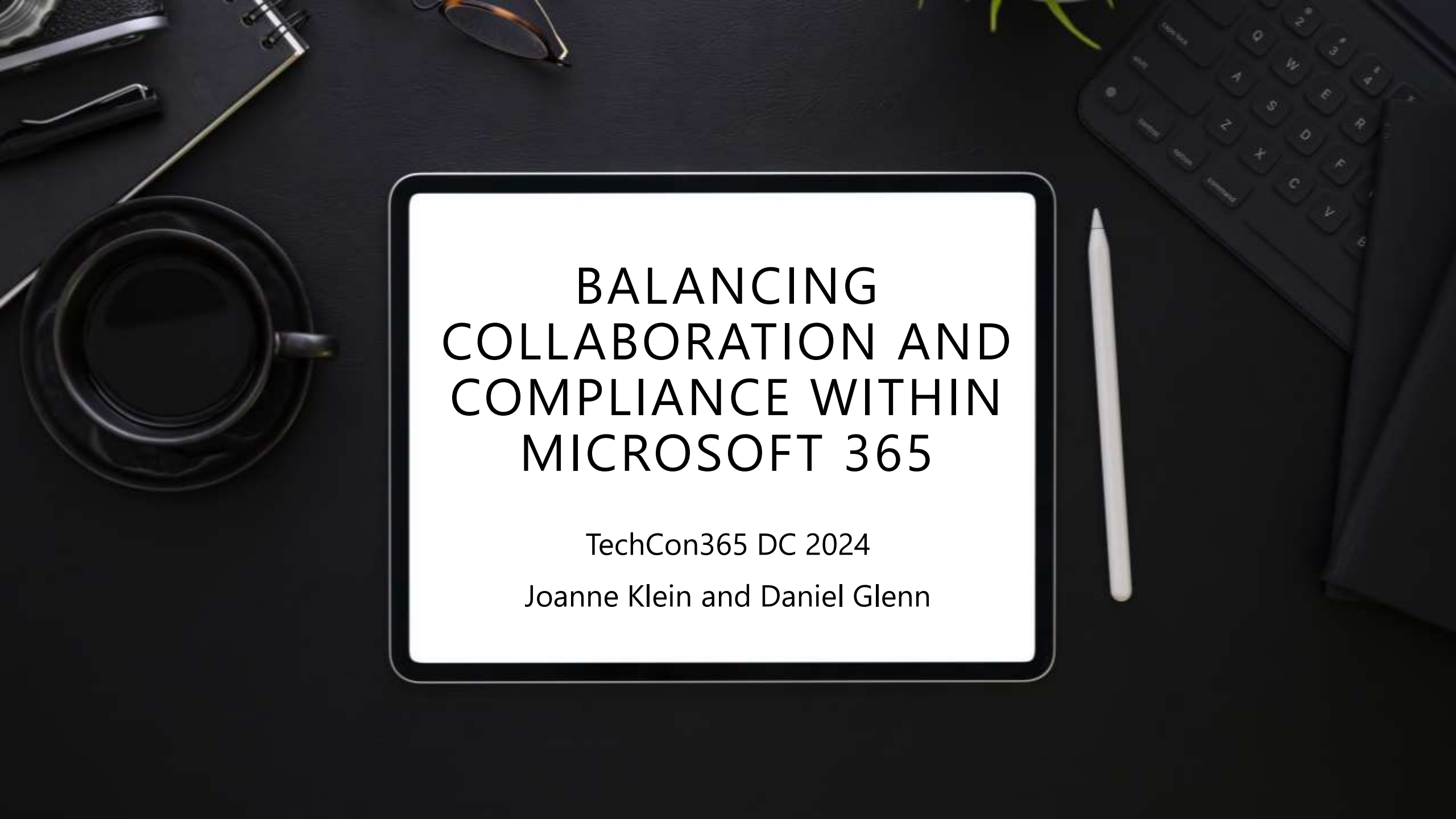


BALANCING COLLABORATION AND COMPLIANCE WITHIN MICROSOFT 365

TechCon365 DC 2024

Joanne Klein and Daniel Glenn

OUR WORKSHOP ½-DAY TOGETHER

AGENDA	TIME
Start	9:00AM
Collaboration tools	9:00-10:15AM
Break	10:15-10:30AM
Purview tools to help Copilot Readiness	10:30-11:45AM 11:45AM-12:30PM
Lunch	12:30-1:30PM

Hi! I’m Joanne!

@JoanneCKlein
joannecklein@nexnovus.com
joannecklein.com

Microsoft® Most Valuable Professional

SharePoint & Microsoft 365 consultant | Advanced Compliance and Content Management

Subscribe to our YouTube channel!

www.youtube.com/@ComplianceUnplugged

Daniel Glenn

Owner & Microsoft 365 Consultant
CollabFront

9-time Microsoft MVP (M365)

Microsoft Global Community Initiative Regional Lead

M365 Nashville Executive Director

365 Message Center Show - 365MCS.com

DanielGlenn.com

/DanielGlenn

Let's connect!

DanielGlenn.com/HELLO

Subscribe via your favorite podcast app or on YouTube

365MCS.com

New show every Monday!

Microsoft Viva

Empower organizations to continuously improve workforce engagement and performance

Drive mission and alignment

Viva Goals

Viva Engage

Viva Amplify

Enable a high-performance workforce

Viva Connections

Viva Learning

Viva Topics

Measure engagement and productivity

Viva Glint

Viva Pulse

Viva Insights

Microsoft 365 + Copilot in Viva

Platform and admin services

Copilot in Microsoft Viva, people, answers, admin experience, common navigation

Privacy and security

Granular feature access controls, inherited permissions for 3P, differential privacy for insights

Integrations to HCM, CRM, LMS, wellness, and more

Workday, Qualtrics, SAP SuccessFactors, LinkedIn, Headspace, and more

How Microsoft Viva can help drive performance

Engaged employees	Productive teams	Resilient business
Leadership connection Viva Engage, Viva Amplify	**Team collaboration** Viva Insights	**Agility to change** Viva Glint, Viva Pulse
Focus and alignment Viva Goals, Viva Engage	**Skilling and onboarding** Viva Learning, Viva Topics	**Efficient processes** Viva Connections, Viva Topics
Culture and wellbeing Connections, Viva Insights, Pulse	**Creativity and innovation** Viva Learning, Viva Goals	**Flexible workplace** Viva Glint, Viva Goals

The Shift for Communicators

- One-way communications ▶ Multi **Directional**
- Channel Management ▶ Multi **Channel**
- Noisy & Interruptive Comms ▶ Multi **Speed**
- Text-heavy content ▶ Multi **Media**
- Top-down official channels ▶ Multi **Voice**

Source: Viva Engage and AI Transform Communications (Youtube)

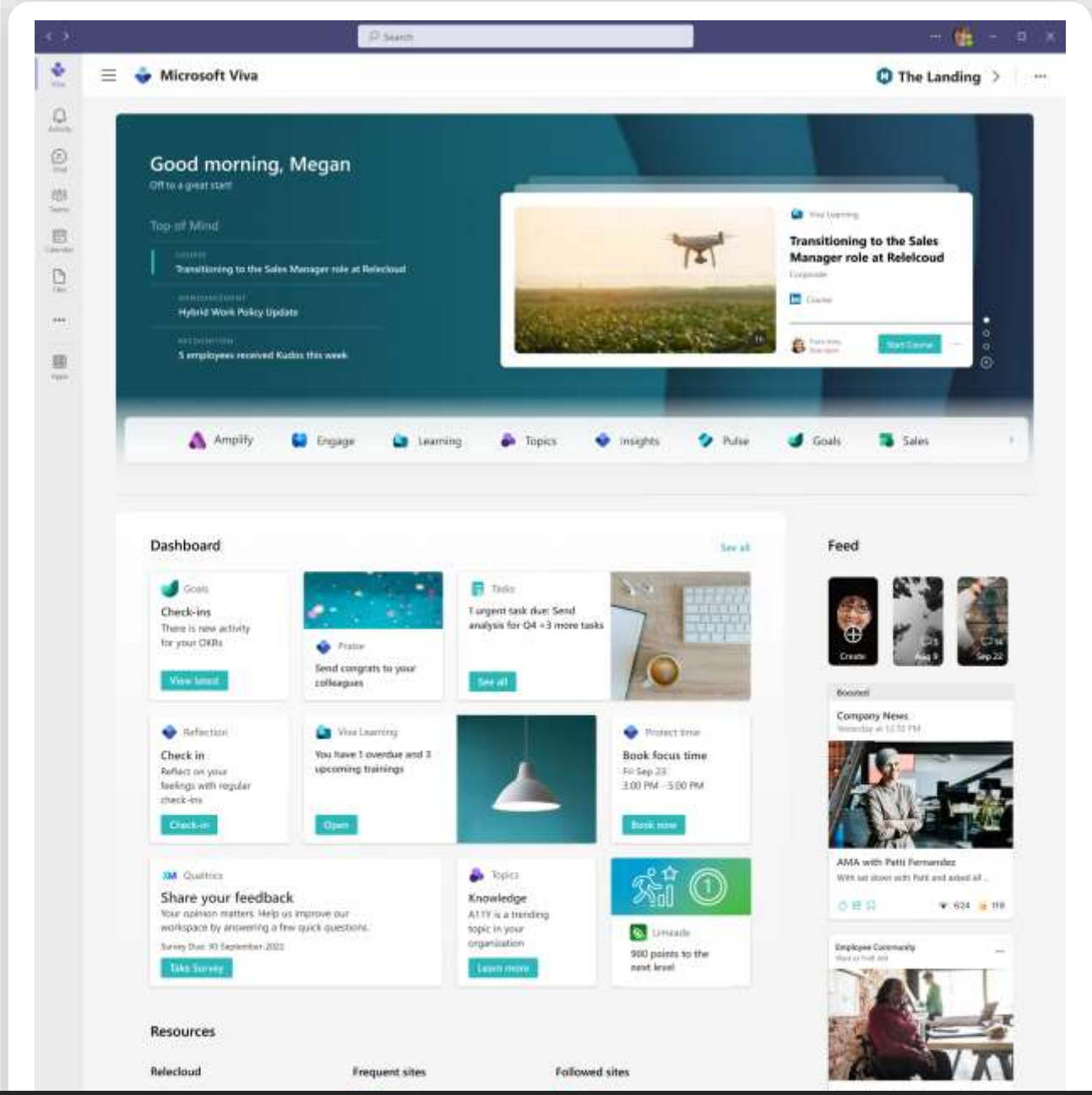
Viva Connections

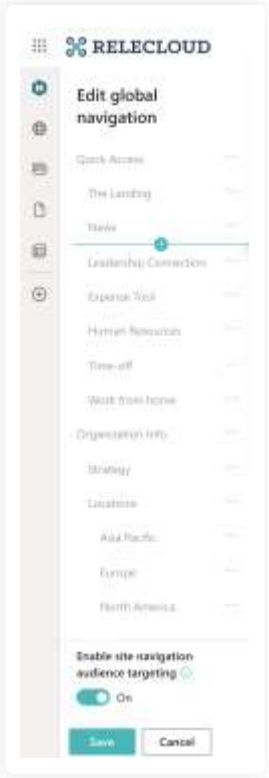
The home for your employee experience

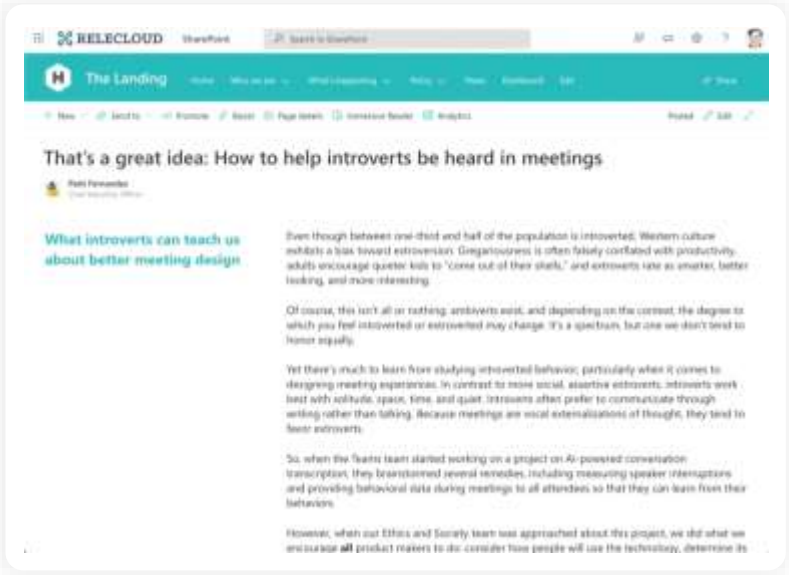
Simplify employees' days through an integrated and personalized dashboard

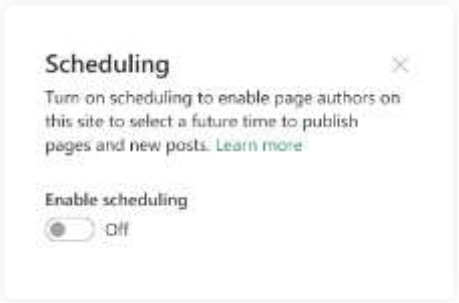
Keep employees connected with targeted news and information from across Microsoft 365

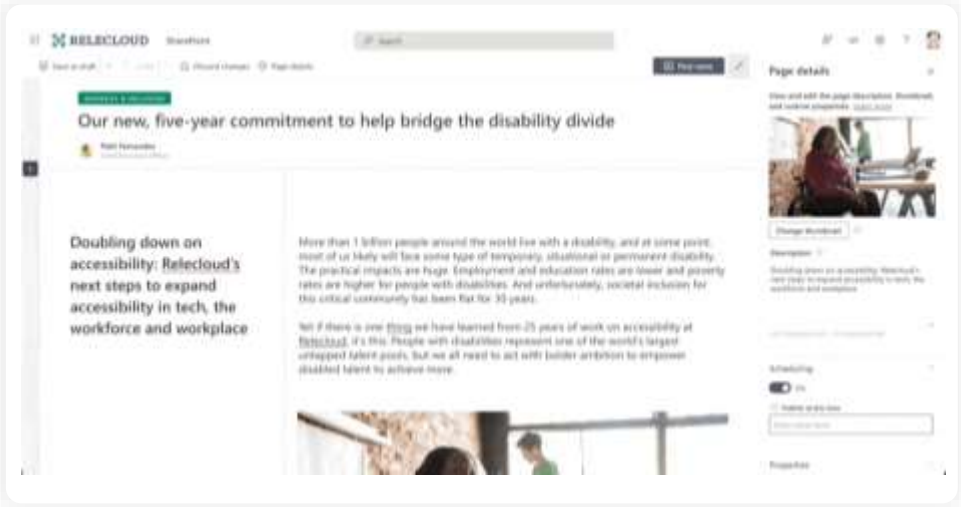
Seamlessly move across different Microsoft Viva apps without navigating away











