17	0	0	Active	Mar 26, 2021 11:38...	Apr 13, 2021 1:29 AM
Offensive language ML a...	admin@M365x525973.onmicrosoft.com	8	0	0	Active	Mar 26, 2021 9:15 ...	Apr 13, 2021 4:13 AM
Offensive Language Non-...	admin@M365x525973.onmicrosoft.com	11	0	0	Active	Mar 26, 2021 3:49 ...	Apr 12, 2021 11:41 PM
Offensive language ML a...	admin@M365x525973.onmicrosoft.com	7	0	0	Active	Mar 26, 2021 9:37 ...	Apr 13, 2021 5:29 AM
Offensive Language ML ...	admin@M365x525973.onmicrosoft.com	56	0	0	Active	Mar 25, 2021 2:55 ...	Apr 13, 2021 5:57 AM
Test globalized OCR supp...	admin@M365x525973.onmicrosoft.com	79	0	0	Active	Mar 18, 2021 11:49...	Apr 13, 2021 5:58 AM
Conflict of interest	admin@M365x525973.onmicrosoft.com	0	0	0	Active	Feb 4, 2021 9:48 PM	Apr 13, 2021 9:13 AM
Custom Test Policy OL	admin@M365x525973.onmicrosoft.com	1312	1	172	Active	Apr 6, 2021 8:35 AM	Apr 13, 2021 5:26 AM
Adult image detection	AdeleV@M365x525973.OnMicrosoft.c...	52	0	0	Active	Aug 10, 2020 10:00...	Apr 13, 2021 4:13 AM
Yammer msg only	admin@M365x525973.onmicrosoft.co...	18	1	1	Active	Feb 22, 2021 9:46 P...	Apr 13, 2021 3:12 AM
Privacy breach	supervisors@M365x525973.onmicros...	1904	3	4	Active	Jul 31, 2020 3:23 AM	Apr 13, 2021 5:21 AM
Top secret project	admin@M365x525973.OnMicrosoft.co...	465	1	26	Active	Mar 1, 2021 8:04 PM	Apr 13, 2021 4:32 AM
Instant Bloomberg ONLY	admin@M365x525973.OnMicrosoft.co...	65	0	5	Active	Apr 29, 2020 12:20 ...	Apr 13, 2021 4:20 AM
Offensive messages	admin@M365x525973.onmicrosoft.co...	327	9	110	Active	Mar 29, 2021 12:32...	Apr 13, 2021 8:30 AM
Teams msgs only	AdeleV@M365x525973.OnMicrosoft.c...	598	1	302	Active	Oct 22, 2020 9:53 A...	Apr 12, 2021 11:17 PM
Insiders	admin@M365x525973.OnMicrosoft.co...	1604	14	634	Active	Apr 6, 2021 10:25 ...	Apr 12, 2021 4:10 PM

Recommended policies

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.

View

Monitor for sensitive info

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

View

Monitor for financial regulatory compliance

Add a policy that monitors communications that might contain info related to insider trading.

View

Monitor for conflict of interest

Add a policy to monitor communications between two groups of users to help avoid conflicts of interest.

View

Communication compliance

Communication compliance settings | Learn more | Remove from navigation

Policies | Alerts | Reports

Create policy | Refresh | Export policy updates | 21 items | Search | Customize columns

Policy name	Reviewer	Items pending revi...	Escalated items	Resolved items	Status	Last modified	Last policy scan
SSN and Profanity	admin@M365x525973.onmicrosoft.com	1	0	0	Active	Mar 27, 2021 2:23 ...	Apr 13, 2021 4:54 AM
Offense SIT Dict ML	admin@M365x525973.onmicrosoft.com	5	0	0	Active	Mar 26, 2021 12:16...	Apr 13, 2021 12:50 AM
Sensitive Info Taboo Only	admin@M365x525973.onmicrosoft.com	17	0	0	Active	Mar 26, 2021 11:38...	Apr 13, 2021 1:29 AM
Offensive language ML and SIT - with O...	admin@M365x525973.onmicrosoft.com	8	0	0	Active	Mar 26, 2021 9:15 ...	Apr 13, 2021 4:13 AM
Offensive Language Non-Ocr	admin@M365x525973.onmicrosoft.com	11	0	0	Active	Mar 26, 2021 3:49 ...	Apr 12, 2021 11:41 PM
Offensive language ML and SIT	admin@M365x525973.onmicrosoft.com	7	0	0	Active	Mar 26, 2021 9:37 ...	Apr 13, 2021 5:29 AM
Offensive Language ML Only	admin@M365x525973.onmicrosoft.com	56	0	0	Active	Mar 25, 2021 2:55 ...	Apr 13, 2021 5:57 AM
Test globalized OCR support	admin@M365x525973.onmicrosoft.com	79	0	0	Active	Mar 18, 2021 11:49...	Apr 13, 2021 5:58 AM
Conflict of interest	admin@M365x525973.onmicrosoft.com	0	0	0	Active	Feb 4, 2021 9:48 PM	Apr 13, 2021 9:13 AM
Custom Test Policy OL	admin@M365x525973.onmicrosoft.com	1312	1	172	Active	Apr 6, 2021 8:35 AM	Apr 13, 2021 5:26 AM
Adult image detection	AdeleV@M365x525973.OnMicrosoft.c...	52	0	0	Active	Aug 10, 2020 10:00...	Apr 13, 2021 4:13 AM
Yammer msg only	admin@M365x525973.onmicrosoft.co...	18	1	1	Active	Feb 22, 2021 9:46 P...	Apr 13, 2021 3:12 AM
Privacy breach	supervisors@M365x525973.onmicros...	1904	3	4	Active	Jul 31, 2020 3:23 AM	Apr 13, 2021 5:21 AM
Top secret project	admin@M365x525973.OnMicrosoft.co...	465	1	26	Active	Mar 1, 2021 8:04 PM	Apr 13, 2021 4:32 AM
Instant Bloomberg ONLY	admin@M365x525973.OnMicrosoft.co...	65	0	5	Active	Apr 29, 2020 12:20 ...	Apr 13, 2021 4:20 AM
Offensive messages	admin@M365x525973.onmicrosoft.co...	327	9	110	Active	Mar 29, 2021 12:32...	Apr 13, 2021 8:30 AM
Teams msgs only	AdeleV@M365x525973.OnMicrosoft.c...	598	1	302	Active	Oct 22, 2020 9:53 A...	Apr 12, 2021 11:17 PM
Insiders	admin@M365x525973.OnMicrosoft.co...	1604	14	634	Active	Apr 6, 2021 10:25 ...	Apr 12, 2021 4:10 PM

Recommended policies

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.

View

Monitor for sensitive info

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

View

Monitor for financial regulatory compliance

Add a policy that monitors communications that might contain info related to insider trading.

View

Monitor for conflict of interest

Add a policy to monitor communications between two groups of users to help avoid conflicts of interest.

View

Communication compliance

Communication compliance settings | Learn more | Remove from navigation

Policies | Alerts | Reports

Create policy | Refresh | Export policy updates | 21 items | Search | Customize columns

- Monitor for offensive language
- Monitor for sensitive info
- Monitor for regulatory compliance
- Monitor for conflict of interest
- Custom policy

	Reviewer	Items pending revi...	Escalated items	Resolved items	Status	Last modified	Last policy scan
	admin@M365x525973.onmicrosoft.com	1	0	0	Active	Mar 27, 2021 2:23 ...	Apr 13, 2021 4:54 AM
	admin@M365x525973.onmicrosoft.com	5	0	0	Active	Mar 26, 2021 12:16...	Apr 13, 2021 12:50 AM
	admin@M365x525973.onmicrosoft.com	17	0	0	Active	Mar 26, 2021 11:38...	Apr 13, 2021 1:29 AM
Offensive language ML and SIT - with O...	admin@M365x525973.onmicrosoft.com	8	0	0	Active	Mar 26, 2021 9:15 ...	Apr 13, 2021 4:13 AM
Offensive Language Non-Ocr	admin@M365x525973.onmicrosoft.com	11	0	0	Active	Mar 26, 2021 3:49 ...	Apr 12, 2021 11:41 PM
Offensive language ML and SIT	admin@M365x525973.onmicrosoft.com	7	0	0	Active	Mar 26, 2021 9:37 ...	Apr 13, 2021 5:29 AM
Offensive Language ML Only	admin@M365x525973.onmicrosoft.com	56	0	0	Active	Mar 25, 2021 2:55 ...	Apr 13, 2021 5:57 AM
Test globalized OCR support	admin@M365x525973.onmicrosoft.com	79	0	0	Active	Mar 18, 2021 11:49...	Apr 13, 2021 5:58 AM
Conflict of interest	admin@M365x525973.onmicrosoft.com	0	0	0	Active	Feb 4, 2021 9:48 PM	Apr 13, 2021 9:13 AM
Custom Test Policy OL	admin@M365x525973.onmicrosoft.com	1312	1	172	Active	Apr 6, 2021 8:35 AM	Apr 13, 2021 5:26 AM
Adult image detection	AdeleV@M365x525973.OnMicrosoft.c...	52	0	0	Active	Aug 10, 2020 10:00...	Apr 13, 2021 4:13 AM
Yammer msg only	admin@M365x525973.onmicrosoft.co...	18	1	1	Active	Feb 22, 2021 9:46 P...	Apr 13, 2021 3:12 AM
Privacy breach	supervisors@M365x525973.onmicros...	1904	3	4	Active	Jul 31, 2020 3:23 AM	Apr 13, 2021 5:21 AM
Top secret project	admin@M365x525973.OnMicrosoft.co...	465	1	26	Active	Mar 1, 2021 8:04 PM	Apr 13, 2021 4:32 AM
Instant Bloomberg ONLY	admin@M365x525973.OnMicrosoft.co...	65	0	5	Active	Apr 29, 2020 12:20 ...	Apr 13, 2021 4:20 AM
Offensive messages	admin@M365x525973.onmicrosoft.co...	327	9	110	Active	Mar 29, 2021 12:32...	Apr 13, 2021 8:30 AM
Teams msgs only	AdeleV@M365x525973.OnMicrosoft.c...	598	1	302	Active	Oct 22, 2020 9:53 A...	Apr 12, 2021 11:17 PM
Insiders	admin@M365x525973.OnMicrosoft.co...	1604	14	634	Active	Apr 6, 2021 10:25 ...	Apr 12, 2021 4:10 PM

Recommended policies

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.

View

Monitor for sensitive info

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

View

Monitor for financial regulatory compliance

Add a policy that monitors communications that might contain info related to insider trading.

View

Monitor for conflict of interest

Add a policy to monitor communications between two groups of users to help avoid conflicts of interest.

View

- Name
- Users and reviewers
- Locations
- Conditions and percentage
- Finish

Name and describe your policy

Name *

Analyze MS Teams IM

Description

Enter a description for your custom policy

Next

Cancel

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

Choose supervised users and reviewers

Supervised users and groups *

Choose the users and group whose communications you want to supervise.

- (•) All users
- ( ) Select users

Start typing to find users or groups

Excluded users and groups

If you choose a group to supervise, you can exclude specific group members.

Start typing to find users or groups

Reviewers *

Choose users to review the communications that are returned by this policy.

AV Adele Vance × AW Alex Wilber × CF Christophe Fiessinger × Start typing to find users

Choose locations to monitor communications

Microsoft 365 locations

- [ ] **Exchange.** ⓘ
  Emails and attachments sent or received by Exchange mailboxes.
- [x] **Teams.**
  Messages in Teams channels and individual and group chats.
- [ ] **Skype for Business.**
  Messages in individual and group conversations.
- [ ] **Yammer**
  Private messages and community conversations.

Third-party sources

Learn more

- [ ] **Bloomberg**

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

Choose conditions and review percentage

Communication direction *

- [x] **Inbound.**
  Detects communications sent to supervised users from external and internal senders, including other supervised users in this policy.
- [x] **Outbound.**
  Detects communications sent from supervised users to external and internal recipients, including other supervised users in this policy.
- [x] **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 to communications matching specific criteria. Learn more about these conditions

+ Add condition

Optical character recognition

- [ ] **Extract printed or handwritten text from images for evaluation (preview).**
  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 from the total that matched any conditions you chose.

10%

- 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 in this policy.

Outbound.
Detects communications sent from supervised users to external and internal recipients, including other supervised users in this policy.

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

Conditions

By default we will monit specified. Add conditions to limit the results to communications matching specific criteria. Learn more abo

+ Add condition

- Content matches any of these classifiers
- Content contains any of these sensitive info types
- Message contains any of these words
- Message contains none of these words
- Message is received from any of these domains
- Message is not received from any of these domains
- Message is sent to any of these domains
- Message is not sent to any of these domains
- Attachment size is larger than
- Attachment size is not larger than
- Attachment contains any of these words
- Attachment contains none of these words
- Attachment is one of these file types
- Attachment is none of these file types
- Message size is larger than
- Message size is not larger than
- Message is classified with any of these labels
- Message is not classified with any of these labels

Optical character recog

Extract printed or ew).
Only enabled for po sitive info types.

Review percentage

If you want to reduce th We'll randomly select the amount of content from the total that matched any conditions you chose.

Back Next Cancel

- 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

Add

Trainable classifiers

Add condition

Optical character recognition

Extract printed or handwritten text from images for evaluation (preview).
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%

Back Next

Trainable classifiers

Search

6 selected

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
Adult images	
Racy images	
Gory images	

Add Cancel

- 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 in this policy.
- **Outbound.**
  Detects communications sent from supervised users to external and internal recipients, including other supervised users in this policy.
- **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 to communications matching specific criteria. Learn more about these conditions

Content matches any of these classifiers

Any of these

Trainable classifiers

- Harassment
- Profanity
- Threat
- Adult images
- Racy images
- Gory images

Add

Back Next Cancel

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

Harassment

Profanity

Threat

Adult images

Racy images

Gory images

Add

OR

Content contains any of these sensitive info types

Default

Add

Sensitive info types

Add condition

AND

Add condition

Optical character recognition

Extract printed or handwritten text from images for evaluation (preview).

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%

Back Next

Sensitive info types

Add new

Search for Sensitive info types

1 selected

Name	Publisher
Kamakshi_Test_OMGCA	Contoso
Lexicon test 1	Contoso
New INSIDERS lexicon	Contoso
New LEXICON 2	Contoso
Profanities	Contoso
Profanities- keywords dictionary	Contoso
profanity v1	Contoso
Project enigma v2	Contoso
Taboo words	Contoso
test_regex	Contoso
Test2	Contoso
TestSITAshishEscalation	Contoso
Profanity	CC FHL
Targeted Harassment	CC FHL
Bad SIT	BitServer, LLC.