TARGET, PRIOROTIZE AND SCHEDULE

Deliver updates to the right people at the right time

Scale up or down communications to keep everyone informed

Boost critical content to the top of employee feeds

Drive dialogue and engagement with announcements to specific communities or all employees

Leverage modern editing features to delegate posting, schedule publishing, and track impact

Viva Connections experiences

Dashboard

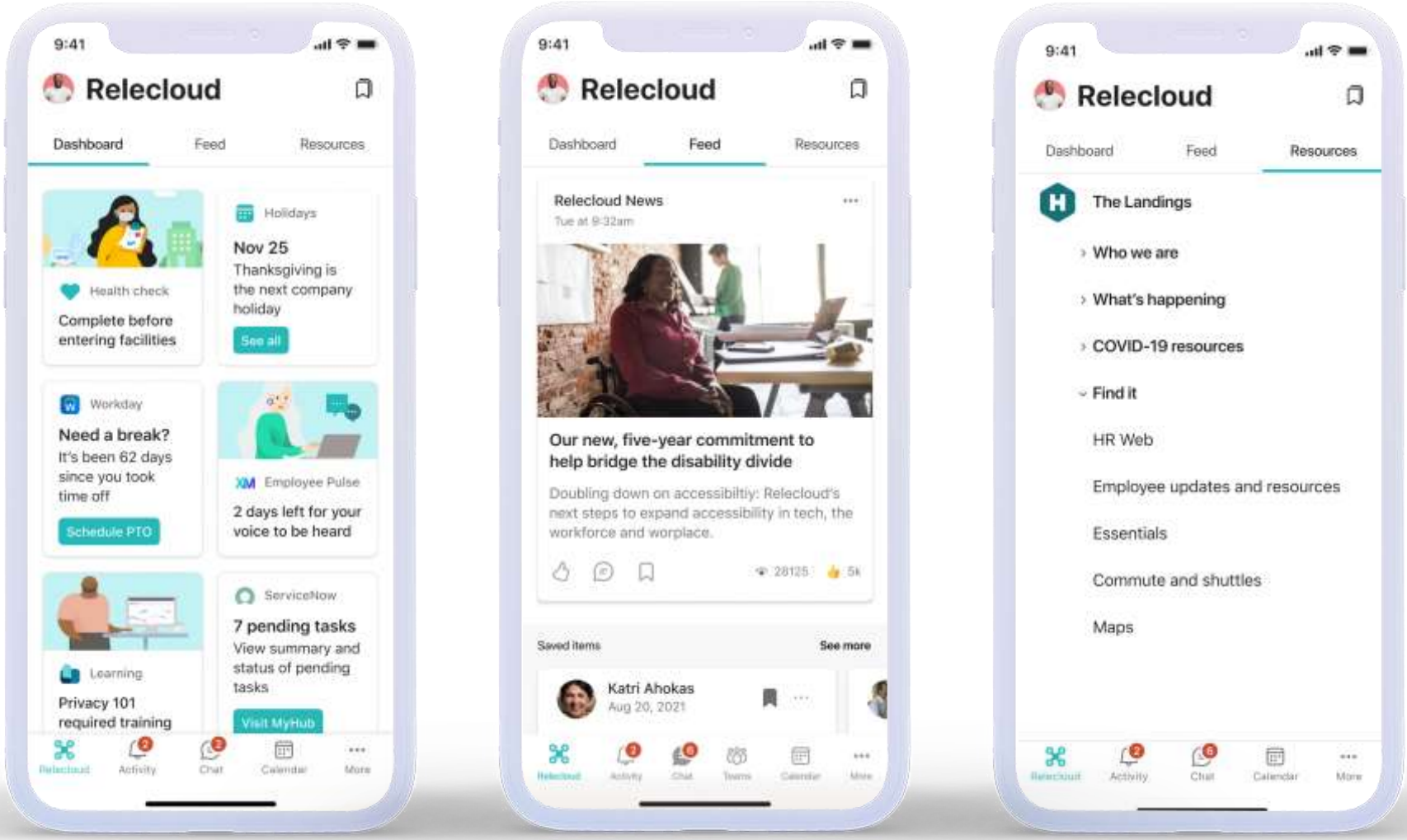
Complete tasks and focus on critical information

Feed

Discover and engage with news and conversations

Resources

Find what you need across your digital workplace



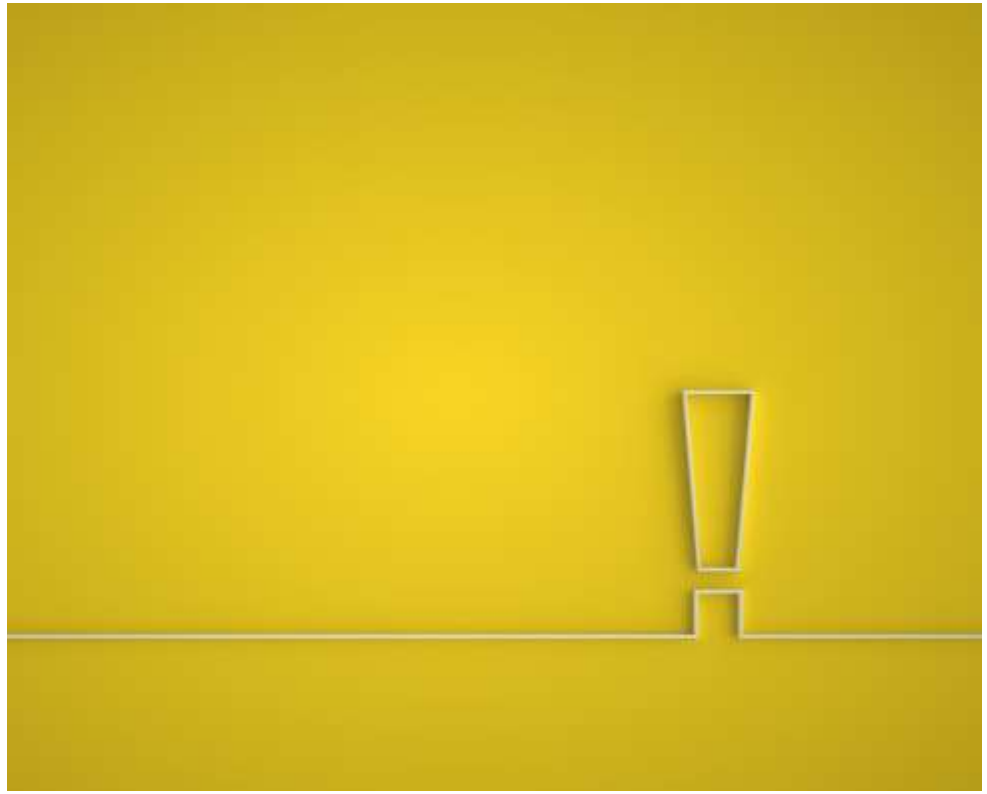
Content Your Way

More than just news - policies and procedures

Targeted content based on roles, memberships, and more

Multiple Home sites

- Create compelling unique experiences for each business unit or subsidiary



Viva Connections

DEMO

Viva Engage

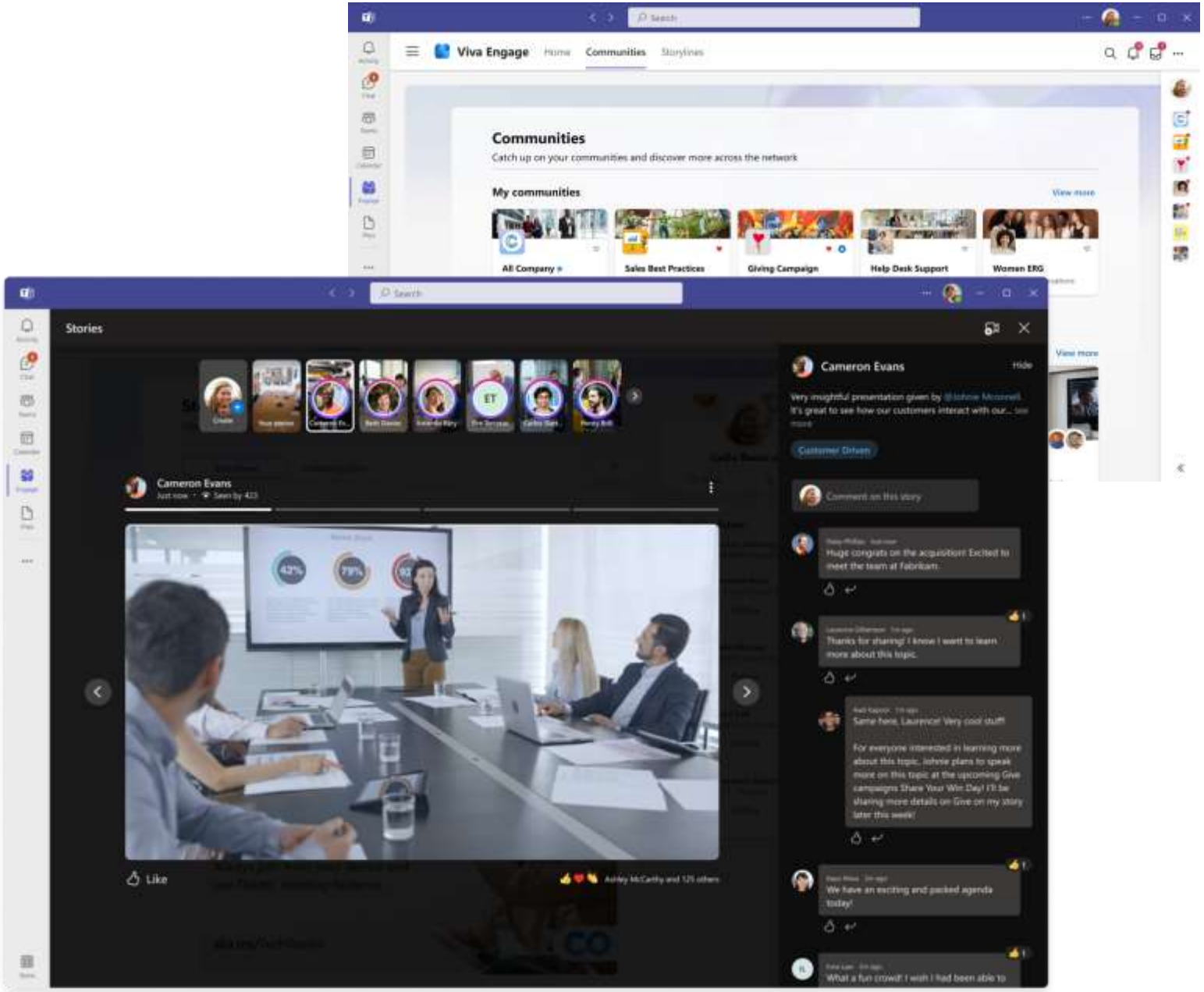
Viva Engage

Connect people across the organization so everyone feels included & invested

Available for all Microsoft 365 customers at no additional charge

Empowers people to connect and contribute with storyline & stories

Engage remains the standalone app on web, desktop and mobile



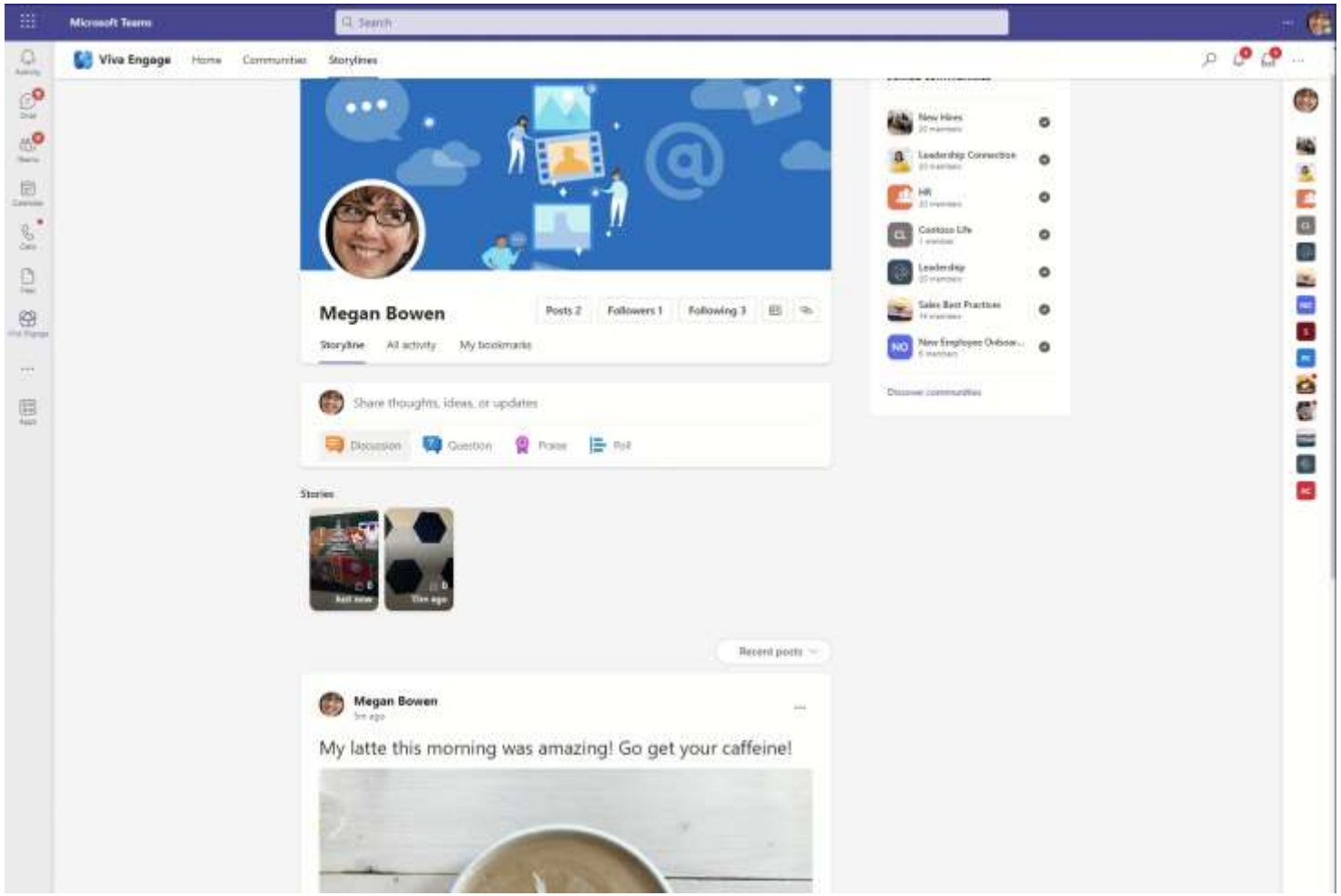
Storyline – Your Voice

Posting outside communities

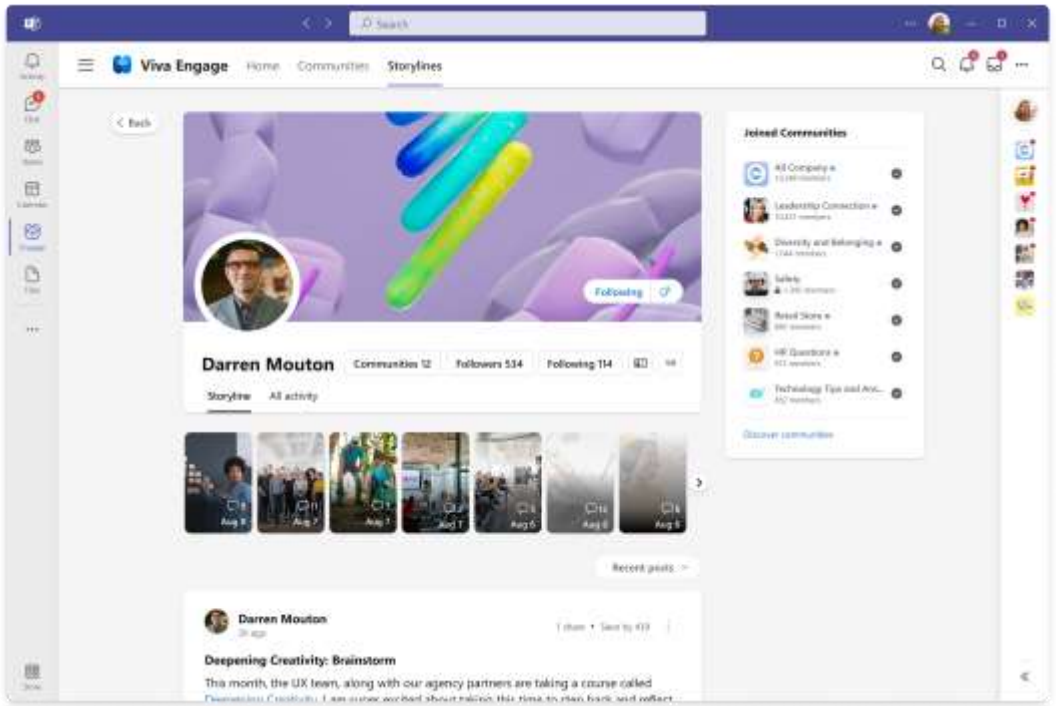
Use posts, video, and images to share perspectives & updates with people across the organization.

Find, follow, and engage with leaders and experts.

Connect and build your personal network to grow professionally and amplify your impact.



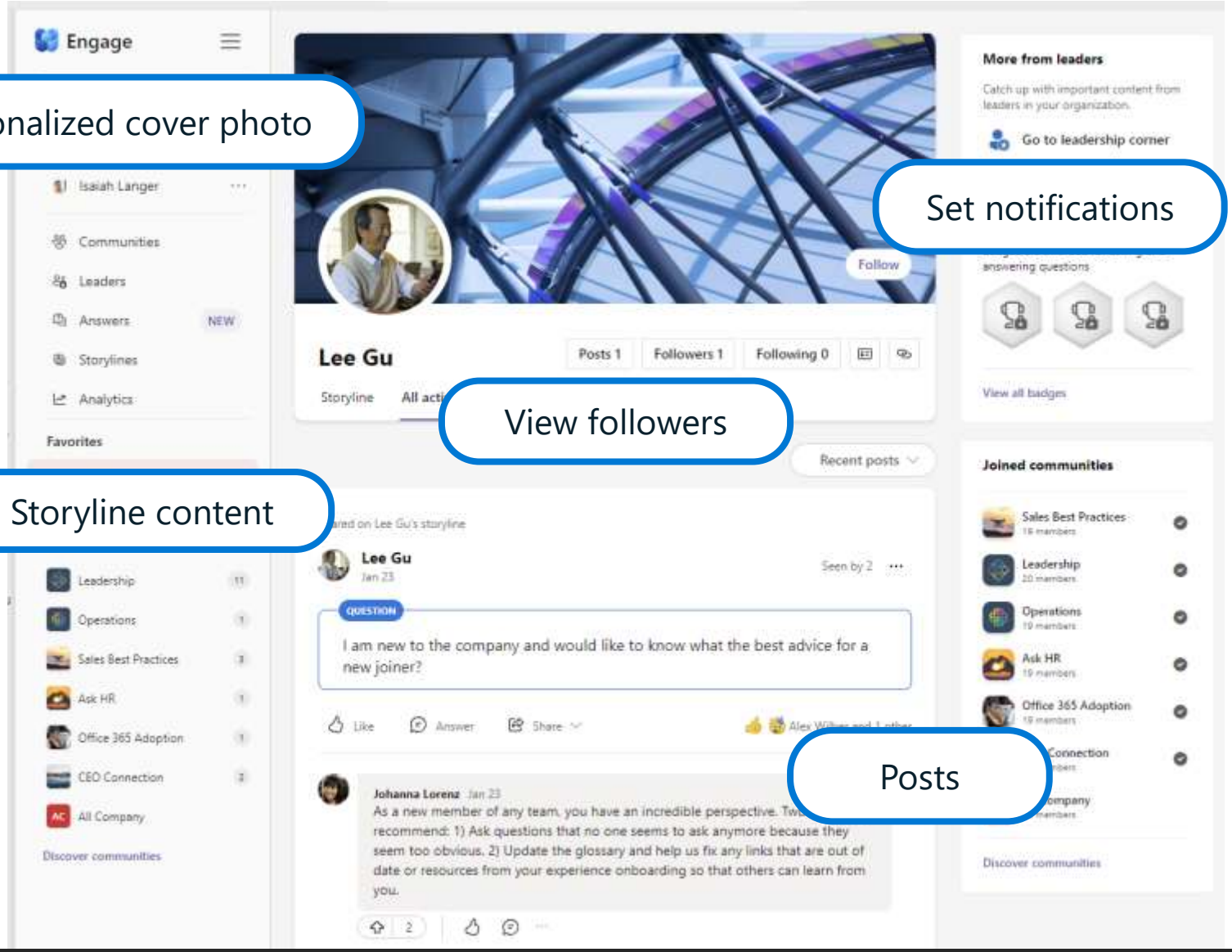
Storyline posts



You can create posts that include links, files, photos, or GIFs.

Posting photos or short videos that can be annotated is easy

Storyline Profile View

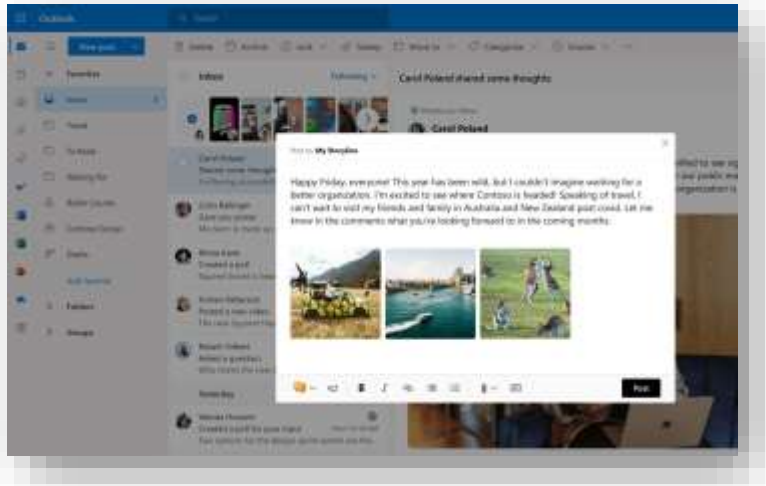


Viewing Storyline

Interact with storyline across Microsoft 365 and Microsoft Viva.

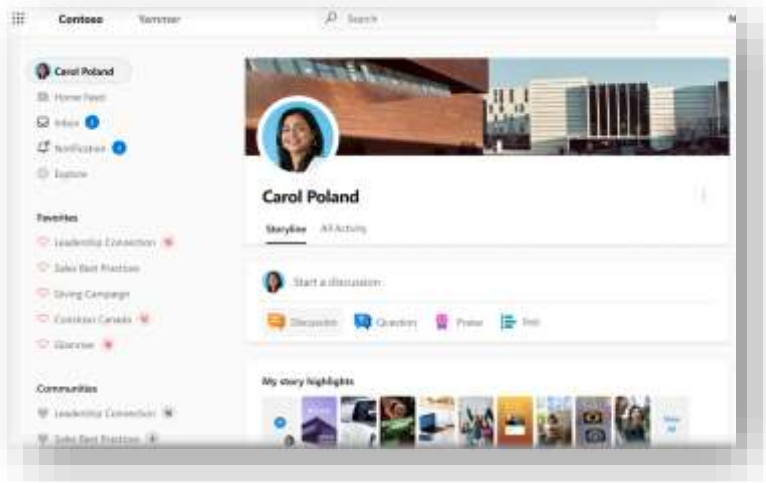
Microsoft Teams - Viva Engage

Pin the Viva Engage app to the app launcher in Microsoft Teams.



Outlook

Start a storyline post or reply directly from email notifications.



Viva Engage

View directly in web & mobile.

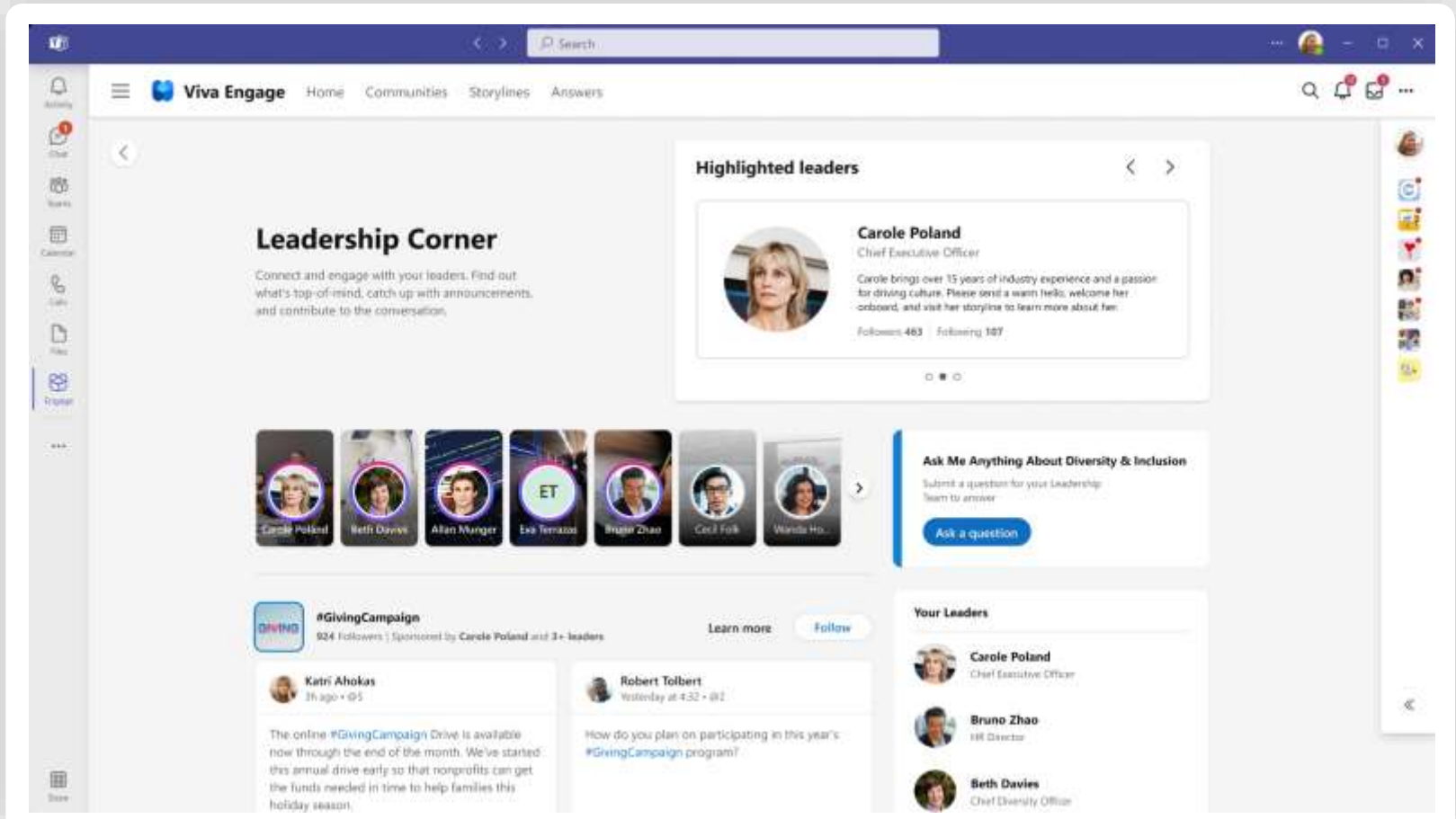
Viva Engage – Leadership Corner

Give leaders the tools to engage directly with employees across the company

Find and engage with highlighted leader posts, articles, events & conversations

Foster open dialog & learn what's top of mind for employees

Get insight into employee engagement, concerns, sentiment, & actionable steps through rich metrics



Viva Engage

DEMO

Viva Connections Planning

- How many
  - Subsidiaries, Countries, Divisions
  - Get 1 for free!
- What site(s)

  Will you use the out of the box experience?

  What site will be your home?

- Where is content? How is it classified?

  Is SharePoint your content publishing platform?

  Who manages permissions / site creation / content (refresh)?

Viva Engage Planning

- What Communities?
  - What communities should be created?
  - What is the process for creation?
    - Self-service
    - Centrally controlled
    - Automated
    - Manual

- Who are communicators/leaders?
  - Think outside the box!
  - Their voice will be heard
  - Campaigns
  - AMAs

COLLABORATION IN MICROSOFT TEAMS

TEAMS IS FOR COLLABORATION
TEAMS MAKES IT EASY TO WORK TOGETHER!