Add Cancel

Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Communication compliance
Settings
More resources
Customize navigation
Show all

Name
Users and reviewers
Locations
Conditions and percentage
Finish

matching specific criteria. Learn more about these conditions

Content matches any of these classifiers

Any of these

Trainable classifiers

- Targeted Harassment
- Profanity
- Threat
- Adult images
- Racy images

Add

OR

Content contains any of these sensitive info types

Default — All of these

Sensitive info types

Taboo words — High confidence — Instance count 1 to Any

Add

Create group

Back Next Cancel

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

Threat

Adult images

Racy images

Gory images

Add

OR

Content contains any of these sensitive info types

Default — Any of these

Sensitive info types

Taboo words — High confidence — Instance count 1 to Any

Add

Create group

Add condition

AND

Add condition

Optical character recognition

Extract printed or handwritten text from images for evaluation (preview).

Review percentage

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

100%

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

Review and finish

Name and description

Name

Analyze MS Teams IM

Users and reviewers

Supervised users and groups

AllUsersGroupsOfTenant

Excluded users and groups

None

Reviewers

AdeleV@M365x525973.OnMicrosoft.com,AlexW@M365x525973.OnMicrosoft.com,admin@M365x525973.onmicrosoft.com

Locations

Monitored locations

Teams

Conditions and percentage

Communication direction

Inbound, Outbound, Internal

Optical character recognition

Enabled

Conditions

Content matches any of these trainable classifiers: Harassment, Profanity, Threat, Adult images, Racy images, Gory images ; Content contains any of these sensitive info types: Taboo words

- Name
- Users and reviewers
- Locations
- Conditions and percentage
- Finish

Your policy was created

It might take up to 1 hour to activate your policy and up to 24 hours to start identifying communications.

Next steps

Monitor policy for matches and items pending review

Learn more

Investigate and remediate communication compliance alerts

Done

Communication compliance

Policies Alerts Reports

Create policy Refresh Export policy updates 22 items Search Customize c

Policy name	Reviewer	Items pending revi...	Escalated items	Resolved items	Status	Last modified	Last policy scan
Analyze MS Teams IM	AdeleV@M365x525973.OnMicrosoft.c...	0	0	0	Active	Apr 13, 2021 11:15 ...	Scan not available
profanity custom	admin@M365x525973.onmicrosoft.com	2	0	2	Active	Apr 5, 2021 1:34 AM	Apr 13, 2021 6:17 AM
SSN Policy	admin@M365x525973.onmicrosoft.com	5	0	0	Active	Mar 27, 2021 4:03 ...	Apr 13, 2021 4:28 AM
All ML and Custom Dict	admin@M365x525973.onmicrosoft.com	4	0	0	Active	Mar 30, 2021 10:38...	Apr 12, 2021 10:49 PM
SSN and Profanity	admin@M365x525973.onmicrosoft.com	1	0	0	Active	Mar 27, 2021 2:23 ...	Apr 13, 2021 4:54 AM
Offense SIT Dict ML	admin@M365x525973.onmicrosoft.com	5	0	0	Active	Mar 26, 2021 12:16...	Apr 13, 2021 12:50 AM
Sensitive Info Taboo Only	admin@M365x525973.onmicrosoft.com	17	0	0	Active	Mar 26, 2021 11:38...	Apr 13, 2021 1:29 AM
Offensive language ML and SIT - with O...	admin@M365x525973.onmicrosoft.com	8	0	0	Active	Mar 26, 2021 9:15 ...	Apr 13, 2021 4:13 AM
Offensive Language Non-Ocr	admin@M365x525973.onmicrosoft.com	11	0	0	Active	Mar 26, 2021 3:49 ...	Apr 12, 2021 11:41 PM
Offensive language ML and SIT	admin@M365x525973.onmicrosoft.com	7	0	0	Active	Mar 26, 2021 9:37 ...	Apr 13, 2021 5:29 AM
Offensive Language ML Only	admin@M365x525973.onmicrosoft.com	56	0	0	Active	Mar 25, 2021 2:55 ...	Apr 13, 2021 5:57 AM
Test globalized OCR support	admin@M365x525973.onmicrosoft.com	79	0	0	Active	Mar 18, 2021 11:49...	Apr 13, 2021 5:58 AM
Conflict of interest	admin@M365x525973.onmicrosoft.com	0	0	0	Active	Feb 4, 2021 9:48 PM	Apr 13, 2021 9:13 AM
Custom Test Policy OL	admin@M365x525973.onmicrosoft.com	1312	1	172	Active	Apr 6, 2021 8:35 AM	Apr 13, 2021 5:26 AM
Adult image detection	AdeleV@M365x525973.OnMicrosoft.c...	52	0	0	Active	Aug 10, 2020 10:00...	Apr 13, 2021 4:13 AM
Yammer msg only	admin@M365x525973.onmicrosoft.co...	18	1	1	Active	Feb 22, 2021 9:46 P...	Apr 13, 2021 3:12 AM
Privacy breach	supervisors@M365x525973.onmicros...	1904	3	4	Active	Jul 31, 2020 3:23 AM	Apr 13, 2021 5:21 AM
Top secret project	admin@M365x525973.OnMicrosoft.co...	465	1	26	Active	Mar 1, 2021 8:04 PM	Apr 13, 2021 4:32 AM

Monitor communications for conflict of interest

About this template

Set up a policy to monitor communications between two groups of users across locations like Exchange, Teams, and more. Just choose the two groups whose communications you want to supervise, specify reviewers, and we'll set up the rest.

Settings we need from you

Policy name *

Conflict of interest

Supervised group A *

LT Legal Team × Start typing to find users or groups

Supervised group B *

FT Finance Team × Start typing to find users or groups

Reviewers *

AV Adele Vance × Start typing to find users

Settings we've filled in for you

You can change these later. Click 'Customize policy' if you want to configure different settings now.

Communications to monitor

Monitored locations	Exchange, Teams, Skype for Business, Yammer

Conditions and percentage

Communication direction	Internal
Percentage to review	100

Create policy Customize policy ...

Offensive or threatening language

Overview | Pending (183) | Resolved (1)

Saved filter queries | Save the query | Clear all | Filters

Item class: **IPM.SkypeTeams.Message**

Resolve | Tag as | Notify | Escalate | Escalate for investigation | Near duplicates (3) | ...

Subject	Sender	Recipients	Date
	Christophe <a...	Lee Gu <LeeG...	Mar 8, 2021 7:48 ...
	Christophe <a...	Mark 8 Project...	Feb 9, 2021 9:50 ...
	Christophe <a...	Diego Siciliani...	Feb 9, 2021 9:45 ...
	Christophe <...	Lee Gu <LeeG...	Feb 9, 2021 9:45 ...
	Christophe <a...	Patti Fernande...	Feb 3, 2021 9:57 ...
	Christophe <a...	Diego Siciliani...	Feb 3, 2021 9:57 ...
	Christophe <a...	Christophe Fie...	Feb 3, 2021 6:43 ...
	Christophe <a...	Diego Siciliani...	Feb 3, 2021 6:32 ...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...

1 item selected. 61 items total.

Pattern detected. Recently, Christophe sent 3 messages matching this policy's conditions to Lee Gu.

Summary | Text view | Annotate view | Translate view | User history (42)

Christophe February 9, 2021, 8:45 PM

Ich werde dich und deine Pflanzen verletzen

Resolve | Tag as | ...

Offensive or threatening language

Overview | Pending (183) | Resolved (1)

Saved filter queries | Save the query | Clear all | Filters

Item class: **IPM.SkypeTeams.Message**

Resolve | Tag as | Notify | Escalate | Escalate for investigation | Near duplicates (3) | ...

Subject	Sender	Recipients	Date
	Christophe <a...	Lee Gu <LeeG...	Mar 8, 2021 7:48 ...
	Christophe <a...	Mark 8 Project...	Feb 9, 2021 9:50 ...
	Christophe <a...	Diego Siciliani...	Feb 9, 2021 9:45 ...
	Christophe <...	Lee Gu <LeeG...	Feb 9, 2021 9:45 ...
	Christophe <a...	Patti Fernande...	Feb 3, 2021 9:57 ...
	Christophe <a...	Diego Siciliani...	Feb 3, 2021 9:57 ...
	Christophe <a...	Christophe Fie...	Feb 3, 2021 6:43 ...
	Christophe <a...	Diego Siciliani...	Feb 3, 2021 6:32 ...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...

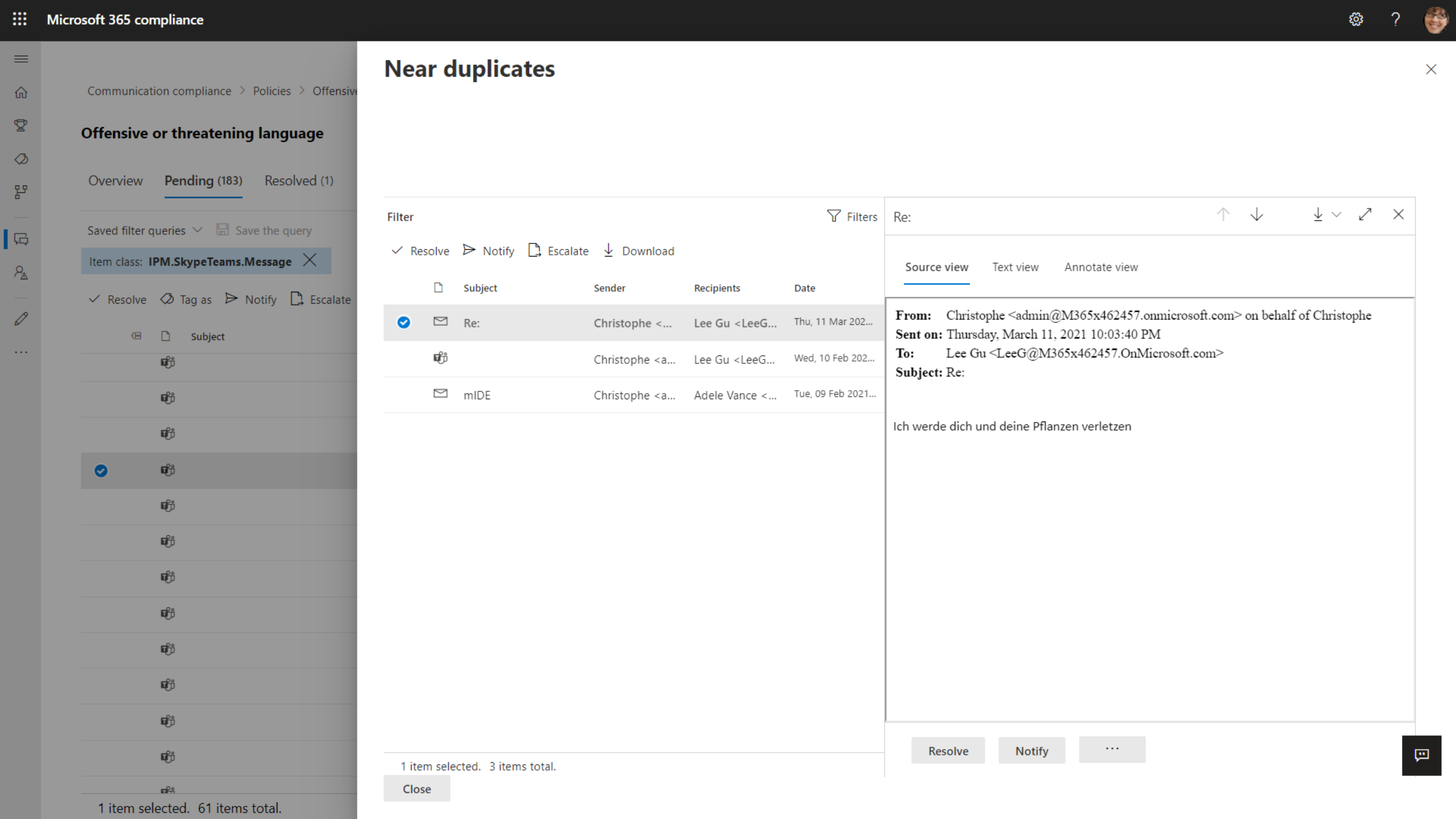
1 item selected. 61 items total.

Pattern detected. Recently, Christophe sent 3 messages matching this policy's conditions to Lee Gu.

Summary | Text view | Annotate view | Translate view | User history (42)

```
1
2  I will hurt you and your plants
3
4
```

Resolve | Tag as | ...


Microsoft 365 compliance
Communication compliance > Policies > Offensive
Offensive or threatening language
Overview
Pending (183)
Resolved (1)
Saved filter queries
Save the query
Item class: IPM.SkypeTeams.Message
Resolve
Tag as
Notify
Escalate
Subject
1 item selected. 61 items total.
Near duplicates
Filter
Filters
Resolve
Notify
Escalate
Download
Subject
Sender
Recipients
Date
Re:
Christophe <...
Lee Gu <LeeG...
Thu, 11 Mar 202...
Christophe <a...
Lee Gu <LeeG...
Wed, 10 Feb 202...
mIDE
Christophe <a...
Adele Vance <...
Tue, 09 Feb 2021...
1 item selected. 3 items total.
Close
Re:
Source view
Text view
Annotate view
From: Christophe <admin@M365x462457.onmicrosoft.com> on behalf of Christophe
Sent on: Thursday, March 11, 2021 10:03:40 PM
To: Lee Gu <LeeG@M365x462457.OnMicrosoft.com>
Subject: Re:
Ich werde dich und deine Pflanzen verletzen
Resolve
Notify
...