Meet

Chat

Call

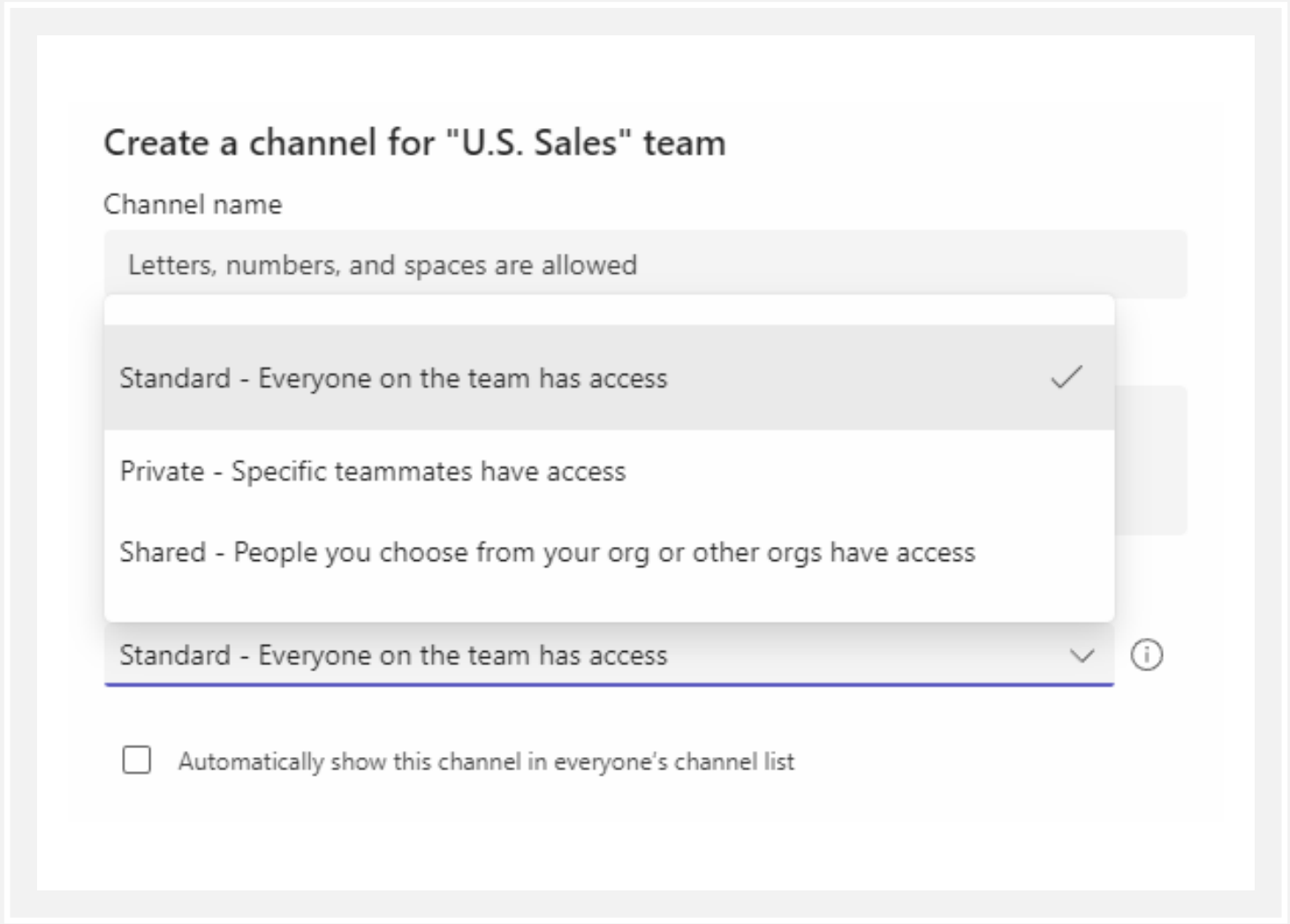
Share

Automate

Connect

TEAM STRUCTURE

- Flexible and it moves with you
- Microsoft 365 Group integrated
- Apps and pinning for a evolving work canvas
- Add channels any time



CHANNEL OPTIONS

- Standard
- Private
- Shared

HOW DO I CHOOSE?

Standard

- Conversations for teams
- Shared content and tabs
- Same users and permissions

Private

- Subset of users for secured access
- Files/convos that need to be private

Shared

- Give access to outside users & internal users not in team
- Not “guests” like M365 Groups

MICROSOFT 365 GROUPS

- Group of Microsoft 365 resources with a shared membership
- Resources can include:
  - Shared Outlook inbox
  - Shared calendar
  - SharePoint site
  - Planner Plan
  - Viva Engage Community
  - A Microsoft Teams team
  - and more!

COLLABORATING

- With your teammates
- Sharing with external partners and guests
- Meeting Captions & transcripts
- Collaborative meeting notes
- Intelligent Recaps (AI)

COLLABORATE WITH GUESTS

- Allow anyone with a business or consumer email account, such as Outlook, Gmail, or others, can participate as a guest in Teams.
- Channels, chat, and apps!
- Each one gets an Azure AD guest account

TEAMS STORAGE

EXCHANGE

- Messages (for compliance)
- Images (for compliance)
- Voicemails
- Calendar Meetings
- Meeting chats
- Contacts

SHAREPOINT / ONEDRIVE

- Team files (SharePoint)
- Chat files (OneDrive)
- Recordings (>24 hrs)

AZURE

- Messages (Cosmos DB)
- Images (Blob)
- Recordings (Blob <24 hrs)
- Telemetry (no customer content)

Teams

DEMO

TEAMS PLANNING

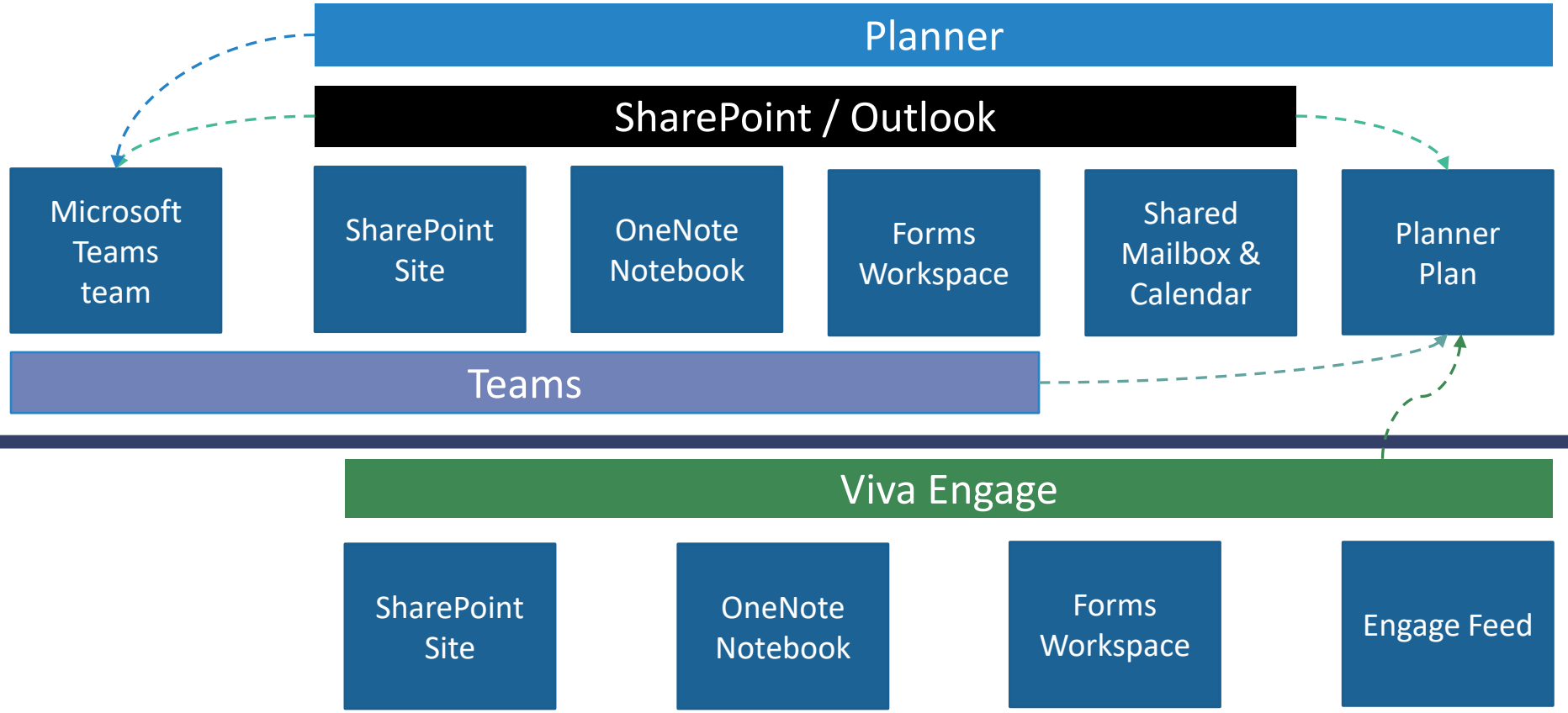
- What Teams
  - What determines a Team is needed
  - Who determines?
  - All-org team - yes/no & why
  -
- Files
  - How will files be accessed
-
- Creation Process
  - Self-service
  - Centrally controlled
  - Automated
  - Manual
  -
- Granting access
  - Owners get the keys
  - Powered by Microsoft 365 Groups

TEAM SITES – PRIVATE OR PUBLIC

- Public space for collaborating and information sharing
- Or a Private place for projects, departments, working teams, etc.
- Sharing with internal and external members
- Different types of records, checklists, project files, etc.

Microsoft 365 Groups

What you get, when



Collaboration… navigating potential issues

Common issues:

- Data hoarding
- Regulatory compliance infractions
- Privacy breaches
- Insider threats (both unintended and malicious)
  - Data oversharing
  - IP theft
  - Data leakage

1 Trillion

New files added last year

420 million files added during this workshop!

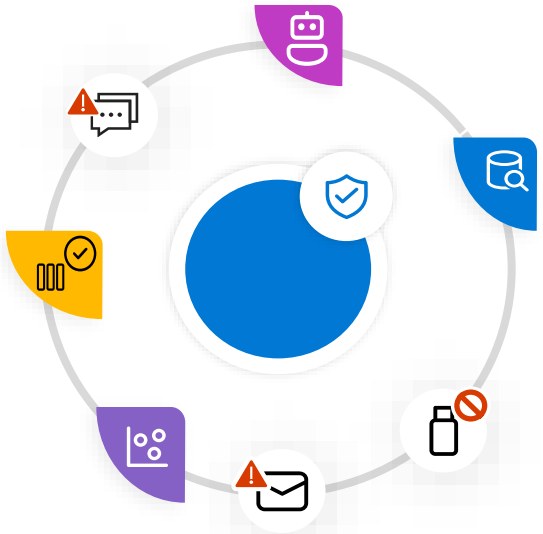
Top data security concerns in the modern workplace

Data security incidents are more common than the headline news.	59	Number of data security incidents experienced by organizations on average in the past year—with 20% being severe.
Business value can be lost due to poor data security.	74%	Organizations that have had business data exposed in the past year.
A fragmented solution landscape can weaken security posture.	2.8X	Number of data security incidents experienced by organizations that use 16 or more security tools.

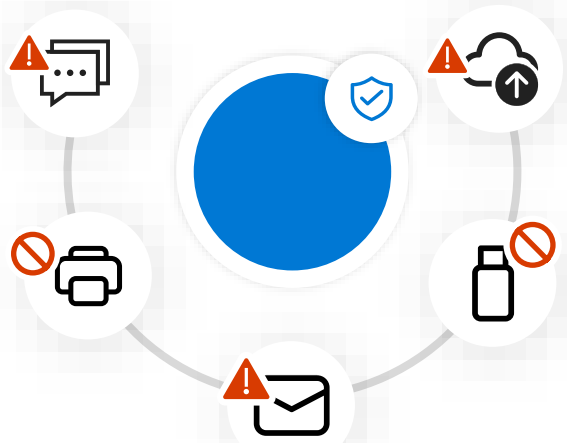
Source: Data Security Index, Microsoft, 2023

How organizations must approach compliance to scale

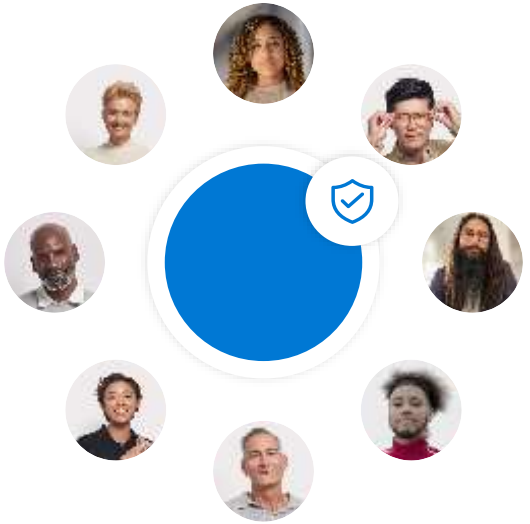
Intelligence to continuously monitor the entire digital data estate



Unified, integrated policies and incident management



Built-in and enables end users to be productive and secure



Let’s use an **insider threat** scenario to showcase how Purview features can help navigate these common data security concerns…

The Scenario


I’m outta here!
Jane Doe

Jane Doe's story (a departing, disgruntled employee)

Jane Doe

Trusted employee for 5 years

Before resigning, Jane downloads confidential Teams files to USB.

Jane hands in her official resignation to HR.

Jane downloads files a few at a time to her personal Dropbox.

Jane emails a few files at a time to her personal email.

Jane deletes the files from Teams including recycle bins.

Her activities go unnoticed

Contoso has no visibility into sensitive data.

Jane's risk level is not identified.

Jane's data exfiltration activities go undetected…

Files are permanently destroyed.

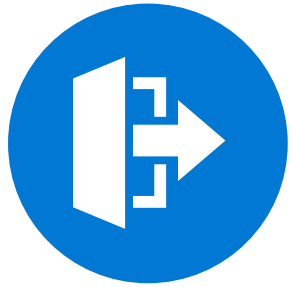
Microsoft Purview

Microsoft Purview

A platform for governing and securing data across your data estate.

DATA GOVERNANCE	DATA SECURITY	RISK AND COMPLIANCE
Set of solutions to help you manage data services across your on-prem, multi-cloud, and SaaS estate.	Set of solutions to help you discover and protect your sensitive information.	Set of solutions to help you minimize compliance risks and meet regulatory requirements.
• Data Catalog • Data Estate Insights • Data Map • Data Policies • Data Sharing	• **Data Loss Prevention** • Information Barriers • **Information Protection** • **Insider Risk Management**	• Audit • Communication Compliance • Compliance Manager • eDiscovery • **Data Lifecycle/Records Mgmt**

Take a defense-in-depth approach for Data Security

Information Protection	Insider Risk Management	Data Loss Prevention	Data Lifecycle Management
			

Adaptive Protection

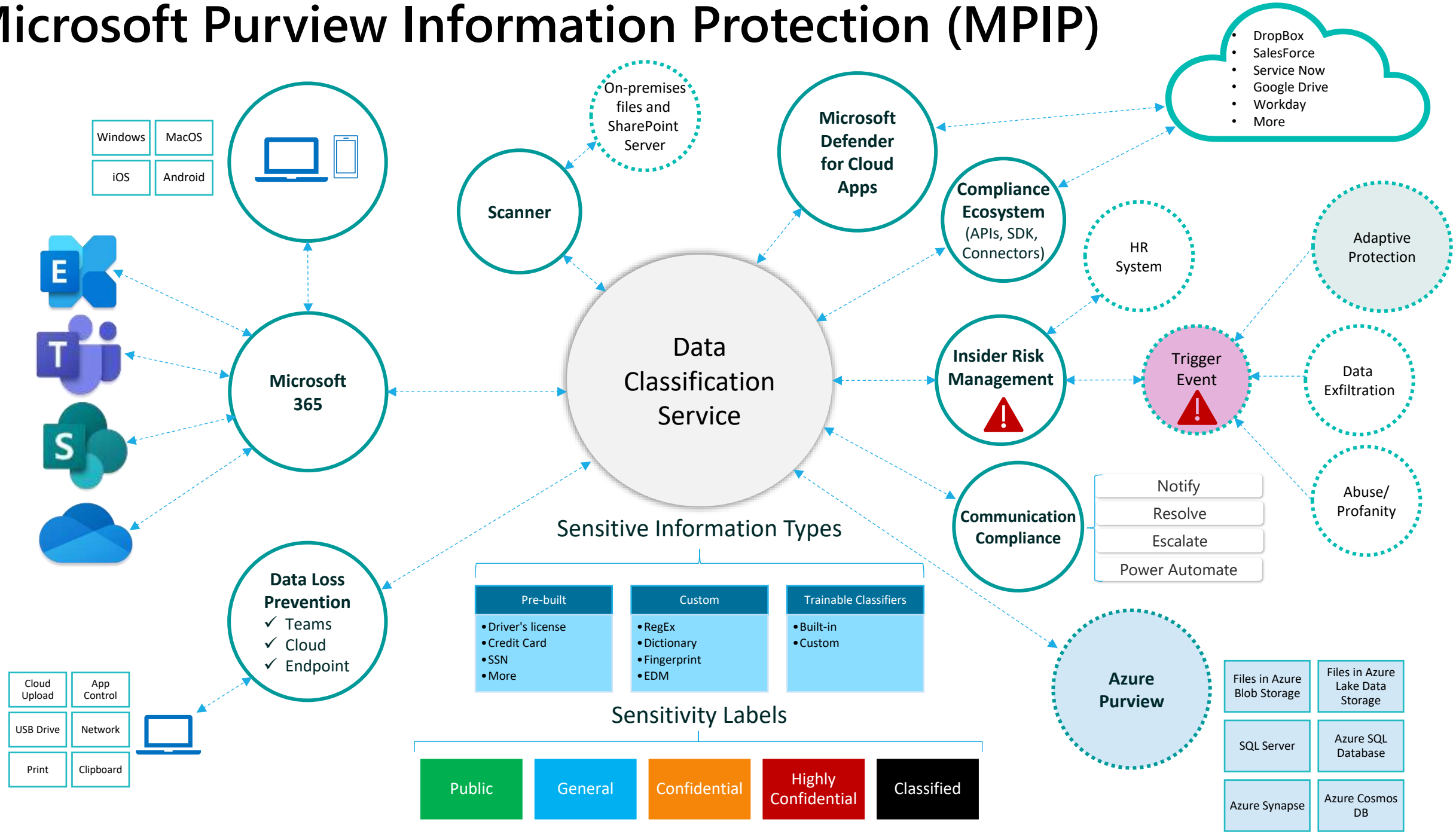
Microsoft Purview Information Protection

What business problems are we trying to solve with Information Protection?

"When users are collaborating with sensitive content, we must ensure the content is protected in the tools they're already using even if the content leaves the tenant."

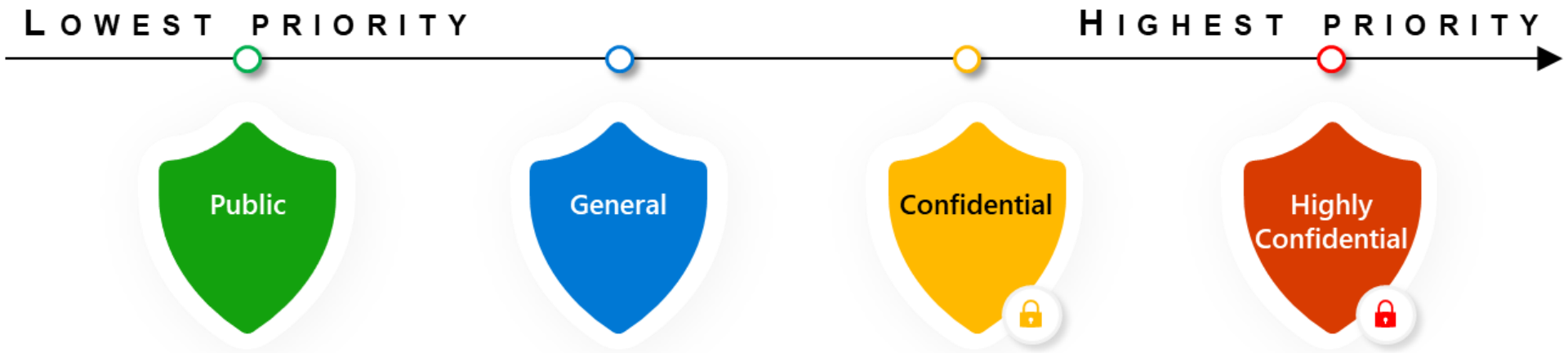
"Automatically apply protection guardrails when users are using Copilot for Microsoft 365."

Microsoft Purview Information Protection (MPIP)



What can Information Protection do at a file level?

- **Understands** data sensitivity and the associated risk
- **Classifies** data with a sensitivity label that you define



- Applies **precise protection** controls (encryption, access levels)
- **Informs** many other Purview features

Best-in-class classification technologies

Sensitive info types

200+ out of the box info types like SSN, CCN

Clone, edit, or create your own

Supports regex, keywords, and dictionaries

AVAILABLE TODAY

Named entities

50+ entities covering person name, medical terms, and drug names

Best used in combination with other sensitive info types

AVAILABLE TODAY

Exact data match

Provides a lookup to exactly match content with unique customer data

Supports 100m rows and multiple lookup fields

AVAILABLE TODAY

Optical Character Recognition (OCR)

Expanded OCR for EXO, SPO, ODB, Teams & endpoint devices

Supports over 150 languages

Supports image files and images embedded in PDFs

AVAILABLE TODAY

Trainable classifiers

35+ pre-trained ready-to-use trainable classifiers

Create your own classifier based on business data

AVAILABLE TODAY

Credentials SITs

42 new SITs for digital authentication credential types

Use in auto-labeling and DLP policies to detect sensitive credentials in files

AVAILABLE TODAY

Fingerprint SITs

Detect exact or partial matching of sensitive intellectual property

Use in Exchange, SharePoint, Teams and Devices

AVAILABLE TODAY

Context-based classification

ODSP default site label

Service-side auto-labeling

- File extension
- Document name contains word
- Document property is
- Document size greater than
- Document created by

AVAILABLE TODAY

What can Information Protection do at a container level?

CONTENT LABELS FOR “CONTAINERS”

Privacy controls: Controls whether the group/team is Public, Private, or settable by members

Guest access: Controls if guests can be added to the group

External sharing: controls level of sharing (Anyone, New/existing guests, Existing guests, internal org only)

Conditional access: Use CA policies to restrict access from unmanaged devices, use authentication contexts

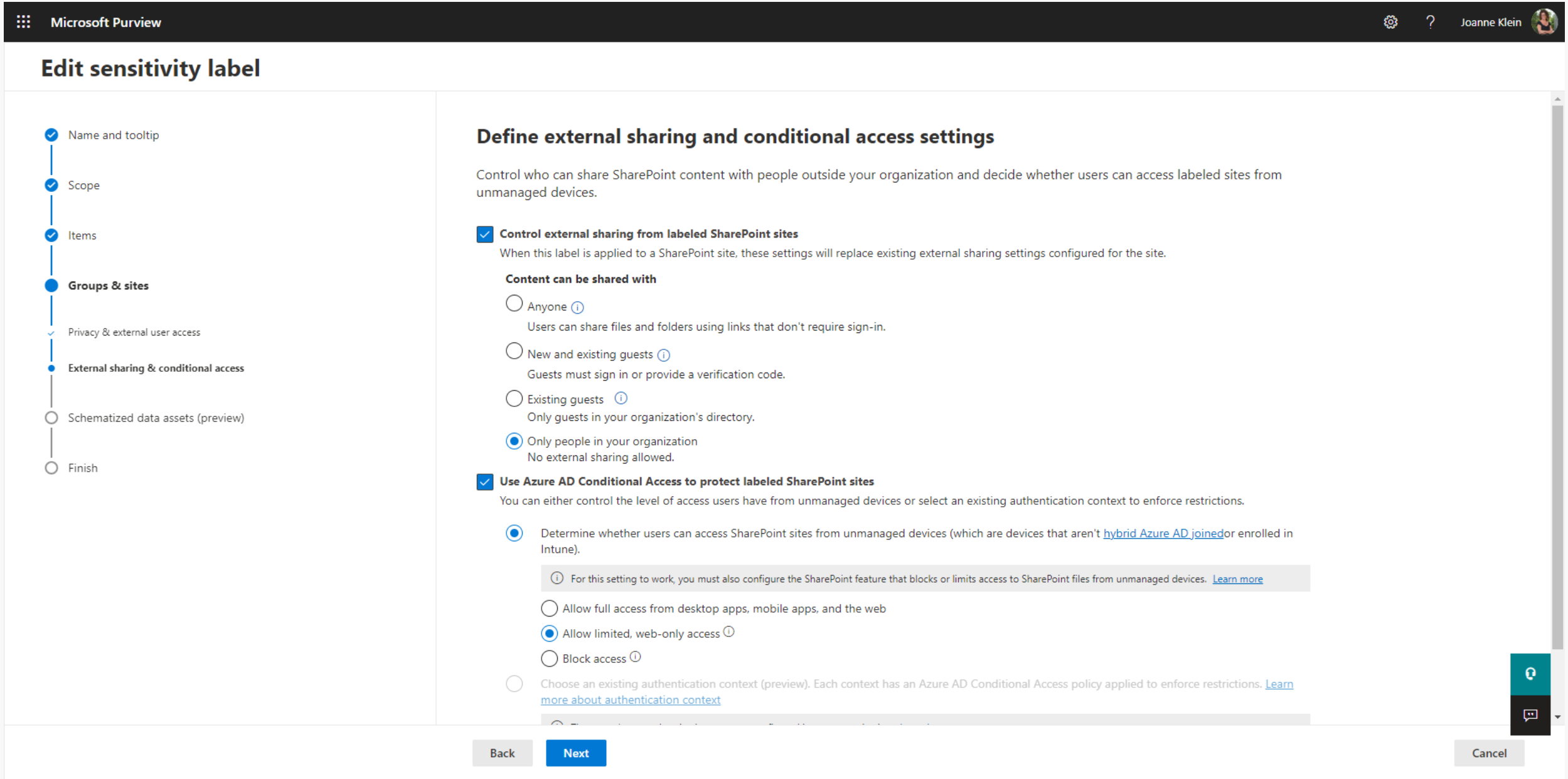
Default sharing link, Site sharing settings: PowerShell-only configuration

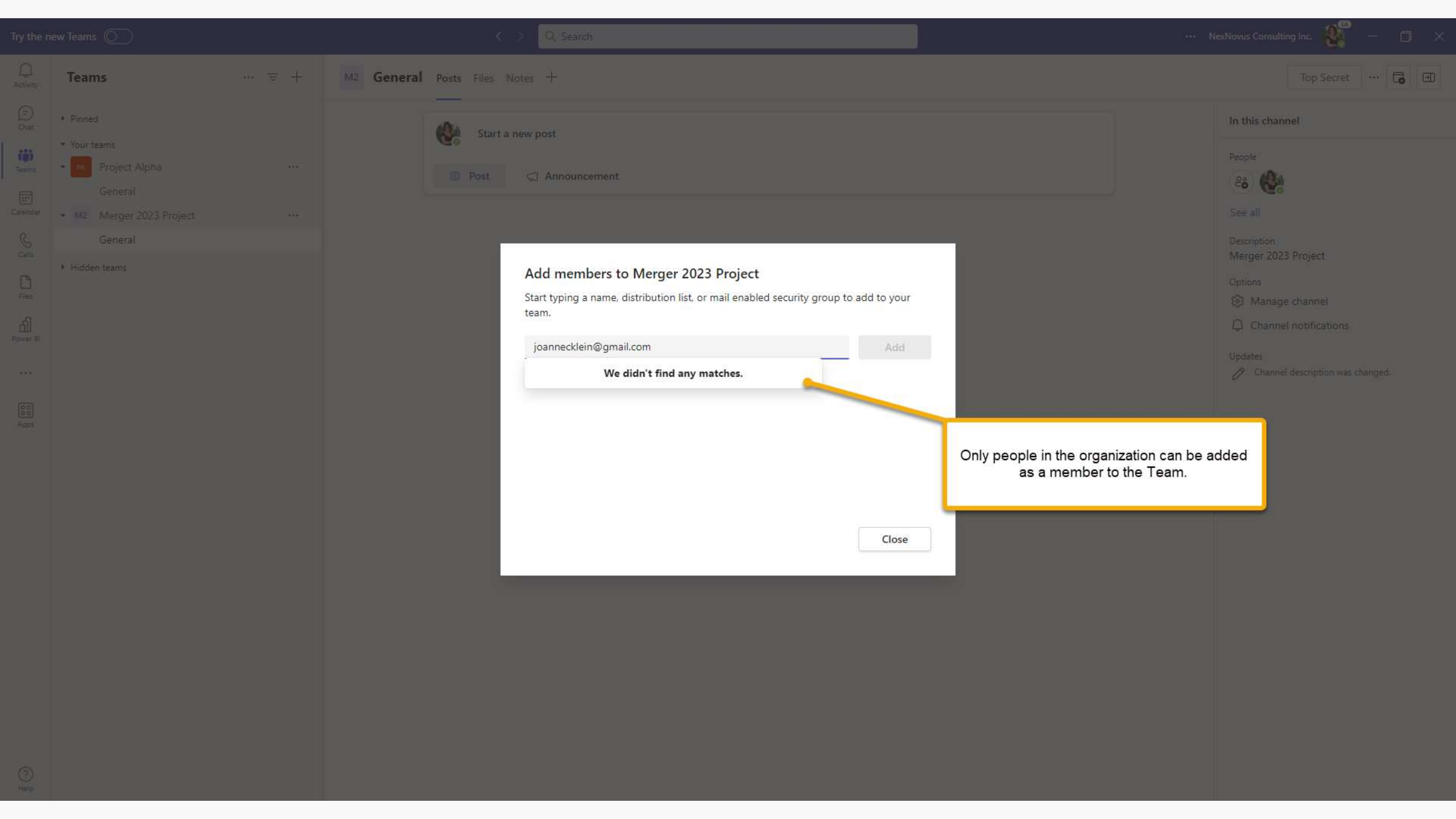
What it does NOT do: Automatically label everything on the Group/site with the same sensitivity label