Offensive messages

Overview | Pending (327) | Resolved (110)

Saved filter queries | Save the query | Reset | Filters

Item class: Any

1 of 327 selected

Subject	Sender	Recipients	Date
Money Stuff: Libor Is Going Away for Real	Matt Levine <nore...	leeg@m365x52597...	Mar 8, 2021 10:28 ...
SANS NewsBites Vol. 23 Num. 018 : HAFNIUM Activel...	SANS NewsBites <...	leeg@m365x52597...	Mar 5, 2021 3:04 PM
c2	Christophe Fiessing...	Megan Bowen <M...	Mar 3, 2021 4:06 PM
	Christophe Fiessing...	Patti Fernandez <P...	Mar 3, 2021 4:06 PM
	Christophe Fiessing...	Diego Siciliani <Di...	Mar 3, 2021 4:04 PM
0-wus-d3-755a532739a21b3626b489df6eece1bd.jpg			
c	Christophe Fiessing...	Diego Siciliani <Di...	Mar 3, 2021 4:04 PM
	Christophe Fiessing...	Lynne Robbins <Ly...	Mar 2, 2021 2:23 PM
	Christophe Fiessing...	Lynne Robbins <Ly...	Mar 2, 2021 2:22 PM
	Christophe Fiessing...	Lynne Robbins <Ly...	Mar 2, 2021 2:22 PM
AA	Christophe Fiessing...	Lee Gu <LeeG@M3...	Mar 1, 2021 10:02 ...
Powell Was Just Gloomy Enough to Make Stocks Happy	John Authers <nor...	leeg@m365x52597...	Feb 23, 2021 11:41 ...

0-wus-d3-755a532739a21b3626b489df6eece1bd.jpg

Source view | Metadata

Resolve | Automate | Show Translate view

Offensive or threatening language

Overview | Pending (183) | Resolved (1)

Saved filter queries | Save the query | Clear all | Filters

Item class: **IPM.SkypeTeams.Message**

Resolve | Tag as | Notify | Escalate | Escalate for investigation | Near duplicates (3) | ...

Subject	Sender	Recipients	Date
	Christophe <a...	Patti Fernande...	Mar 8, 2021 7:49 ...
	Christophe <a...	Lee Gu <LeeG...	Mar 8, 2021 7:48 ...
	Christophe <a...	Mark 8 Project...	Feb 9, 2021 9:50 ...
	Christophe <a...	Diego Siciliani...	Feb 9, 2021 9:45 ...
	Christophe <...	Lee Gu <LeeG...	Feb 9, 2021 9:45 ...
	Christophe <a...	Patti Fernande...	Feb 3, 2021 9:57 ...
	Christophe <a...	Diego Siciliani...	Feb 3, 2021 9:57 ...
	Christophe <a...	Christophe Fie...	Feb 3, 2021 6:43 ...
	Christophe <a...	Diego Siciliani...	Feb 3, 2021 6:32 ...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...
	Christophe <a...	Diego Siciliani...	Jan 27, 2021 12:3...

Pattern detected. Recently, Christophe sent 3 messages matching this policy's conditions to Lee Gu.

Summary | Text view | Annotate view | Translate view | User history (50)

Christophe

Recent policy matches and remediation actions

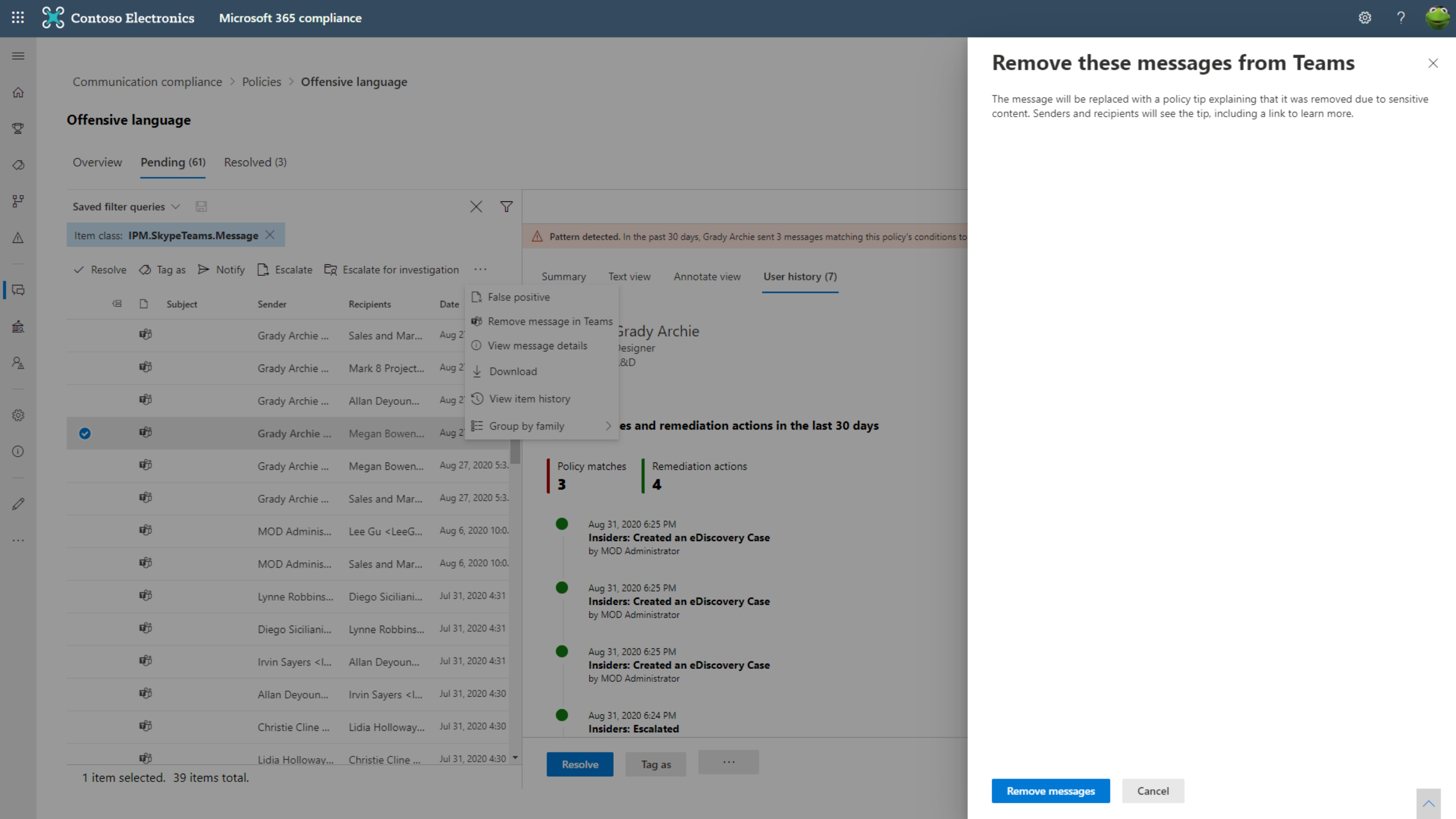
Policy matches	Remediation actions
3	47

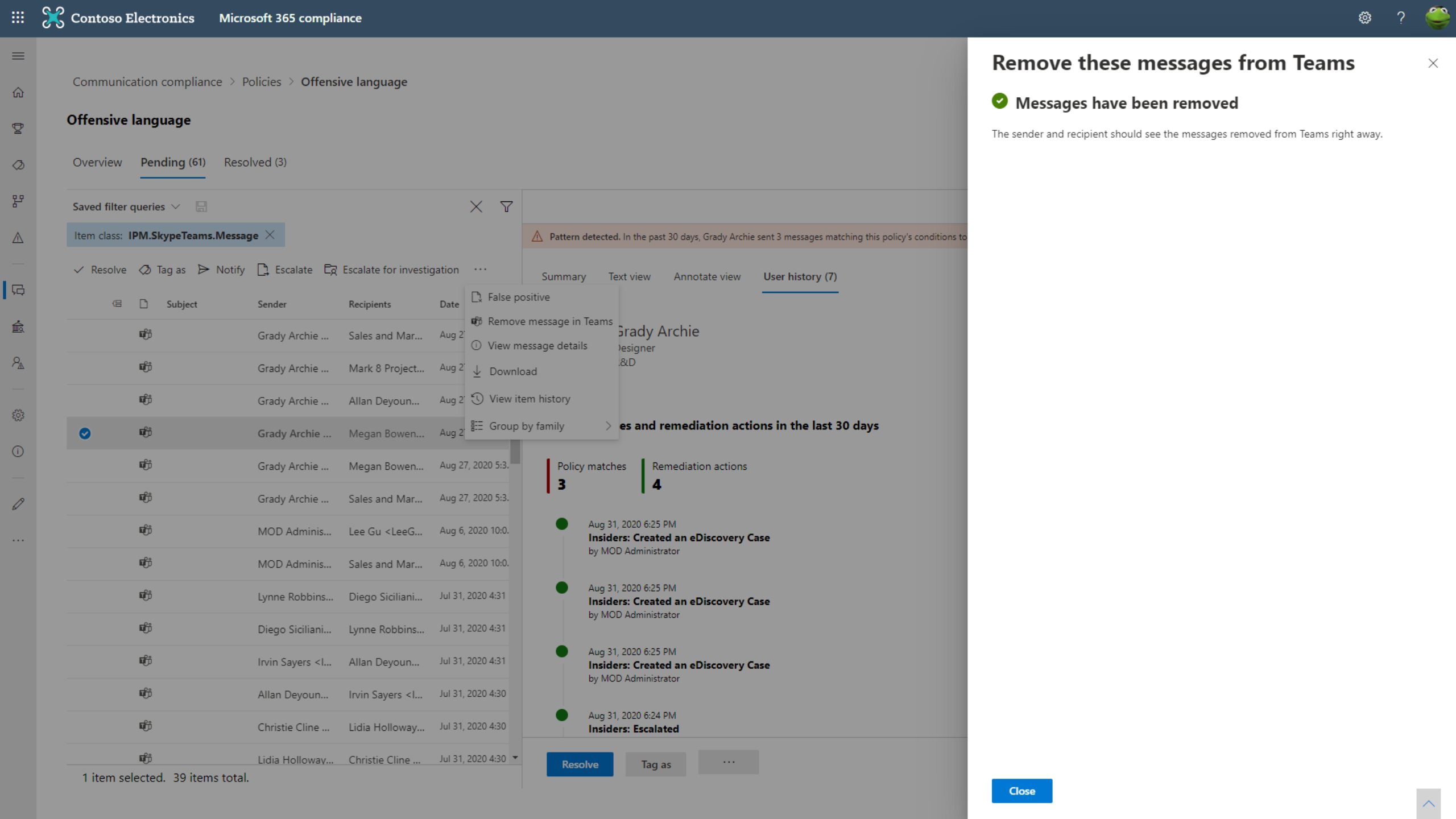
Apr 5, 2021 6:06 PM
Policy match in Teams message

Apr 5, 2021 5:56 PM
Policy match in Email "MLFP1"

Mar 25, 2021 2:34 PM
Policy match in Teams message

Mar 5, 2021 9:39 AM
Adult images: Message removed from Teams
by Christophe


Contoso Electronics
Microsoft 365 compliance
Communication compliance > Policies > Offensive language
Offensive language
Overview
Pending (61)
Resolved (3)
Saved filter queries
Item class: IPM.SkypeTeams.Message
Resolve
Tag as
Notify
Escalate
Escalate for investigation
False positive
Remove message in Teams
View message details
Download
View item history
Group by family
Subject
Sender
Recipients
Date
1 item selected. 39 items total.
Pattern detected. In the past 30 days, Grady Archie sent 3 messages matching this policy's conditions to
Summary
Text view
Annotate view
User history (7)
Policy matches
3
Remediation actions
4
Aug 31, 2020 6:25 PM
Insiders: Created an eDiscovery Case
by MOD Administrator
Aug 31, 2020 6:24 PM
Insiders: Escalated
Resolve
Tag as
Remove these messages from Teams
The message will be replaced with a policy tip explaining that it was removed due to sensitive content. Senders and recipients will see the tip, including a link to learn more.
Remove messages
Cancel


Contoso Electronics
Microsoft 365 compliance
Communication compliance > Policies > Offensive language
Offensive language
Overview
Pending (61)
Resolved (3)
Saved filter queries
Item class: IPM.SkypeTeams.Message
Resolve
Tag as
Notify
Escalate
Escalate for investigation
Subject
Sender
Recipients
Date
False positive
Remove message in Teams
View message details
Download
View item history
Group by family
1 item selected. 39 items total.
Pattern detected. In the past 30 days, Grady Archie sent 3 messages matching this policy's conditions to
Summary
Text view
Annotate view
User history (7)
Policy matches
3
Remediation actions
4
Aug 31, 2020 6:25 PM
Insiders: Created an eDiscovery Case
by MOD Administrator
Aug 31, 2020 6:24 PM
Insiders: Escalated
Resolve
Tag as
Remove these messages from Teams
Messages have been removed
The sender and recipient should see the messages removed from Teams right away.
Close

Microsoft Teams

Search

Activity
Chat
Teams
Calendar
Calls
Files
...
Apps
Help

Chat

Recent

Allan Deyoung 11:44 AM

Lee Gu 10:34 AM
You: you're so dumb

Patti Fernandez 10:33 AM
You: I'm going to jump off the roof

Miriam Graham 9:38 AM
You: how can you be so dumb and stupid

Megan Bowen 9:26 AM
You: I hate you, stupid! GIF

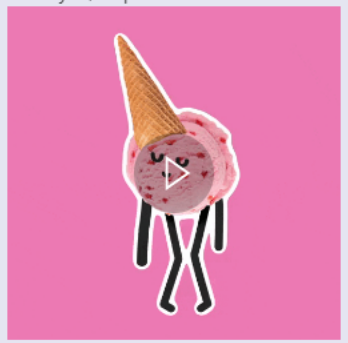
Megan Bowen Chat Files Organization Activity +

8/27 5:38 PM
you're so dumb

This message was blocked. What can I do?
i'll hurt you

Today

9:26 AM
I hate you, stupid!



Type a new message

Microsoft Teams

Search

Activity
Chat 2
Teams
Calendar
Calls
Files
...
Apps
Help

Chat

Recent

Grady Archie 9:26 AM
I hate you, stupid! GIF

Alex Wilber 7/31
Alex: Please give final review by EOD so we c...

Isaiah Langer 7/31
Isaiah: Hey Megs! I just wanted to volunteer t...

Grady Archie Chat Files Organization Activity +

Grady Archie 8/27 5:38 PM
you're so dumb

This message was blocked due to organization policy. What's this?

Today

Grady Archie 9:26 AM
I hate you, stupid!

Type a new message

Adult images

Overview | Pending (8) | Resolved (0)

Resolve | Tag as | Notify | Escalate | Escalate for investigation | ...

	Subject	Sender	Recipients	Date
	acs3	Grady Archie ...	Allan Deyoun...	Aug 31, 2020 11:...
✓		Grady Archie ...	Allan Deyoun...	Aug 31, 2020 11:...
	acs2	Grady Archie ...	Lee Gu <LeeG...	Aug 31, 2020 11:...
	acs1	Grady Archie ...	Lee Gu <LeeG...	Aug 31, 2020 11:...