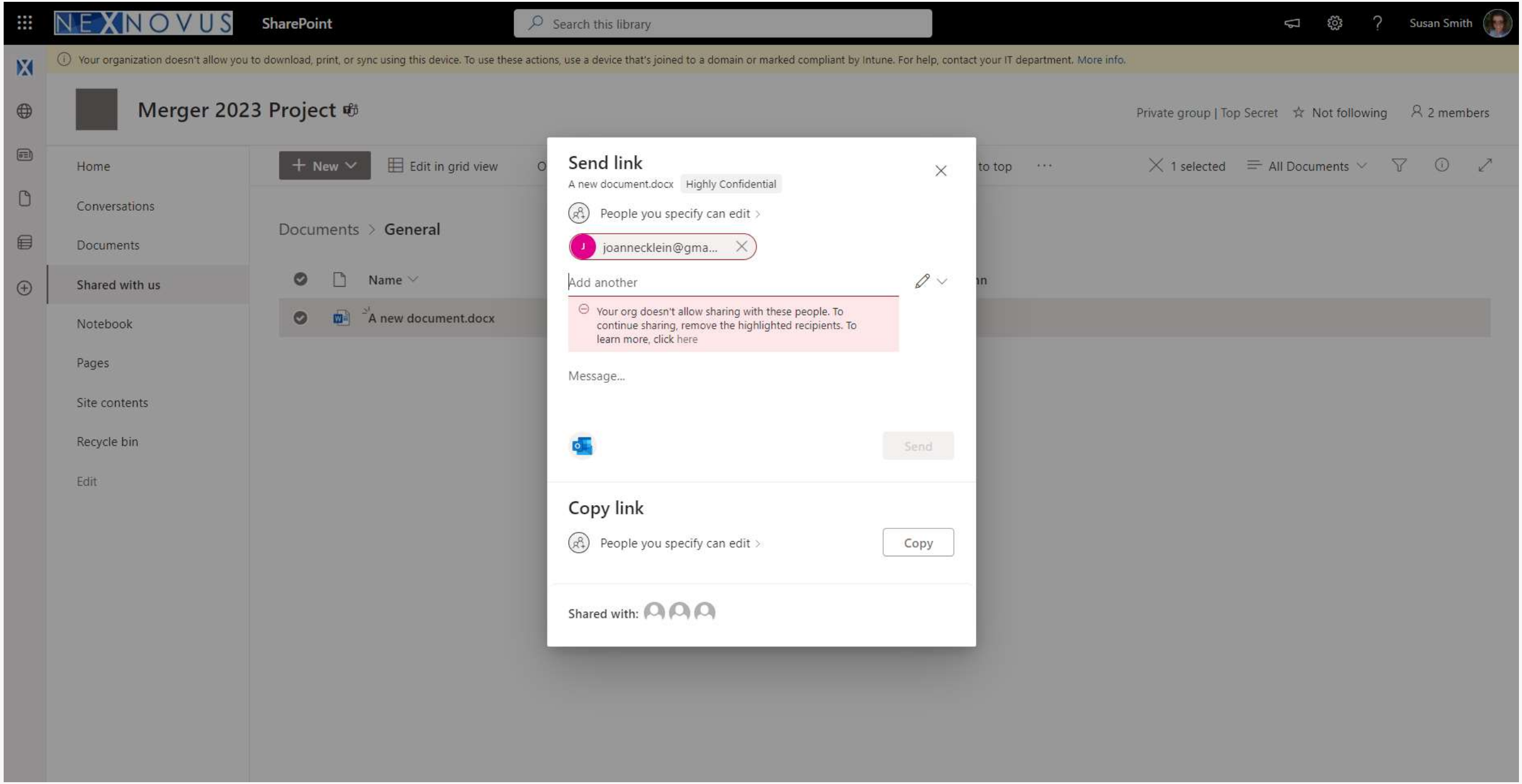
Information Protection

DEMO

A ‘TOP SECRET’ CONTAINER SENSITIVITY LABEL EXAMPLE




Try the new Teams
Search
NexNovus Consulting Inc.
Teams
Pinned
Your teams
Project Alpha
General
Merger 2023 Project
General
Hidden teams
M2 General
Posts
Files
Notes
Top Secret
Start a new post
Post
Announcement
In this channel
People
See all
Description
Merger 2023 Project
Options
Manage channel
Channel notifications
Updates
Channel description was changed.
Add members to Merger 2023 Project
Start typing a name, distribution list, or mail enabled security group to add to your team.
joannecklein@gmail.com
Add
We didn't find any matches.
Close
Only people in the organization can be added as a member to the Team.

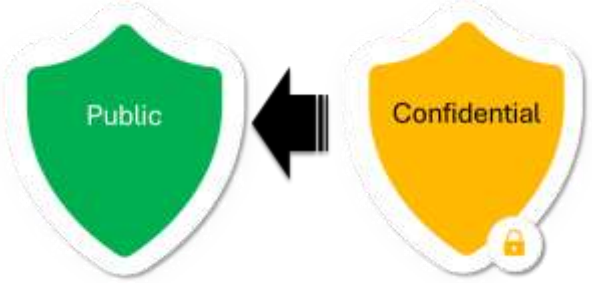

NEXNOVUS
SharePoint
Search this library
Susan Smith
Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune. For help, contact your IT department. More info.
Merger 2023 Project
Private group | Top Secret
Not following
2 members
Home
Conversations
Documents
Shared with us
Notebook
Pages
Site contents
Recycle bin
Edit
New
Edit in grid view
to top
1 selected
All Documents
Documents > General
Name
A new document.docx
Send link
A new document.docx
Highly Confidential
People you specify can edit
joannecklein@gma...
Add another
Your org doesn't allow sharing with these people. To continue sharing, remove the highlighted recipients. To learn more, click here
Message...
Send
Copy link
People you specify can edit
Copy
Shared with:

Before handing in her resignation, Jane downloads confidential Teams files to her laptop and copies them to a USB.

How can **Information Protection** help with this scenario?

- **Sensitivity label** remains with a document wherever the end-user takes it
- **Priority** sensitivity labels are an indicator for **risky activity**

- **Downgrading** a label can be an indicator for **risky activity**



Information Protection for Teams channels

CHANNEL TYPE	PROTECTION CONTROLS AVAILABLE
Standard	• Guest access controlled by either a Team **sensitivity label** or the org-level setting • External sharing setting for all standard channels inherits from the Parent Team's **sensitivity label** if one is applied
Private	• Inherits the **sensitivity label** from the parent team (synchronized) • Allow guests (if allowed by **sensitivity label** and org-level setting) • External sharing setting for all private channels inherits from the Parent Team's **sensitivity label** if one is applied
Shared	• Uses external federation via cross-tenant access policies rather than guest access • Inherits the **sensitivity label** from the parent team when initially created; however, it is NOT synchronized for future changes • External sharing setting is determined from the **sensitivity label** of the SharePoint site associated with the Shared Channel

Information Protection for Viva Engage Communities

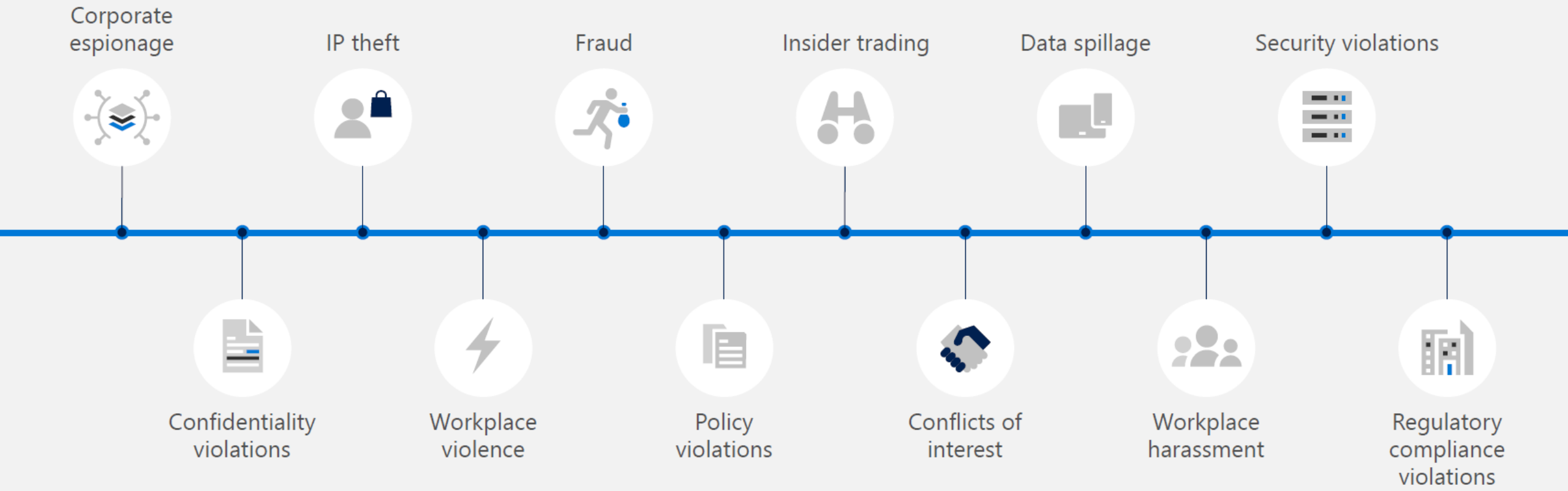
COMMUNITY SETTING	PROTECTION CONTROLS AVAILABLE
Public or Private	• Viva Engage admin settings • Anyone in your network can view and join this community (Public) OR only approved community members can view or participate (Private
Internal or External	• To collaborate with people inside/outside your organization
Sensitivity label for the “Container”	• **Currently not supported**
Sensitivity labels on the files for the community	• Supported. These work the same way as files in any other type of SharePoint site

Microsoft Purview Insider Risk Management and Adaptive Protection

What business problem are we trying to solve with Insider Risk Management?

"Prevent data exfiltration from malicious and negligent workers in an intelligent and automated way."

Organizations face a broad range of risks from insiders



The path leading to a malicious insider risk

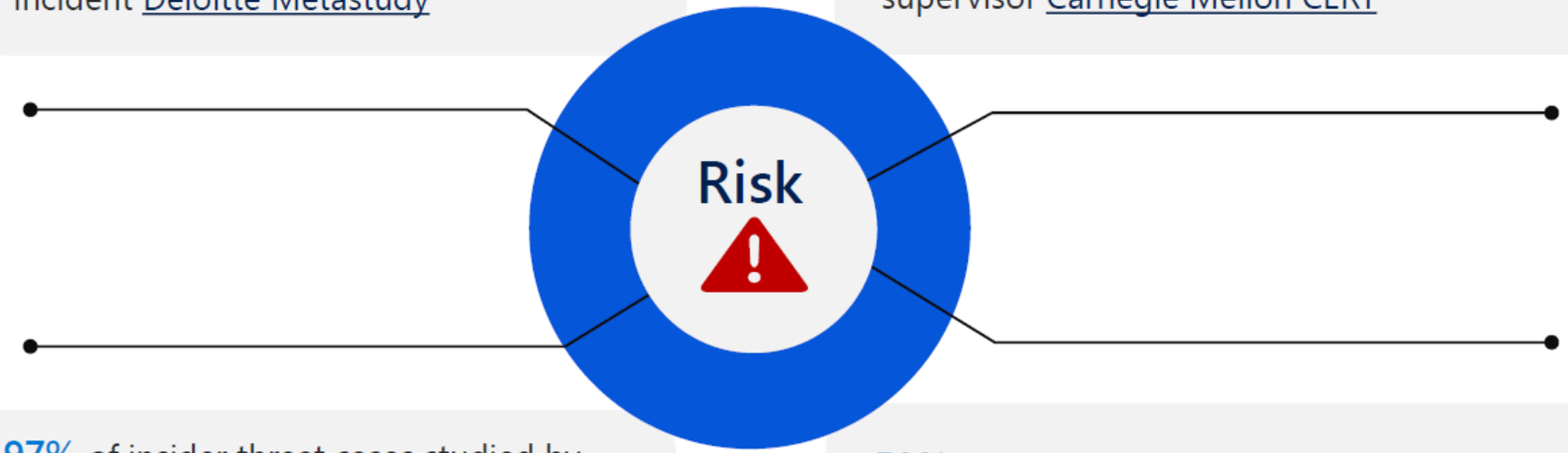
Identifying indicators across phases of the critical-path can help to enable higher fidelity detections

Predisposition

51% of employees involved in an insider threat incident had a history of violating IT security policies leading up to the incident Deloitte Metastudy

Stressor

92% of Insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor Carnegie Mellon CERT



97% of insider threat cases studied by Stanford University involved an employee whose behavior a supervisor had flagged, but the organization failed to follow up on Deloitte Metastudy