1 item selected. 8 items total.

Pattern detected. In the past 30 days, Grady Archie sent 2 messages matching this policy's conditions to Allan Deyoung.

Summary | Text view | Annotate view | User history (2)

Grady Archie August 31, 2020, 11:44 AM

IMG_20161012_074007_734.jpg

Resolve | Tag as | ...

Offensive language

Overview | Pending (12) | Resolved (0)

Resolve | Tag as | Notify | Escalate | Escalate for investigation | ...

		Subject	Sender	Recipients	Date
✓			MOD Admini...	Patti Fernand...	Aug 2
			MOD Adminis...	Patti Fernande...	Aug 2
			MOD Adminis...	Mark 8 Project...	Aug 2
			MOD Adminis...	Digital Initiativ...	Aug 2
			MOD Adminis...	Sales and Mar...	Aug 2
			MOD Adminis...	Alex Wilber <...	Aug 27, 2020 5:2...
			MOD Adminis...	Grady Archie ...	Aug 27, 2020 5:2...
			MOD Adminis...	Grady Archie ...	Aug 27, 2020 5:2...
			MOD Adminis...	Grady Archie ...	Aug 27, 2020 5:2...
		Test	MOD Adminis...	Allan Deyoun...	Aug 27, 2020 5:2...

1 item selected. 12 items total.

- False positive
- Remove message in Teams
- Power Automate
- View message details
- Improve classification
- Download
- View item history
- Group by family

Summary | Text view | Annotate view | User history (0)

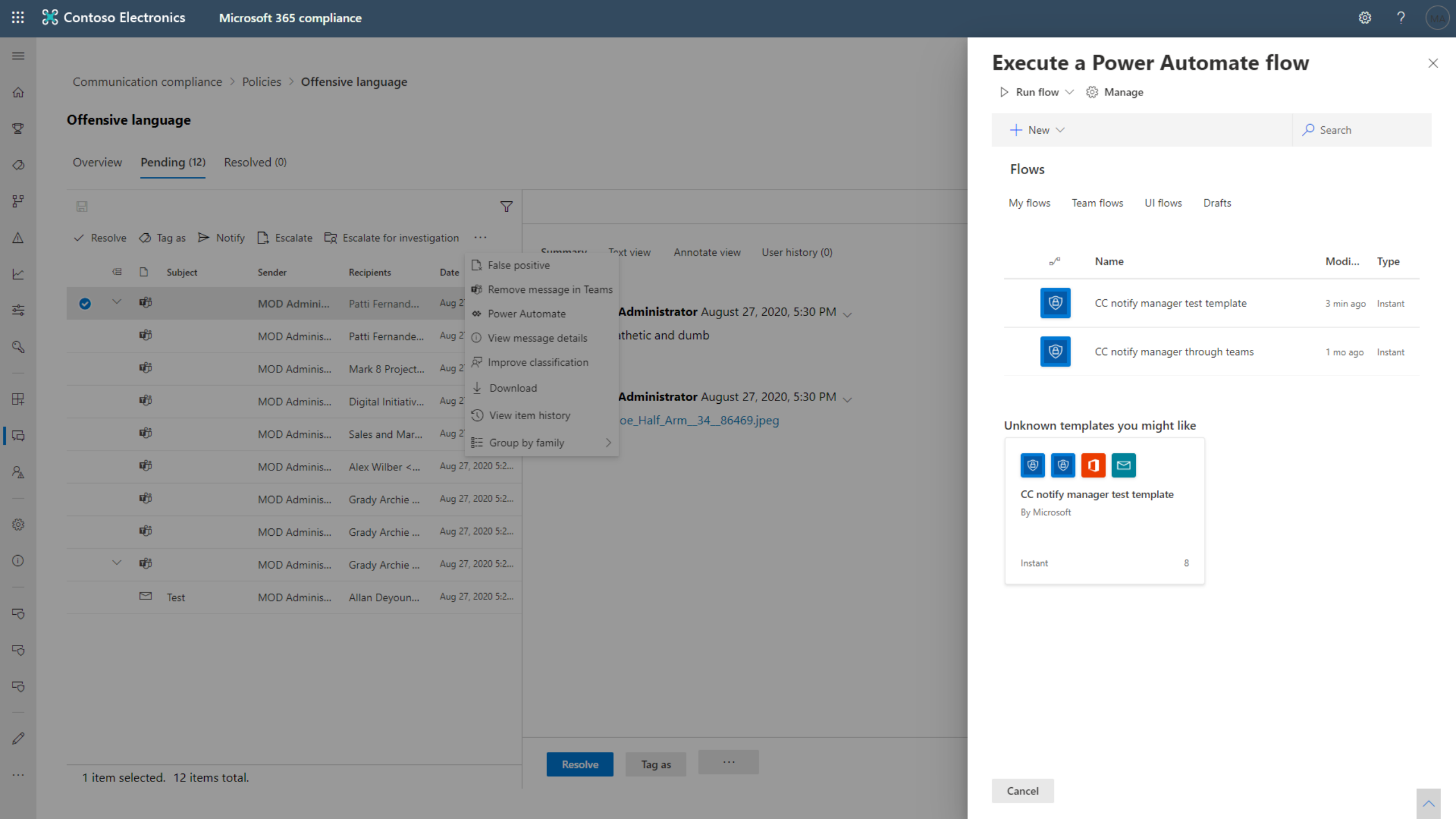
Administrator August 27, 2020, 5:30 PM

thetic and dumb

Administrator August 27, 2020, 5:30 PM

oe_Half_Arm__34__86469.jpeg

Resolve | Tag as | ...


Contoso Electronics
Microsoft 365 compliance
Communication compliance > Policies > Offensive language
Offensive language
Overview
Pending (12)
Resolved (0)
Resolve
Tag as
Notify
Escalate
Escalate for investigation
False positive
Remove message in Teams
Power Automate
View message details
Improve classification
Download
View item history
Group by family
Summary
Text view
Annotate view
User history (0)
Subject
Sender
Recipients
Date
Test
1 item selected. 12 items total.
Resolve
Tag as
Execute a Power Automate flow
Run flow
Manage
New
Search
Flows
My flows
Team flows
UI flows
Drafts
Name
Modi...
Type
CC notify manager test template
3 min ago
Instant
CC notify manager through teams
1 mo ago
Instant
Unknown templates you might like
CC notify manager test template
By Microsoft
Instant
8
Cancel

Contoso Electronics Microsoft 365 compliance

Communication compliance > Policies > Offensive language

Offensive language

Overview Pending (12) Resolved (0)

Resolve Tag as Notify Escalate Escalate for investigation ...

Subject	Sender	Recipients	Date
	MOD Admini...	Patti Fernand...	Aug 2
	MOD Adminis...	Patti Fernande...	Aug 2
	MOD Adminis...	Mark 8 Project...	Aug 2
	MOD Adminis...	Digital Initiativ...	Aug 2
	MOD Adminis...	Sales and Mar...	Aug 2
	MOD Adminis...	Alex Wilber <...	Aug 27, 2020 5:2...
	MOD Adminis...	Grady Archie ...	Aug 27, 2020 5:2...
	MOD Adminis...	Grady Archie ...	Aug 27, 2020 5:2...
	MOD Adminis...	Grady Archie ...	Aug 27, 2020 5:2...
Test	MOD Adminis...	Allan Deyoun...	Aug 27, 2020 5:2...

1 item selected. 12 items total.

- False positive
- Remove message in Teams
- Power Automate
- View message details
- Improve classification
- Download
- View item history
- Group by family

Summary Text view Annotate view User history (0)

Administrator August 27, 2020, 5:30 PM

thetic and dumb

Administrator August 27, 2020, 5:30 PM

oe_Half_Arm__34__86469.jpeg

Resolve Tag as ...

Execute a Power Automate flow

Run flow Manage

CC notify manager test template

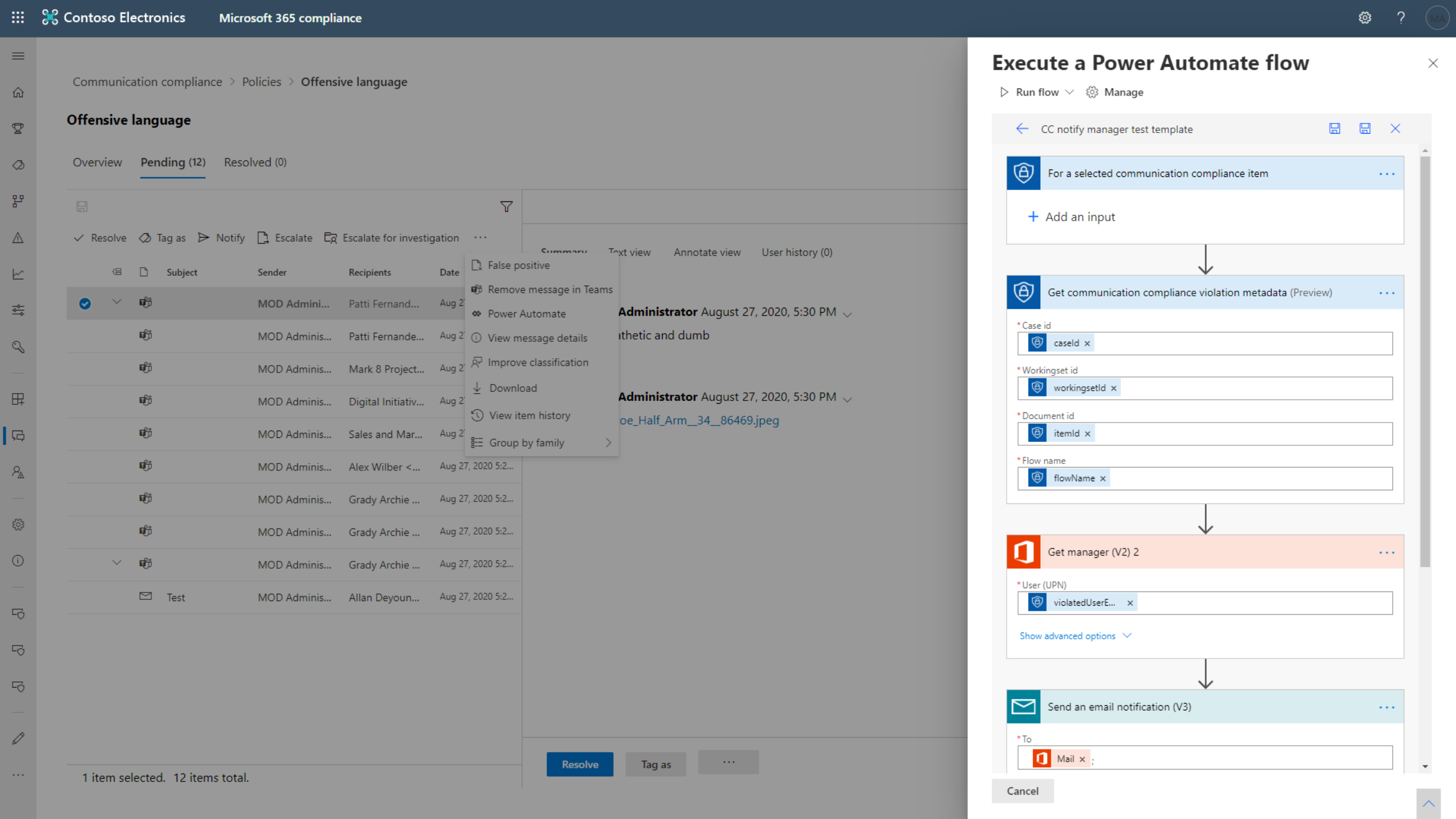
CC notify manager test template

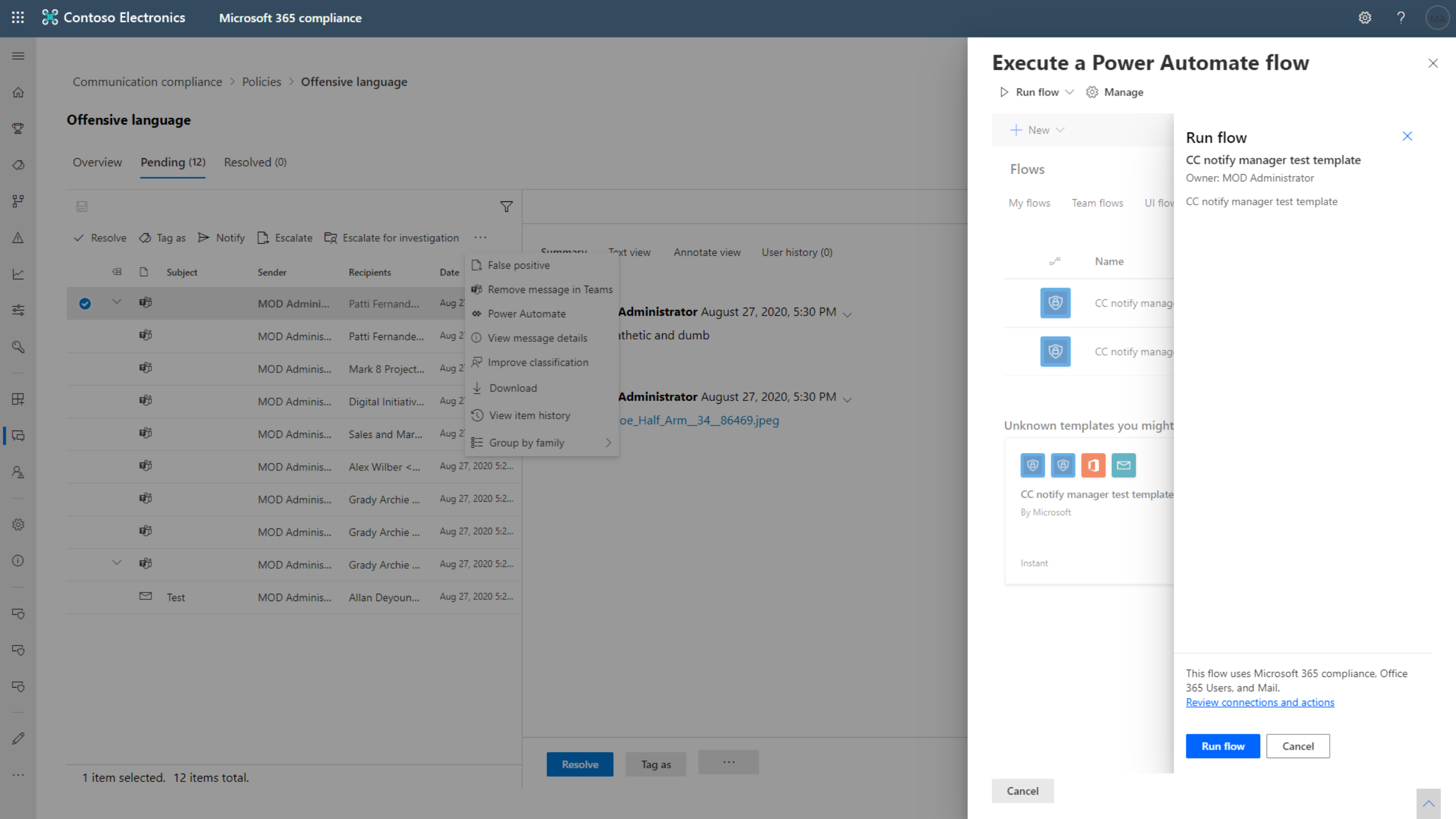
This flow will connect to:

Microsoft 365 compliance	admin@M365x65006...	
Office 365 Users Permissions	admin@M365x65006...	
Mail	Mail	

Continue

Cancel


Contoso Electronics
Microsoft 365 compliance
Communication compliance > Policies > Offensive language
Offensive language
Overview
Pending (12)
Resolved (0)
Resolve
Tag as
Notify
Escalate
Escalate for investigation
False positive
Remove message in Teams
Power Automate
View message details
Improve classification
Download
View item history
Group by family
Subject
Sender
Recipients
Date
Summary
Text view
Annotate view
User history (0)
Administrator August 27, 2020, 5:30 PM
Administrator August 27, 2020, 5:30 PM
1 item selected. 12 items total.
Resolve
Tag as
Execute a Power Automate flow
Run flow
Manage
CC notify manager test template
For a selected communication compliance item
Add an input
Get communication compliance violation metadata (Preview)
Case id
caseId
Workingset id
workingsetId
Document id
itemId
Flow name
flowName
Get manager (V2) 2
User (UPN)
violatedUserE...
Show advanced options
Send an email notification (V3)
To
Mail
Cancel


Contoso Electronics
Microsoft 365 compliance
Communication compliance > Policies > Offensive language
Offensive language
Overview
Pending (12)
Resolved (0)
Resolve
Tag as
Notify
Escalate
Escalate for investigation
False positive
Remove message in Teams
Power Automate
View message details
Improve classification
Download
View item history
Group by family
Summary
Text view
Annotate view
User history (0)
Subject
Sender
Recipients
Date
MOD Adminis...
Patti Fernand...
Patti Fernande...
Mark 8 Project...
Digital Initiativ...
Sales and Mar...
Alex Wilber <...
Grady Archie ...
Test
Allan Deyoun...
Aug 27, 2020 5:2...
Administrator August 27, 2020, 5:30 PM
thetic and dumb
Administrator August 27, 2020, 5:30 PM
oe_Half_Arm__34__86469.jpeg
1 item selected. 12 items total.
Resolve
Tag as
Execute a Power Automate flow
Run flow
Manage
New
Flows
My flows
Team flows
Name
CC notify manag
CC notify manag
Unknown templates you might
CC notify manager test template
By Microsoft
Instant
Run flow
CC notify manager test template
Owner: MOD Administrator
CC notify manager test template
This flow uses Microsoft 365 compliance, Office 365 Users, and Mail.
Review connections and actions
Run flow
Cancel
Cancel

Home
Compliance score
Data classification
Data connectors
Alerts

Solutions

Communication compliance
eDiscovery
Insider risk management

Settings
More resources

Customize navigation
Show all

Communication compliance

Communication compliance settings | Remove from navigation

Policies | Alerts | Reports

Create policy | Refresh | Export policy updates | 8 items | Search

Policy name	Reviewer	Items pending revi...	Escalated items	Resolved items	Status	Last modified
ThirdParty Whatsapp OL	AdeleV@M365x462457.OnMicrosoft.com, ...	0	0	0	Active	Aug 30, 2020 11:02...
ThridParty Whatsapp	AdeleV@M365x462457.OnMicrosoft.com, ...	0	0	0	Active	Aug 30, 2020 10:58...
Adult images	admin@M365x462457.onmicrosoft.com, ...	0	0	0	Active	Aug 27, 2020 5:43 ...
Yammer msgs only	AdeleV@M365x462457.OnMicrosoft.com, ...	11	0	0	Active	Aug 7, 2020 4:49 PM
Confidential project	AdeleV@M365x462457.OnMicrosoft.com, ...	0	0	0	Active	Aug 31, 2020 12:03...
Teams msgs only	admin@M365x462457.onmicrosoft.com, ...	230	11	0	Active	Aug 7, 2020 5:08 PM
Insiders	admin@M365x462457.OnMicrosoft.com, ...	62	3	2	Active	Aug 31, 2020 11:36...
Offensive language	admin@M365x462457.OnMicrosoft.com, ...	61	1	3	Active	Aug 31, 2020 2:17 ...

Recommended policies

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.

View

Monitor for sensitive info

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

View

Monitor for financial regulatory compliance

Add a policy that monitors communications that might contain info related to insider trading.

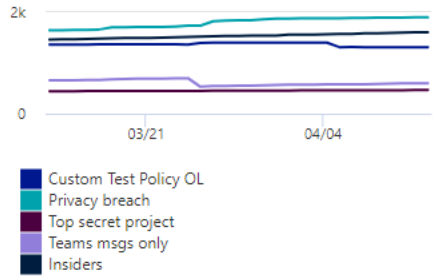
View

Communication compliance

Policies | Alerts | Reports

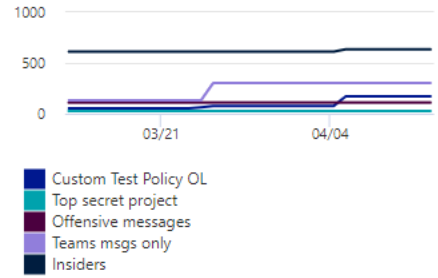
Recent policy matches

Last 30 days, updated 12:32 PM today



Resolved items by policy

Last 30 days, updated 12:32 PM today



Policies with most matches

Updated 12:32 pm today

Policy name	Total matches
Privacy breach	1904
Insiders	1604
Custom Test Policy OL	1312

Users with most policy matches

Last 30 days, updated 12:32 PM today

Display name	Matches
Christophe Fiessinger	191
RSS	74
Christophe Fiessinger in Tea...	35

Escalations by policy

Last 30 days, updated 12:32 PM today

Policy	Escalations
Insiders	14
Offensive messages	9
Privacy breach	3
Custom Test Policy OL	1

Detailed reports (4)

Policy settings and status

Review and export policy details like configuration settings, status, total matches, items reviewed or pending review, and more.

View details

Items and actions per policy

Review and export matching items and remediation actions per policy.

View details

Items and actions per location

Review and export matching items and remediation actions per Microsoft 365 location.

View details

Export Refresh

Policy name	Users or groups	Locations	Conditions	Review Percentage	Revie
Analyze MS Teams IM	AllUsersGroupsOfTenant	TeamsChats	3 conditions	100	Adele
profanity custom	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	2 conditions	100	admi
SSN Policy	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	2 conditions	100	admi
All ML and Custom Dict	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
SSN and Profanity	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
Offense SIT Dict ML	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
Sensitive Info Taboo Only	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	2 conditions	100	admi
Offensive language ML and SIT ...	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
Offensive Language Non-Ocr	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
Offensive language ML and SIT	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
Offensive Language ML Only	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	2 conditions	100	admi
Test globalized OCR support	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer	3 conditions	100	admi
Conflict of interest	FinanceTeam@M365x525973.OnMicrosoft.com, SalesTea...	Exchange, TeamsChats, SkypeForBusiness, Yammer	1 conditions	100	admi
Custom Test Policy OL	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer, Bloo...	2 conditions	100	admi
Adult image detection	AllUsersGroupsOfTenant	Exchange, TeamsChats, SkypeForBusiness, Yammer, Bloo...	2 conditions	100	Adele
Yammer msg only	AllUsersGroupsOfTenant	Yammer	1 conditions	100	admi
Privacy breach	Employees@M365x525973.OnMicrosoft.com	Exchange, TeamsChats, SkypeForBusiness, Bloomberg	2 conditions	100	super
Top secret project	Employees@M365x525973.OnMicrosoft.com, SalesAndM...	Exchange, TeamsChats, SkypeForBusiness, Yammer, Bloo...	2 conditions	100	admi

Customize columns

Select columns

- [x] Policy name
- [x] Users or groups
- [x] Locations
- [x] Conditions
- [x] Review Percentage
- [x] Reviewers
- [x] Status
- [ ] Items matched
- [ ] Items pending review
- [ ] Escalated items
- [ ] Resolved items
- [x] Last modified

Apply Cancel

Policy settings and st....csv
Open file

Show all

Export

18 items Customize columns

Filters: Choose a date range: 2/13/2021-4/13/2021

Policy name	Policy Id	Items matched	Escalated items	Resolved items	Compliant	Non-Compliant	Questionable	Items pending review	User notified	Case created
Privacy breach	c05a4628-3991-4940-a959-47ed14fea028	47	0	0	0	0	0	47	0	0
Top secret project	6038cea2-c731-4925-a774-420af7607daa	59	0	0	0	0	0	59	0	0
Insiders	e97deed4-68af-4acb-9c04-38a020a2602c	301	0	1	0	0	0	300	1	1
Teams msgs only	e11ba14e-7890-4b1b-bc98-c1440a93326f	132	0	109	0	0	0	23	0	0
Custom Test Policy OL	e3db73fe-a7ca-451d-933f-2bd3fcb30ec6	11	0	20	0	0	0	0	2	0
Offensive messages	0baae255-c7a3-4280-a944-82dcd9bf1c72	73	0	0	0	0	0	73	0	0
Yammer msg only	6ac6be81-1029-4513-8f1c-37e489464e53	5	0	0	0	0	0	5	0	0
Adult image detection	b7e21fd5-ba8a-45d2-8df7-d451853e71c5	3	0	0	0	0	0	3	0	0
Test globalized OCR support	088848d6-67ef-49b1-ab17-a2aafbbdde80	7	0	0	0	0	0	7	0	0
Offensive language ML and SIT - with OCR	61bb3833-2e75-41ea-97f4-f28bc2480898	8	0	0	0	0	0	8	0	0
Offensive language ML and SIT	68aa391e-df34-4689-9940-3708a4763cbe	6	0	0	0	0	0	6	0	0
Offense SIT Dict ML	857393b5-35d2-4601-8bd4-e1e065ba07e7	4	0	0	0	0	0	4	0	0
Sensitive Info Taboo Only	2c2437fc-bdf7-4e6d-80c2-cb2e96cbcddc	17	0	0	0	0	0	17	0	0
Offensive Language Non-Ocr	53b059a6-0450-47a2-82b0-13af142398c9	4	0	0	0	0	0	4	0	0
Offensive Language ML Only	c7395475-2c9a-49a9-834e-0dc06ad35c6e	1	0	0	0	0	0	1	0	0
All ML and Custom Dict	79a1397f-b0be-4bd0-bd93-08336abac11f	4	0	0	0	0	0	4	0	0
SSN Policy	6fcaa2cb-9824-4688-9ddc-1daa2787e78b	5	0	0	0	0	0	5	0	0
profanity custom	a2d3c3a2-5f1c-4edf-855c-f64889955f79	4	0	2	0	0	0	2	0	0

Export

21 items Customize columns

Filters: Choose a date range: 2/13/2021-4/13/2021

User	Items pending review	Resolved items	Compliant	Non-Compliant	Questionable	User notified	Escalated items	Case created
noreply@mail.bloombergbusiness.com	142	2	0	1	0	0	0	0
RSS@teams.microsoft.com	84	69	0	0	0	2	0	0
noreply@mail.bloombergview.com	139	3	0	0	0	0	0	0
sans@email.sans.org	17	0	0	0	0	0	0	0
consensussecurityvulnerabilityalert@email.sans.org	10	0	0	0	0	0	0	0
no-reply@microsoft.com	4	0	0	0	0	0	0	0
noreply@email.teams.microsoft.com	64	5	0	0	0	0	0	0
admin@M365x525973.onmicrosoft.com	225	80	0	0	0	1	0	
notifications+3pjurw3f@yammer.com	1	0	0	0	0	0	0	0
notifications+qod3y4ug@yammer.com	1	0	0	0	0	0	0	0
notifications+1bwnzoa8@yammer.com	1	0	0	0	0	0	0	0
mcc365@microsoft.com	38	0	0	0	0	0	0	0
newsbites@email.sans.org	6	1	0	0	0	0	0	0
LSpitzner@email.sans.org	1	1	0	0	0	0	0	0
powerautomate@email2.microsoft.com	1	0	0	0	0	0	0	0
flow-noreply@microsoft.com	2	0	0	0	0	0	0	0
postmaster@M365x525973.onmicrosoft.com	1	0	0	0	0	0	0	0
admin@M365x462457.onmicrosoft.com	0	1	0	0	0	0	0	0
azure-noreply@microsoft.com	0	4	0	0	0	0	0	0

Phases & actions

Create & tune policies

- Pre-configured playbooks
- Custom policy creation
- Power Automate flow

Audit

- Alerts
- Productivity reports
- Audit

Identify violations

- Tag and comment
- Document review
- User history

Resolve violations

- Resolve
- Notify
- Escalate
- Remove message from Teams
- Compliance solution handoff

Communication Compliance

Identify risky communications that violate regulatory compliance and code of conduct policies

Enrich with additional solutions:

Data loss prevention

Alerts: Inform DLP policies based on recent Communication Compliance violations

Information protection

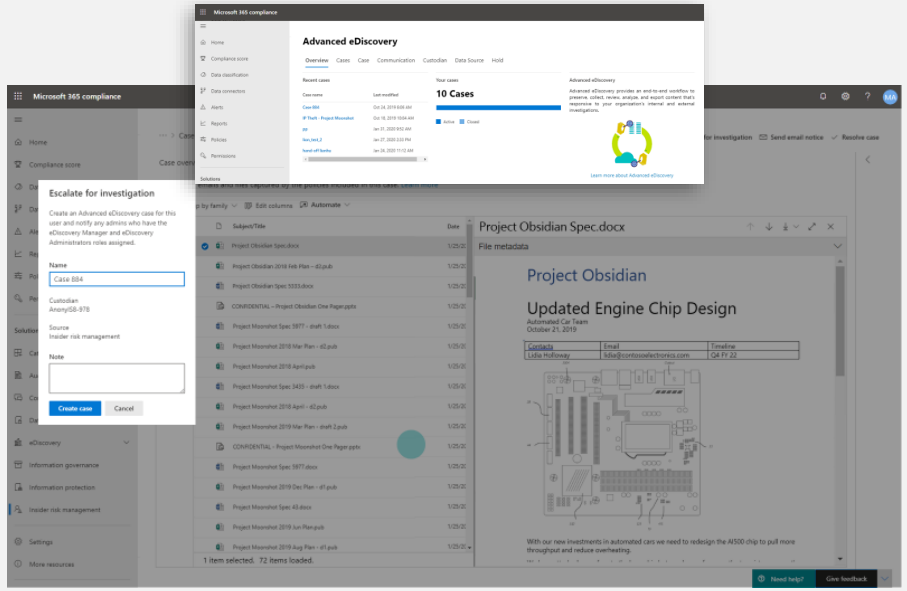
Enrichment: Expand Information Protection labels and built-in sensitive data types based on custom SITs

Insider Risk Management

Sentiment analysis: Identify a user as higher risk based on recent communication patterns

Advanced eDiscovery

Legal collaboration: Escalate policy violations via seamless investigation handoff



Communication Compliance next steps

Configure policies

Investigate & remediate messages

Give us feedback

Key resources	
Ignite sessions	aka.ms/VideoHub/InsiderRiskManagement
Documentation	aka.ms/CommunicationCompliance
Latest announcement	aka.ms/ccrsa2021
Start a trial	Microsoft 365 E5 trial
Roadmap	office.com/roadmap

Microsoft

Data Connectors

Bring in 3P data & create value with M365 Compliance solutions

Data connectors

Bring in non-Microsoft data and benefit from Microsoft compliance value

One catalog for all connectors

Discover connectors built by Microsoft and partners (TeleMessage and Veritas) in one place

Simplified deployment and monitoring

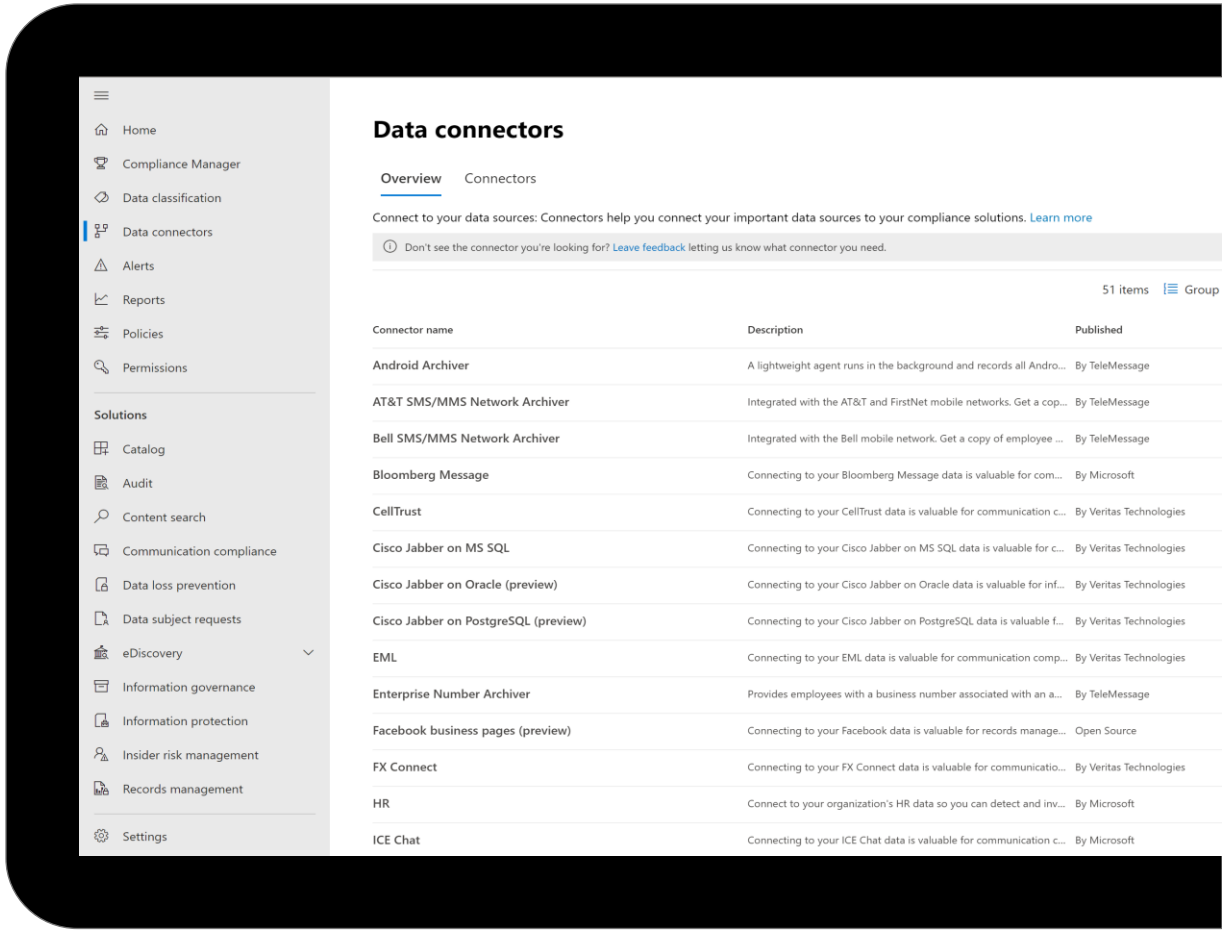
Few clicks to setup data import for most connectors**

Data available for all compliance solutions

Hi-fidelity data ingestion available for all compliance solutions

Built-in connectors for various categories

41 built-in connectors including Bloomberg Message, Slack eDiscovery, Zoom Meetings, Webex, Twitter etc.



*** Connectors by third party vendors requires purchasing the subscription directly with the vendor before deployment.*

41 pre-built connectors available in Microsoft 365 compliance center

2019

Instant Bloomberg	*Facebook*
LinkedIn	*Twitter*

2021

Our connector partners

- Veritas
- TeleMessage

Social

- Facebook
- Twitter
- LinkedIn

Finance

- Instant Bloomberg
- Bloomberg Message
- ICE Chat
- Symphony
- FX Connect
- Thomson Reuters Eikon

IM/ Collaboration

- Slack
- Zoom Meetings
- Facebook Workplace
- Webex Teams
- *Cisco Jabber*

Mobile/Text

- WhatsApp Archiver
- Android Archiver
- AT&T
- Verizon
- Bell Network
- O_2 Telefónica
- Telus
- Enterprise Number Archiver

Other

- HR Connector
- *Physical badging systems*
- Generic text delimited importer
- Generic email importer

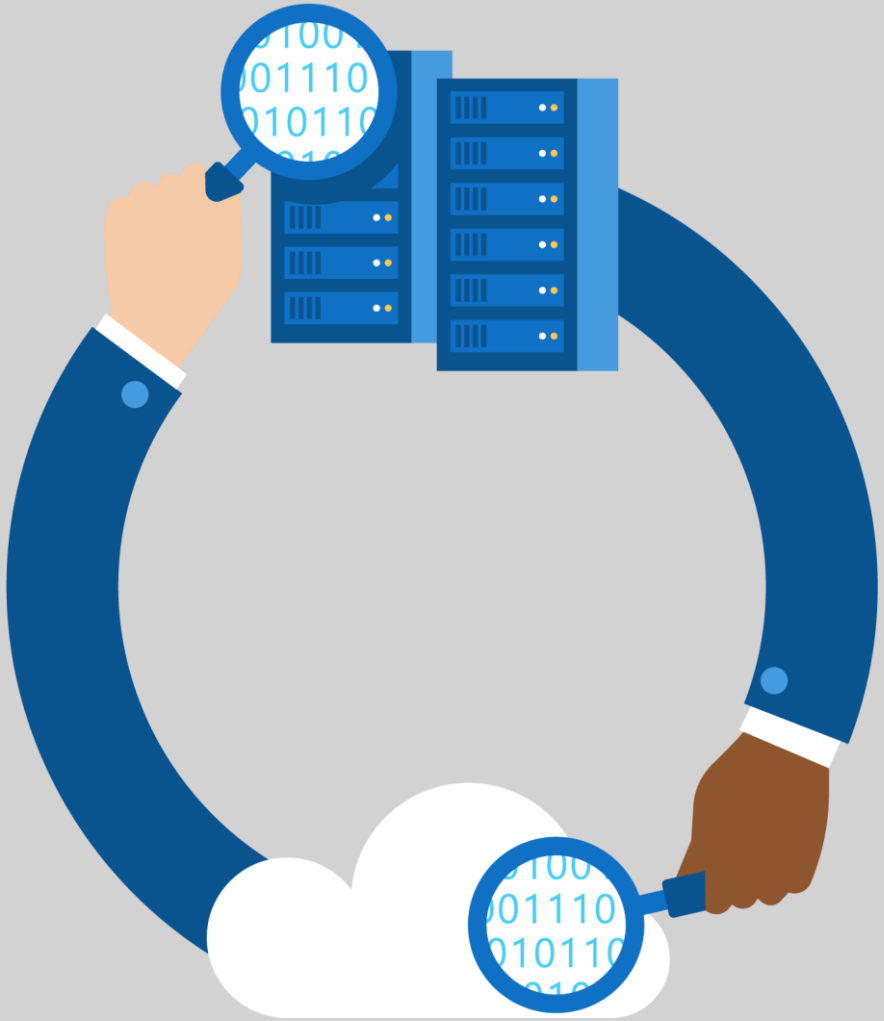
*Pre-built data connectors include connectors built by Microsoft and by partners - TeleMessage and Veritas. Except for TeleMessage and Veritas, Microsoft does not have direct relationships with the data source companies in bringing these data connectors to the platform.

Facebook, Twitter, Physical Badging and Cisco Jabber on PostgresSQL/Oracle are in public preview now.

Microsoft

Data Connectors

Demo



Data connectors

Overview | Connectors

Connect to your data sources: Connectors help you connect your important data sources to your compliance solutions. Learn more

Don't see the connector you're looking for? Leave feedback letting us know what connector you need.

51 items | Group | Filter | Search

Connector name	Description	Published	Category
Android Archiver	A lightweight agent runs in the background and records all Andro...	By TeleMessage	Instant Messaging
AT&T SMS/MMS Network Archiver	Integrated with the AT&T and FirstNet mobile networks. Get a cop...	By TeleMessage	Instant Messaging
Bell SMS/MMS Network Archiver	Integrated with the Bell mobile network. Get a copy of employee ...	By TeleMessage	Instant Messaging
Bloomberg Message	Connecting to your Bloomberg Message data is valuable for com...	By Microsoft	Mail
CellTrust	Connecting to your CellTrust data is valuable for communication c...	By Veritas Technologies	Instant Messaging
Cisco Jabber on MS SQL	Connecting to your Cisco Jabber on MS SQL data is valuable for c...	By Veritas Technologies	Instant Messaging
Cisco Jabber on Oracle (preview)	Connecting to your Cisco Jabber on Oracle data is valuable for inf...	By Veritas Technologies	Instant Messaging
Cisco Jabber on PostgreSQL (preview)	Connecting to your Cisco Jabber on PostgreSQL data is valuable f...	By Veritas Technologies	Instant Messaging
EML	Connecting to your EML data is valuable for communication comp...	By Veritas Technologies	Others
Enterprise Number Archiver	Provides employees with a business number associated with an a...	By TeleMessage	Instant Messaging
Facebook business pages (preview)	Connecting to your Facebook data is valuable for records manage...	Open Source	Social
FX Connect	Connecting to your FX Connect data is valuable for communicatio...	By Veritas Technologies	Instant Messaging
HR	Connect to your organization's HR data so you can detect and inv...	By Microsoft	HR
ICE Chat	Connecting to your ICE Chat data is valuable for communication c...	By Microsoft	Instant Messaging

Data connectors

Overview | Connectors

Connect to your data sources: Connectors help you connect your important data sources to your compliance solutions. Learn more

Don't see the connector you're looking for? Leave feedback letting us know what connector you need.

17 items | Group | Filter | Search

Filters: Published: By TeleMessage

Connector name	Description	Published	Category
Android Archiver	A lightweight agent runs in the background and records all Andro...	By TeleMessage	Instant Messaging
AT&T SMS/MMS Network Archiver	Integrated with the AT&T and FirstNet mobile networks. Get a cop...	By TeleMessage	Instant Messaging
Bell SMS/MMS Network Archiver	Integrated with the Bell mobile network. Get a copy of employee ...	By TeleMessage	Instant Messaging
Enterprise Number Archiver	Provides employees with a business number associated with an a...	By TeleMessage	Instant Messaging
O2 SMS and Voice Network Archiver	Integrated with the O2 UK mobile network. Get a copy of employe...	By TeleMessage	Instant Messaging
Rogers SMS/MMS Network Archiver (INTEGRATION) (preview)	Integrated with the Rogers mobile network. Get a copy of employ...	By TeleMessage	Instant Messaging
Rogers SMS/MMS Network Archiver (preview)	Integrated with the Rogers mobile network. Get a copy of employ...	By TeleMessage	Instant Messaging
Signal Archiver (INTEGRATION) (preview)	Use regular Signal, while capturing all Signal calls, chats, attachme...	By TeleMessage	Instant Messaging
Signal Archiver (preview)	Use regular Signal, while capturing all Signal calls, chats, attachme...	By TeleMessage	Instant Messaging
Telegram Archiver (INTEGRATION) (preview)	Use regular Telegram, while capturing all Telegram calls, chats, att...	By TeleMessage	Instant Messaging
Telegram Archiver (preview)	Use regular Telegram, while capturing all Telegram calls, chats, att...	By TeleMessage	Instant Messaging
TELUS SMS Network Archiver	Integrated with the Telus mobile network. Get a copy of employee...	By TeleMessage	Instant Messaging
Verizon SMS/MMS Network Archiver	Integrated with the Verizon mobile network. Get a copy of employ...	By TeleMessage	Instant Messaging

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Settings
More resources
Customize navigation
Show all

WhatsApp Archiver

Add connector | Share

Overview

Benefits
Capture and archive WhatsApp chats and calls in Microsoft 365.

Solution impact
Can be used to enhance the compliance solutions that support imported third-party data. Learn more

Published
By TeleMessage

Learn

Documentation
Set up the WhatsApp Archiver connector

Community
Microsoft Security and Compliance TechCommunity

Requirements

Subscription
To learn more about licensing requirements, see Microsoft 365 tenant-level services licensing guidance.

Permissions
User must be assigned the Mailbox Import Export role to set up the connector.

By default, this role isn't assigned to any role group in Exchange Online. You can add the Mailbox Import Export role to the Organization Management role group. Or you can create a role group, assign the Mailbox Import Export role, and then add yourself or other users as a member. For more information, see the 'Add a role to a role group' or the 'Create a role group' sections in Manage role groups in Exchange Online.

Partner Pre-requisites
You should have a TeleMessage Admin account before proceeding further. You must finalize your order and payment to get archiving to work for your employees. You must onboard your employees to start mobile archiving.

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog

Settings
More resources

Customize navigation
Show all

Terms of service
Connector name
Connection to source
User mapping
Review

Terms of service

Preview Terms
If this service is designated as "Preview," it is subject to the Preview terms set forth in the Online Service Terms. Microsoft makes no commitments about the functionality, accuracy, or quality of any Connectors (defined below) during the Preview period. We do not recommend using Preview Connectors for production purposes, as data may be lost, deleted, or corrupted.

Microsoft Connector Terms of Service
These Microsoft Connector Terms of Service ("Terms") explain your and Microsoft's rights and obligations with respect to exporting your data from a third party source ("Data Source") and importing that data into M365 or other Microsoft service ("Microsoft Services"), via: (i) an application, bulk upload, service, or connection ("Connector"), or (ii) any third party providing a Connector or otherwise enabling a connection to a Data Source ("Connector Provider"). In addition to these Terms, your use of a third party Connector and your access to (and export of) data from a Data Source may be subject to additional, third party terms and privacy policies. Microsoft is not a party to your agreement with a Data Source, nor your agreement with any Connector Provider or other third party.

Please note that you, as the data controller for your data, are responsible for all data ingested into Microsoft Services, including obtaining applicable consents from individuals whose data is ingested. Only after such data is successfully ingested into the Microsoft Services will such data be considered "Customer Data," for purposes of the Online Service Terms and Privacy Statement, and Microsoft's data processing and other obligations. You can also find more about Microsoft's commitments to data protection and privacy by visiting our Trust Center.

You are responsible for configuring, using, and (to the extent applicable) creating a Connector to access and extract any data from a Data Source, and doing so in compliance with any applicable Data Source and

Accept Cancel

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog

Settings
More resources

Customize navigation
Show all

- Terms of service
- **Connector name**
- Connection to source
- User mapping
- Review

Name your connector

See the step-by-step instructions to help you setup a WhatsApp Archiver connector.

Enter a unique name for this connector.

Name *

Enter a unique name for this connector

Back | Next | Cancel | Need help? | Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Settings
More resources
Customize navigation
Show all

Terms of service
Connector name
Connection to source
User mapping
Review

Name your connector

See the step-by-step instructions to help you setup a WhatsApp Archiver connector.

Enter a unique name for this connector.

Name *

WhatsApp Archiver for Ignite

Back Next Cancel Need help? Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Settings
More resources
Customize navigation
Show all

- Terms of service
- Connector name
- **Connection to source**
- User mapping
- Review

Sign in to your TeleMessage account

To connect to your WhatsApp Archiver data, complete the steps in the TeleMessage WhatsApp Archiver connection wizard.

Sign into TeleMessage

When you sign into your TeleMessage account, you'll leave the Microsoft 365 compliance center and be directed to a TeleMessage site.

If your organization doesn't have an account with TeleMessage, sign up for an account.

By signing into or signing up for TeleMessage account, you agree to their privacy policy and terms of use.

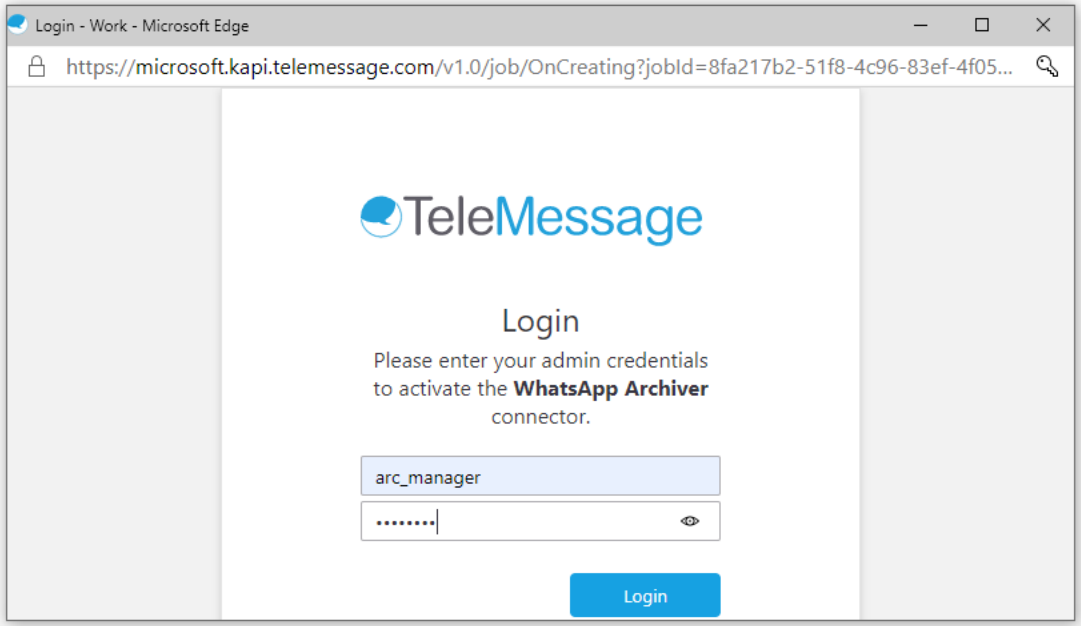
Back Next Cancel Need help? Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Settings
More resources
Customize navigation
Show all

- Terms of service
- Connector name
- **Connection to source**
- User mapping
- Review

Sign in to your TeleMessage account

Please complete the steps in the popup window and wait.



Back | Next | Cancel | Need help? | Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog

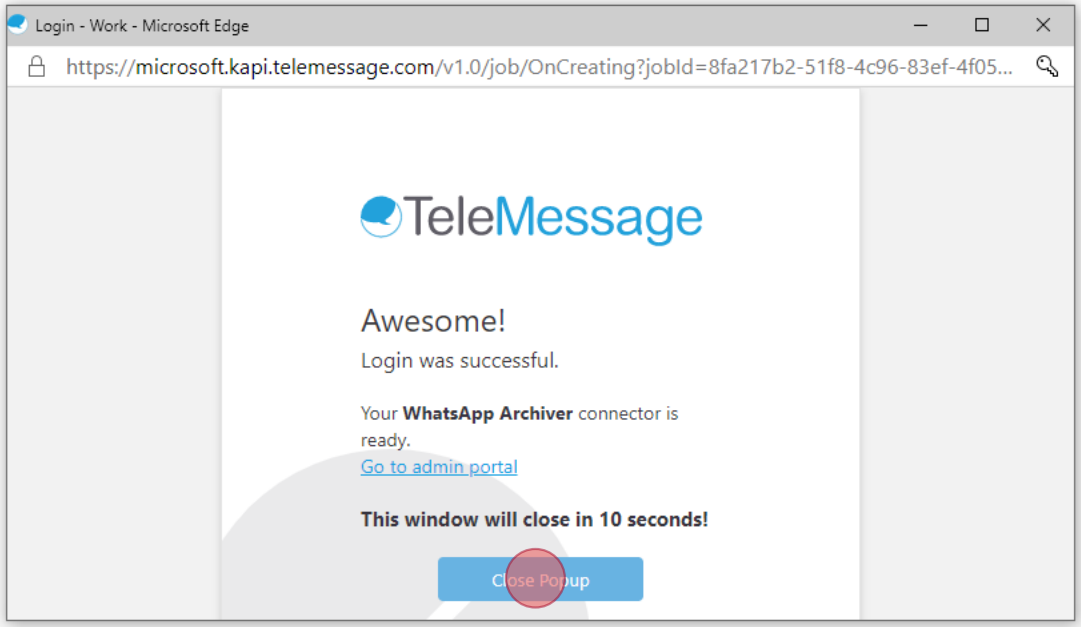
Settings
More resources

Customize navigation
Show all

- Terms of service
- Connector name
- **Connection to source**
- User mapping
- Review

Sign in to your TeleMessage account

Please complete the steps in the popup window and wait.



Back | Next | Cancel | Need help? | Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog

Settings
More resources

Customize navigation
Show all

Terms of service
Connector name
Connection to source
User mapping
Review

Map WhatsApp Archiver users to Microsoft 365 users

Map your organization's WhatsApp Archiver users to their corresponding Microsoft 365 account.

☑ **Enable automatic user mapping**

WhatsApp Archiver items include a property called **User's Email Address**, which contains email addresses for users in your organization. If the connector can associate this address with a Microsoft 365 user, the items are imported to that user's mailbox.

Custom user mapping (optional)

In addition to automatic user mapping, you can also define your custom mapping by uploading a mapping file in CSV format.

Please use the template file below to map the users using the **User's Mobile Number** to their M365 corporate email addresses.

Download CSV mapping template

Upload your custom CSV mapping file

Upload your custom CSV mapping file | Browse | Upload

Back | Next | Cancel | Need help? | Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions
Solutions
Catalog
Settings
More resources
Customize navigation
Show all

- Terms of service
- Connector name
- Connection to source
- User mapping
- **Review**

Review and finish

Name
WhatsApp Archiver for Ignite

User mapping
Automatic user mapping property: User's Email Address

Back | Finish | Cancel | Need help? | Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog

Settings
More resources

Customize navigation
Show all

- Terms of service
- Connector name
- Connection to source
- User mapping
- Review

Your connector was added

An import job has been created.

Connector job ID
9620b342-2fe0-4245-9d1e-bf621d892ba5

Done

Need help? Give feedback

Home
Compliance score
Data classification
Data connectors
Alerts
Reports
Policies
Permissions

Solutions

Catalog

Settings
More resources

Customize navigation
Show all

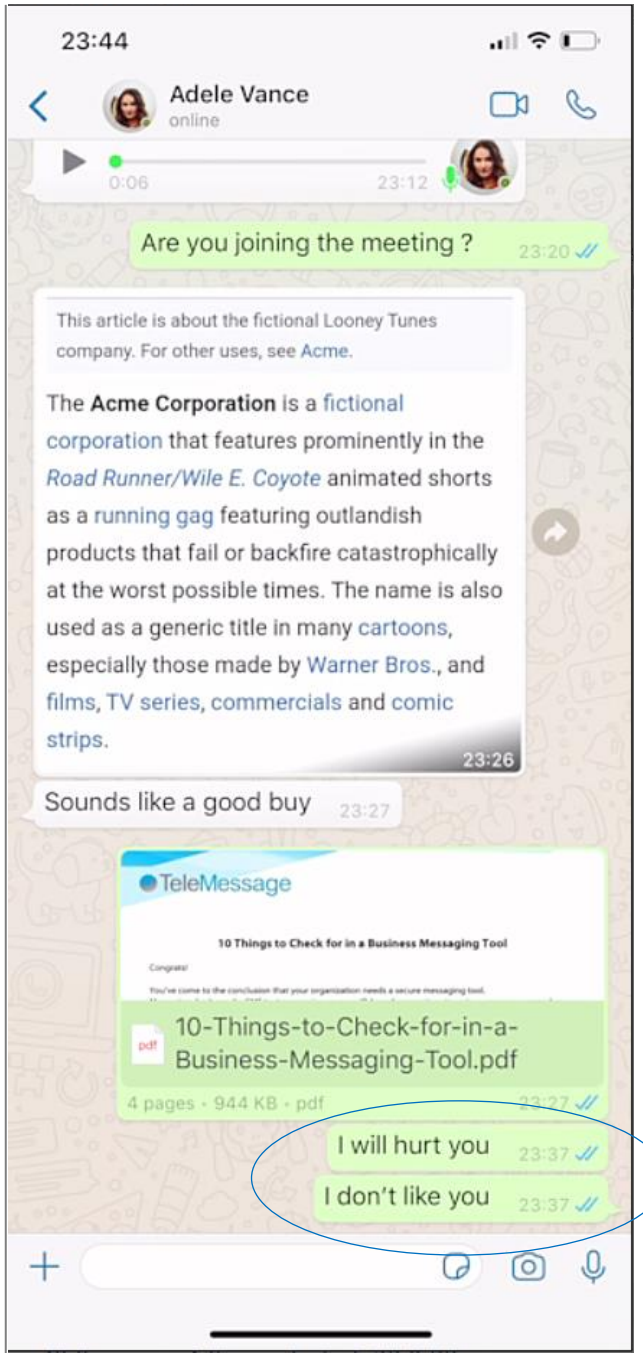
Data connectors

Overview | Connectors

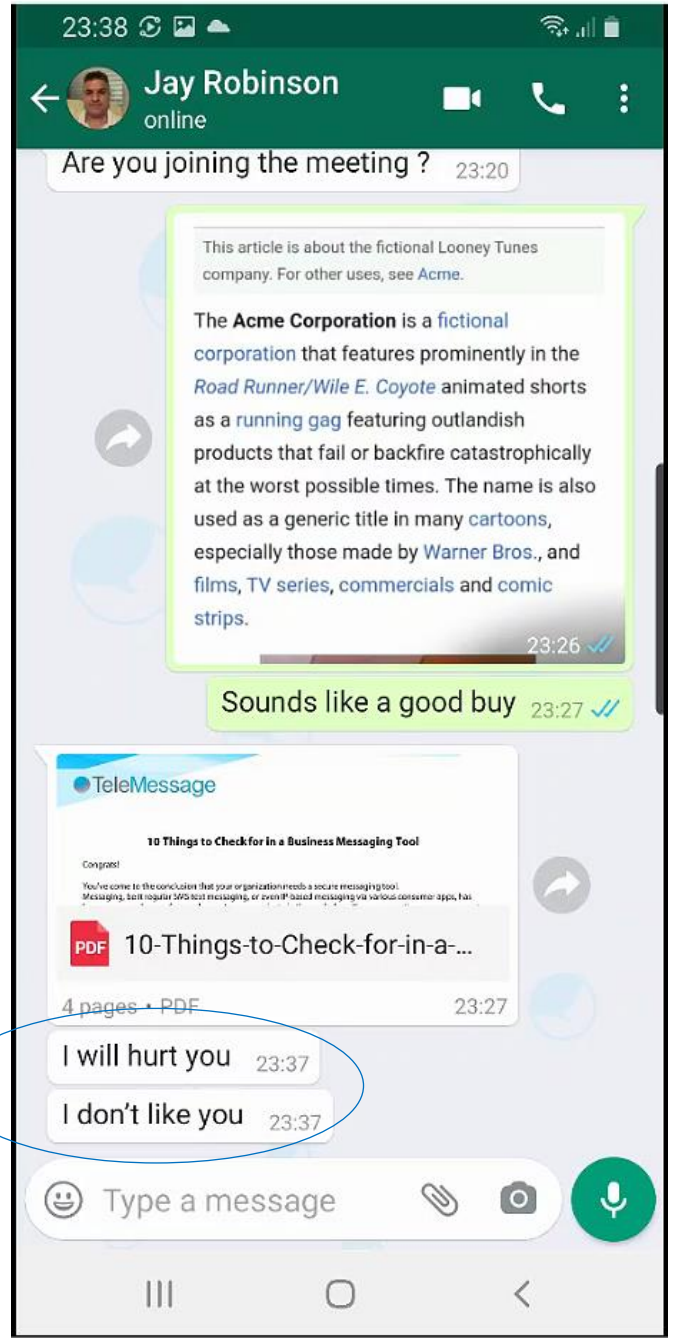
Add a connector | Refresh | 2 items | Search