Concerning Behavior

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them Deloitte Metastudy

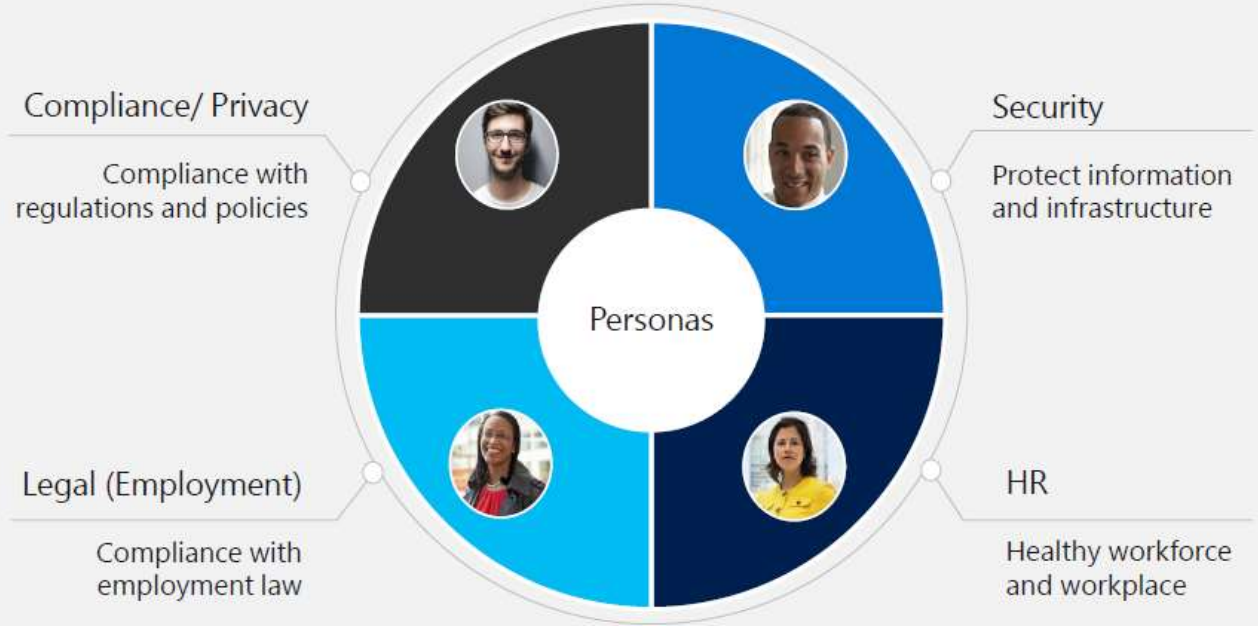
Planning & Preparation

Designing an intelligent insider risks solution

Transparent
Balance employee privacy versus the organization's risk

Intelligent
Leverage machine learning to identify hidden patterns

Integrated
Integrated workflows to support collaboration to address risks



Insider Risk Management can understand…

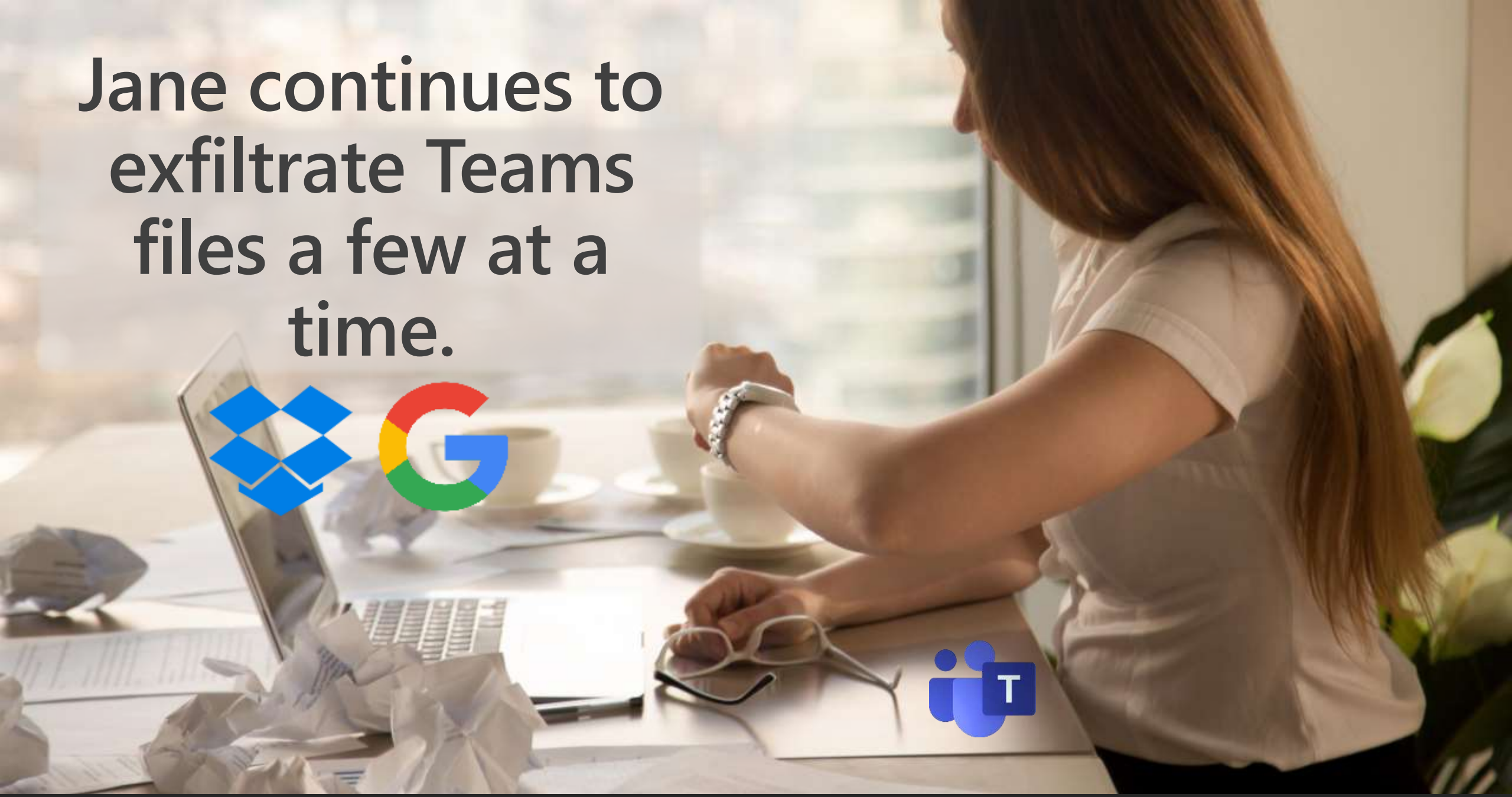
- **Indicators** for "risky activity" (a small sample)

Office indicators	Device indicators	Sequence detection
• Download from SharePoint • Downgrade sensitivity labels • Delete SharePoint files	• Copy files to USB • Delete files from a device	• Potentially risky activities done in sequence

- **User context and intent** across risky activity

Automatically includes Jane in a data theft policy.

Jane continues to exfiltrate Teams files a few at a time.



INSIDER RISK MANAGEMENT (IRM) USE-CASE EXAMPLE

Resignation notice

Termination date

HR system logs resignation and termination date

DATA THEFT POLICY TRIGGERING EVENT

Begin assigning risk scores to Jane's activities. Includes past activity detection up to 90 days; 10 days for email.

DATA THEFT POLICY SETTINGS

POLICY TRIGGER

- HR resignation/termination event
- User account deleted from Azure AD

+

ACTIVITIES TO MONITOR

- Downloading files from SPO/OD
- Printing files, Deleting files, sharing w/external
- Copying data to cloud storage
- Emailing outside org with attachments
- Downgrading/removing sensitivity labels

Examples only. Many more activities available

+

CONTENT TO PRIORITIZE

- SharePoint sites
- Sensitivity labels
- Sensitive information types
- File extensions
- Trainable Classifiers

+

DETECTION OPTIONS

- Sequence detection
- Cumulative exfiltration detection
- Risk score boosters

Jane provides notice of resignation

IRM ALERT GENERATED FOR MATCHING ACTIVITY DETECTED FOR JANE

JANE'S RISK LEVEL SET TO "ELEVATED" DUE TO HER ACTIVITY

SENSITIVE SHAREPOINT SITES ACCESSED

FILES DOWNLOADED FROM SHAREPOINT

EMAILS WITH SENSITIVE ATTACHMENTS SENT OUTSIDE THE ORG

Example of sequence detection

JANE WORKS UNTIL TERMINATION DATE. ACTIVITY IS MONITORED.

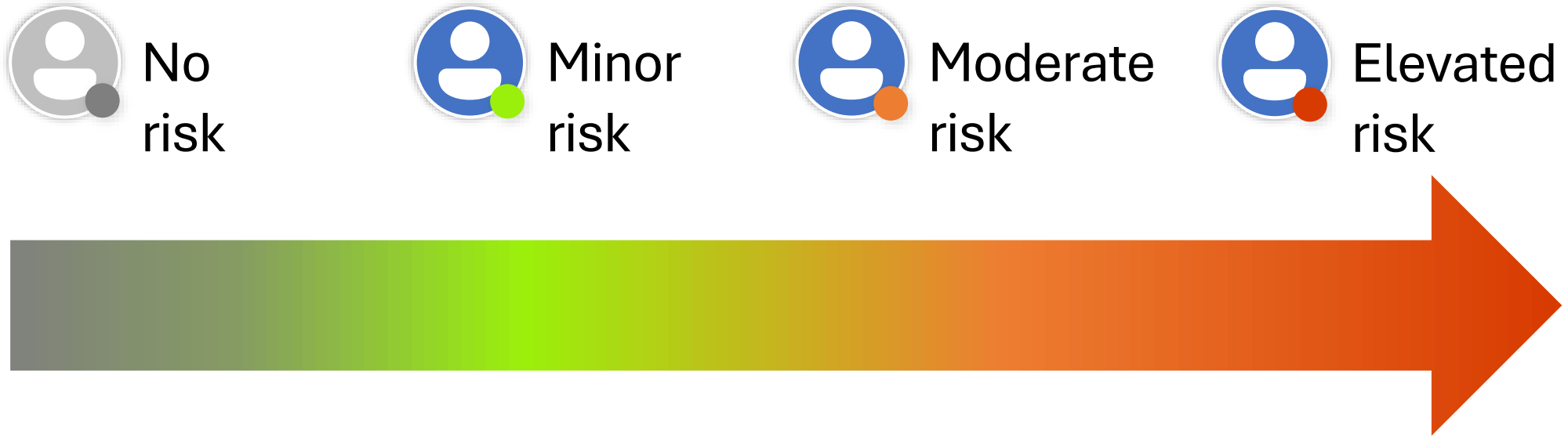
Termination date

How can **Insider Risk Management** help with this scenario?

- Monitors **past and future** activity
- Detects **exfiltration** activities:
- Continuously evaluates Jane's **risk level**

Insider Risk Management uses Adaptive Protection

Adaptive Protection assigns a risk level to a user based on their data-related activity