Name	Connector type	Published	Connection status with source
WhatsApp Archiver for Ignite	WhatsApp Archiver	By TeleMessage	Connected
androidarchiver	Android Archiver	By TeleMessage	Connected

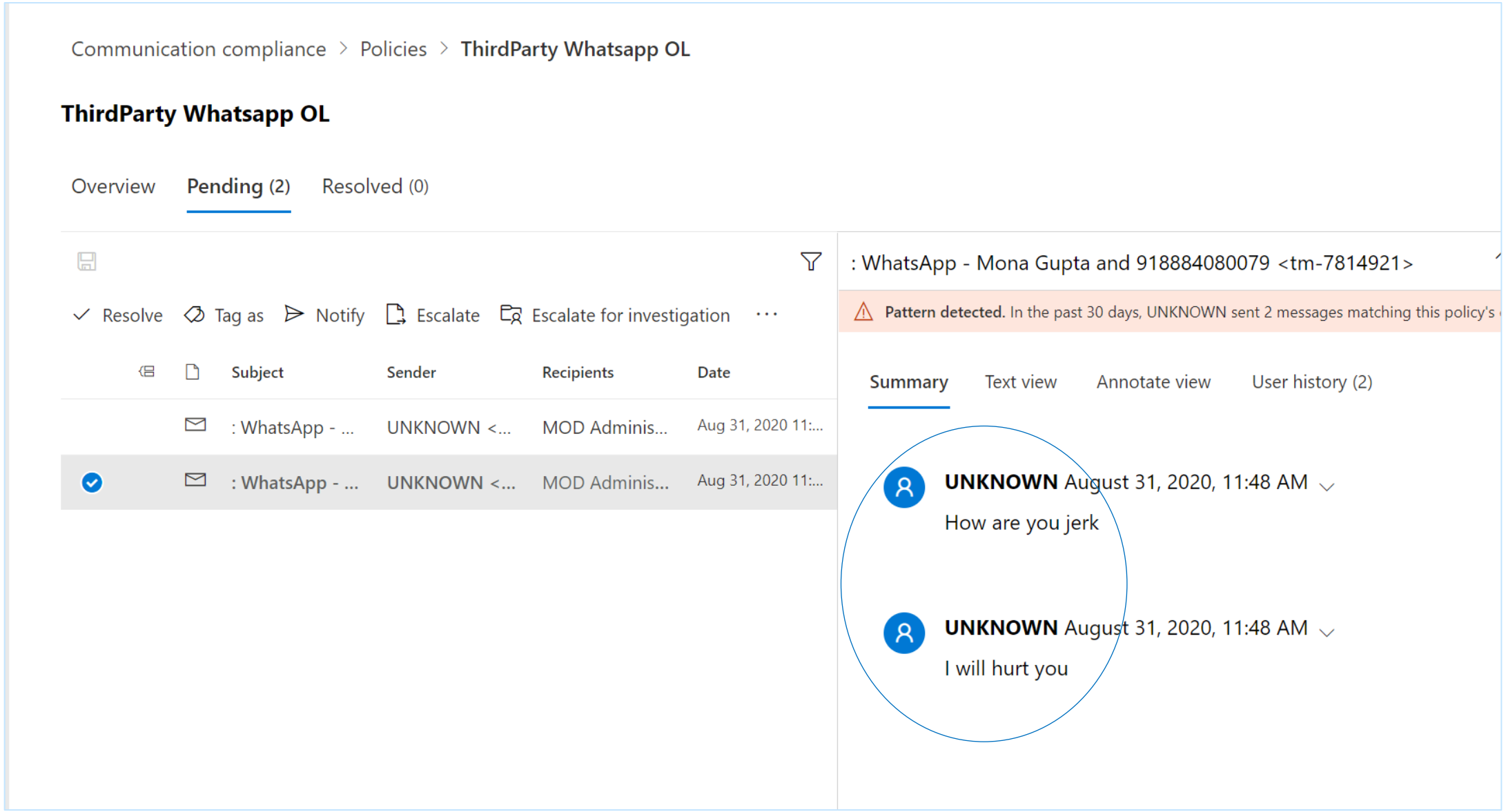
iOS


23:44
Adele Vance
online
0:06
23:12
Are you joining the meeting ?
23:20
This article is about the fictional Looney Tunes company. For other uses, see Acme.
The Acme Corporation is a fictional corporation that features prominently in the Road Runner/Wile E. Coyote animated shorts as a running gag featuring outlandish products that fail or backfire catastrophically at the worst possible times. The name is also used as a generic title in many cartoons, especially those made by Warner Bros., and films, TV series, commercials and comic strips.
23:26
Sounds like a good buy
23:27
TeleMessage
10 Things to Check for in a Business Messaging Tool
10-Things-to-Check-for-in-a-Business-Messaging-Tool.pdf
4 pages · 944 KB · pdf
I will hurt you
23:37
I don't like you
23:37

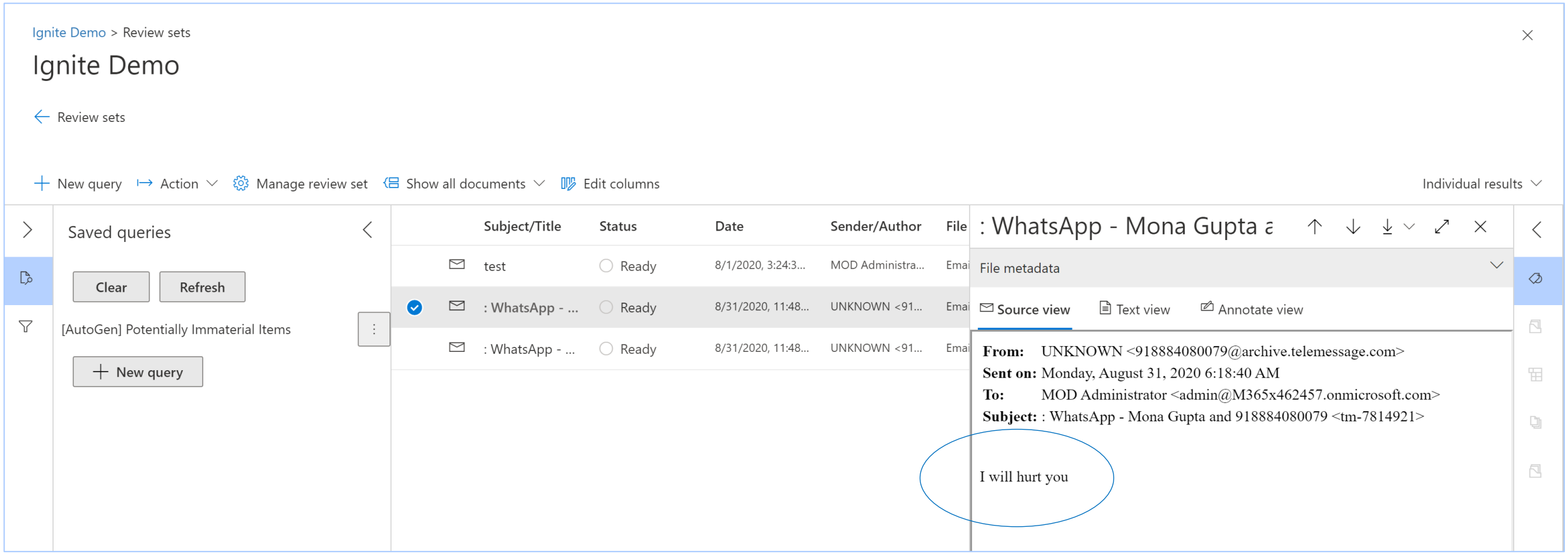
Android


23:38
Jay Robinson
online
Are you joining the meeting ?
23:20
This article is about the fictional Looney Tunes company. For other uses, see Acme.
The Acme Corporation is a fictional corporation that features prominently in the Road Runner/Wile E. Coyote animated shorts as a running gag featuring outlandish products that fail or backfire catastrophically at the worst possible times. The name is also used as a generic title in many cartoons, especially those made by Warner Bros., and films, TV series, commercials and comic strips.
23:26
Sounds like a good buy
23:27
TeleMessage
10 Things to Check for in a Business Messaging Tool
PDF
10-Things-to-Check-for-in-a-...
4 pages • PDF
23:27
I will hurt you
23:37
I don't like you
23:37
Type a message

Data in Communication Compliance



Data in M365 Solutions – Advanced eDiscovery



Useful links and contact info

- Link to Ecosystem blog - https://msft.it/6040TQFd6
- Ignite demo - https://aka.ms/ConnectorsIgniteDemo
- Fill in our survey: https://aka.ms/Microsoft365ComplianceConnectorSurvey
- Reach out to us about connectors – dcfeedback@microsoft.com

Microsoft

Thank you!

© Copyright Microsoft Corporation. All rights reserved.

We’re currently experiencing some technical difficulties. Please stay on, and we will back with you shortly.

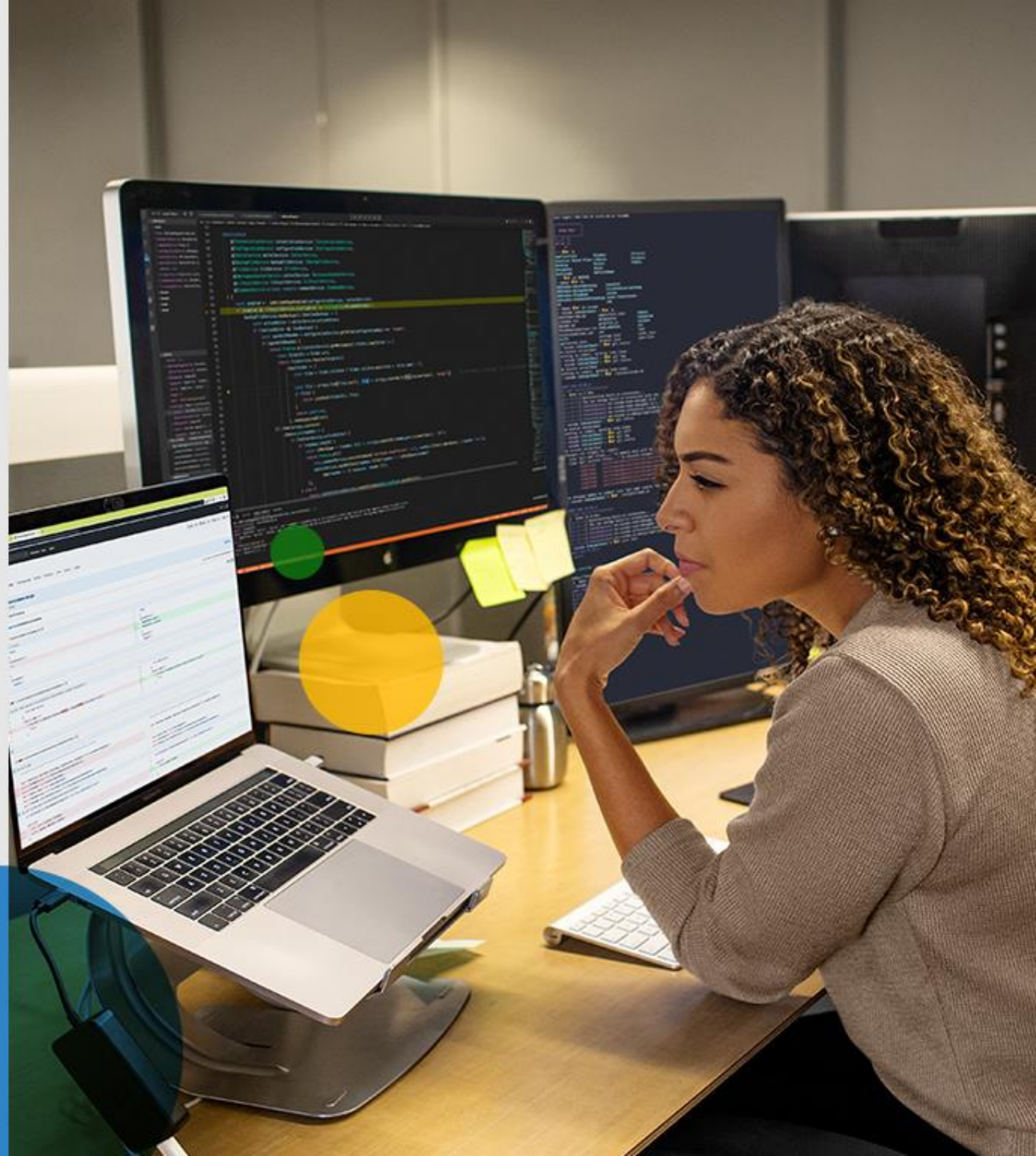
Microsoft Security

Thank you for joining us today.

Contact us

Microsoft 365 Security: aka.ms/365securitysales

Azure Security: aka.ms/azuresecuritysales




Microsoft Security