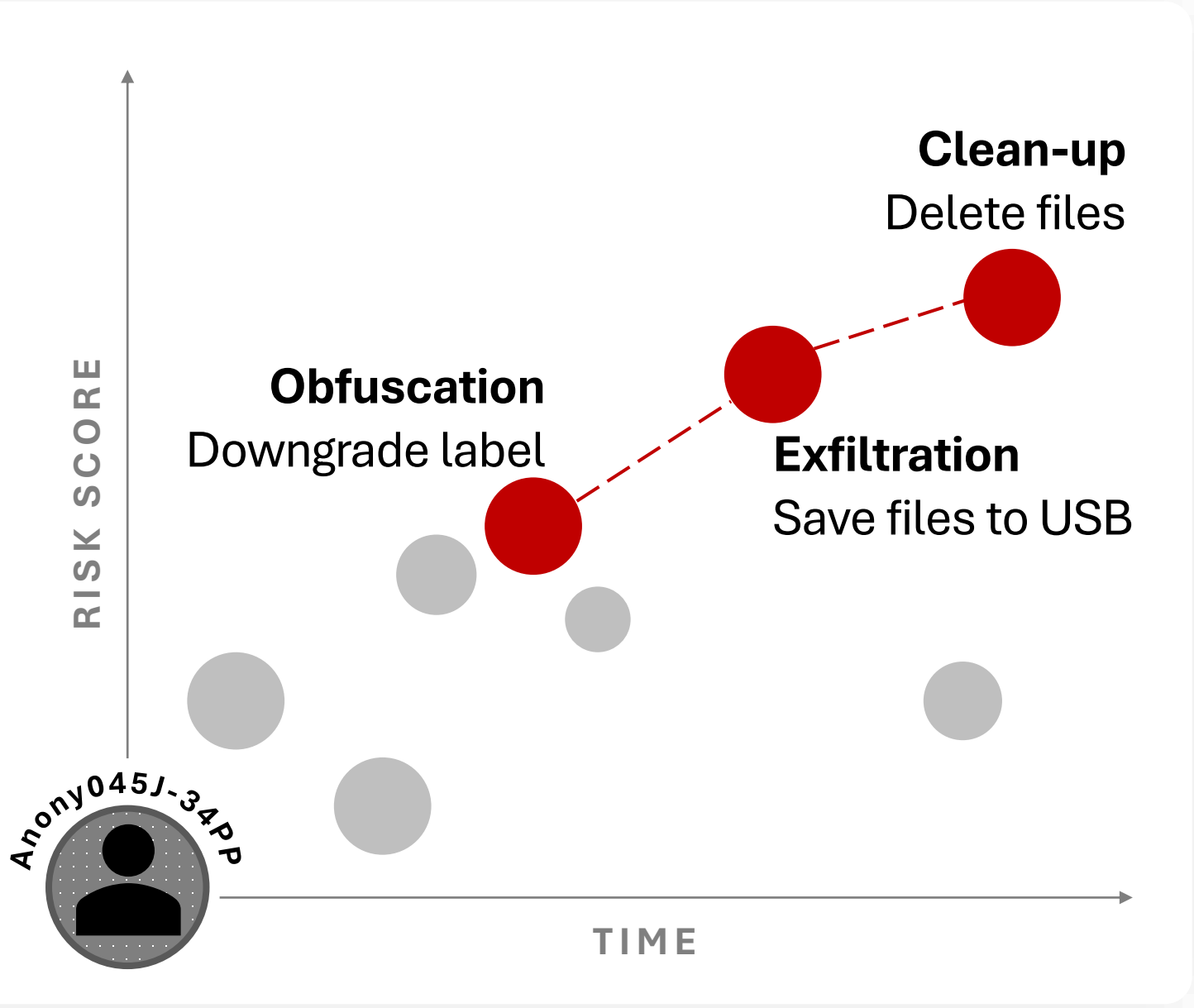
Elevated risk

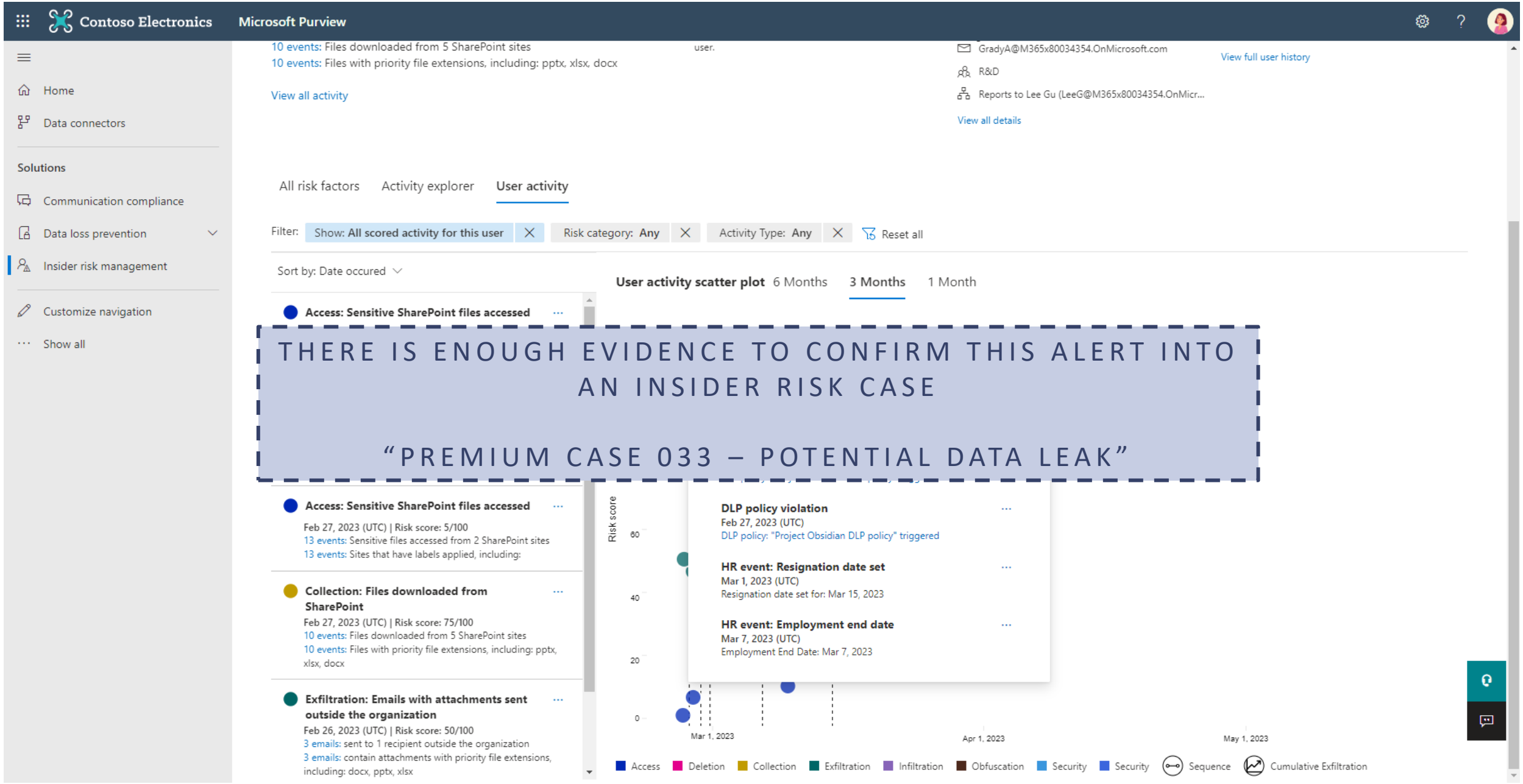
Moderate risk

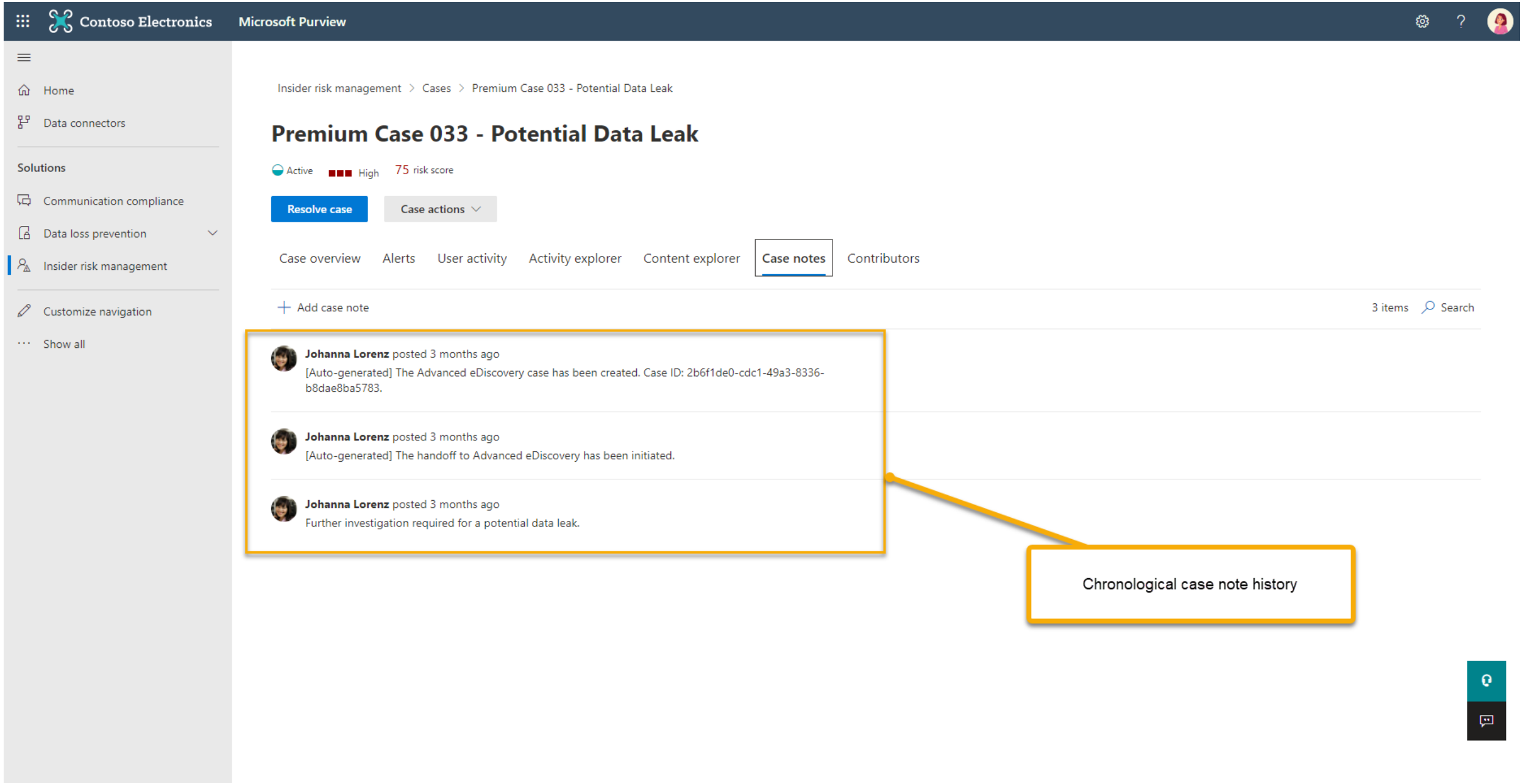
Minor risk

No risk

Jane Doe's activities over time




Contoso Electronics
Microsoft Purview
Home
Data connectors
Solutions
Communication compliance
Data loss prevention
Insider risk management
Customize navigation
Show all
10 events: Files downloaded from 5 SharePoint sites
10 events: Files with priority file extensions, including: pptx, xlsx, docx
View all activity
user.
GradyA@M365x80034354.OnMicrosoft.com
R&D
Reports to Lee Gu (LeeG@M365x80034354.OnMicr...
View full user history
View all details
All risk factors
Activity explorer
User activity
Filter:
Show: All scored activity for this user
Risk category: Any
Activity Type: Any
Reset all
Sort by: Date occured
User activity scatter plot
6 Months
3 Months
1 Month
Access: Sensitive SharePoint files accessed
THERE IS ENOUGH EVIDENCE TO CONFIRM THIS ALERT INTO AN INSIDER RISK CASE
"PREMIUM CASE 033 – POTENTIAL DATA LEAK"
Access: Sensitive SharePoint files accessed
Feb 27, 2023 (UTC) | Risk score: 5/100
13 events: Sensitive files accessed from 2 SharePoint sites
13 events: Sites that have labels applied, including:
Collection: Files downloaded from SharePoint
Feb 27, 2023 (UTC) | Risk score: 75/100
10 events: Files downloaded from 5 SharePoint sites
10 events: Files with priority file extensions, including: pptx, xlsx, docx
Exfiltration: Emails with attachments sent outside the organization
Feb 26, 2023 (UTC) | Risk score: 50/100
3 emails: sent to 1 recipient outside the organization
3 emails: contain attachments with priority file extensions, including: docx, pptx, xlsx
Risk score
60
40
20
0
DLP policy violation
Feb 27, 2023 (UTC)
DLP policy: "Project Obsidian DLP policy" triggered
HR event: Resignation date set
Mar 1, 2023 (UTC)
Resignation date set for: Mar 15, 2023
HR event: Employment end date
Mar 7, 2023 (UTC)
Employment End Date: Mar 7, 2023
Mar 1, 2023
Apr 1, 2023
May 1, 2023
Access
Deletion
Collection
Exfiltration
Infiltration
Obfuscation
Security
Security
Sequence
Cumulative Exfiltration


Contoso Electronics
Microsoft Purview
Home
Data connectors
Solutions
Communication compliance
Data loss prevention
Insider risk management
Customize navigation
Show all
Insider risk management > Cases > Premium Case 033 - Potential Data Leak
Premium Case 033 - Potential Data Leak
Active
High
75 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content explorer
Case notes
Contributors
Add case note
3 items
Search
Johanna Lorenz posted 3 months ago
[Auto-generated] The Advanced eDiscovery case has been created. Case ID: 2b6f1de0-cdc1-49a3-8336-b8dae8ba5783.
Johanna Lorenz posted 3 months ago
[Auto-generated] The handoff to Advanced eDiscovery has been initiated.
Johanna Lorenz posted 3 months ago
Further investigation required for a potential data leak.
Chronological case note history

Microsoft Purview
Data Loss Prevention (DLP)

What business problem are we trying to solve with DLP?

"When users are collaborating with sensitive content, we need to prevent its exfiltration (inadvertent or malicious)."

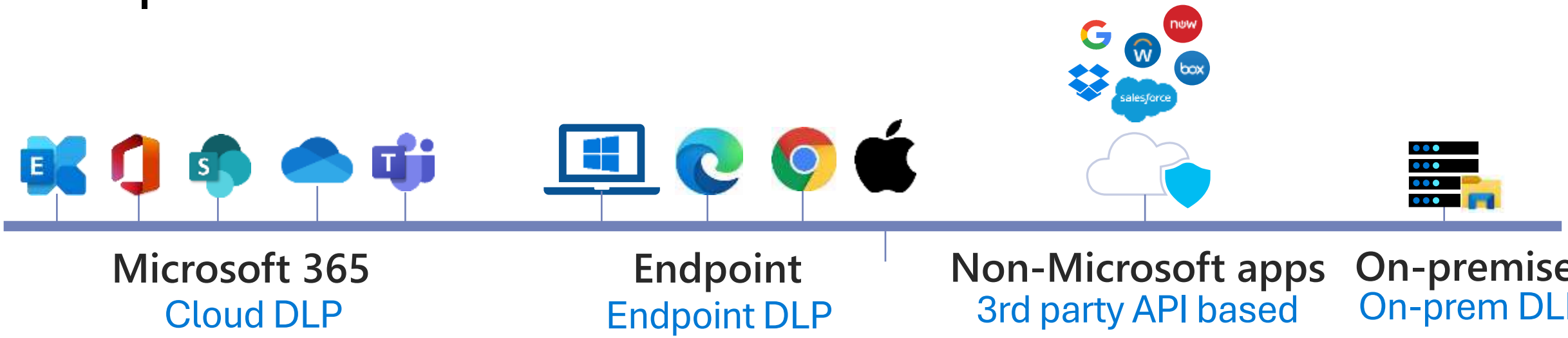
Why do organizations need DLP?

Almost all data leakage occurs inadvertently

Protection without inhibiting productivity

Users need guidance to make the right decisions

DLP | Unified and cloud-native solution



- **Prevent unauthorized use** of sensitive data:
  - Examples: emailing, storing, copying, printing

- Leverage classifiers, labeling, and user risk to **finetune and dynamically adapt**

Data Loss Prevention locations

Status	Location	Included	Excluded
On	Exchange email	All Choose distribution group	None Exclude distribution group
On	SharePoint sites	All Choose sites	None Exclude sites
On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
On	Devices	All Choose user or group	None Exclude user or group
On	Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
On	On-premises repositories	All Choose repositories	None Exclude repositories
Off	Power BI		

Viva Engage messages are not supported by DLP!

But… files shared within a Viva Engage community (SharePoint and OneDrive) are!

DLP is Integrated with information protection

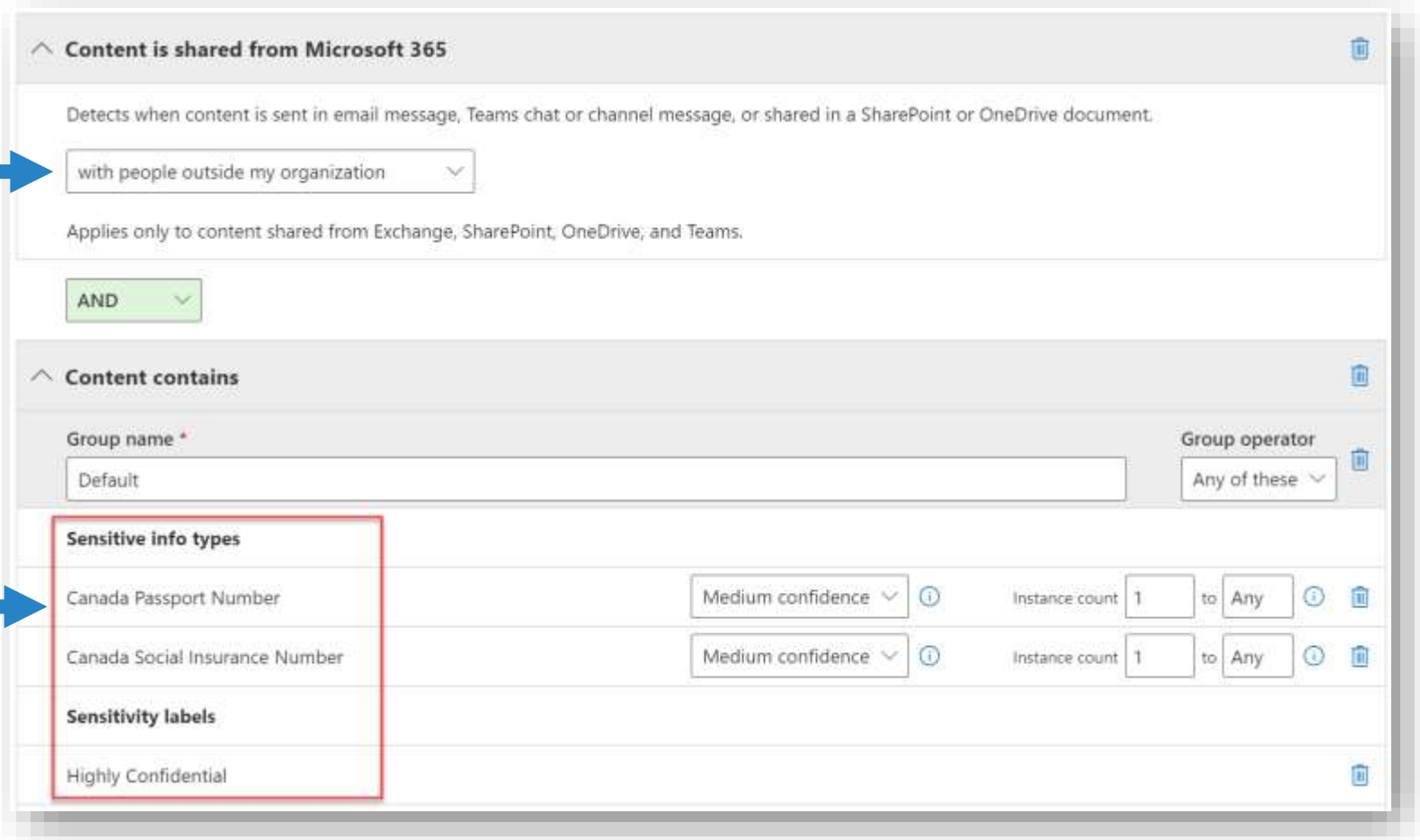
- Many things can be used as a DLP policy condition
  - Sensitivity label, Trainable classifier, Sensitive information types, Retention label

A DLP use-case

If a SharePoint file is being shared with someone outside of the organization

AND

Canadian PII is detected in a SharePoint site file OR it is labeled ‘Highly Confidential’ …



DLP is Integrated with information protection

A DLP use-case

... Then:

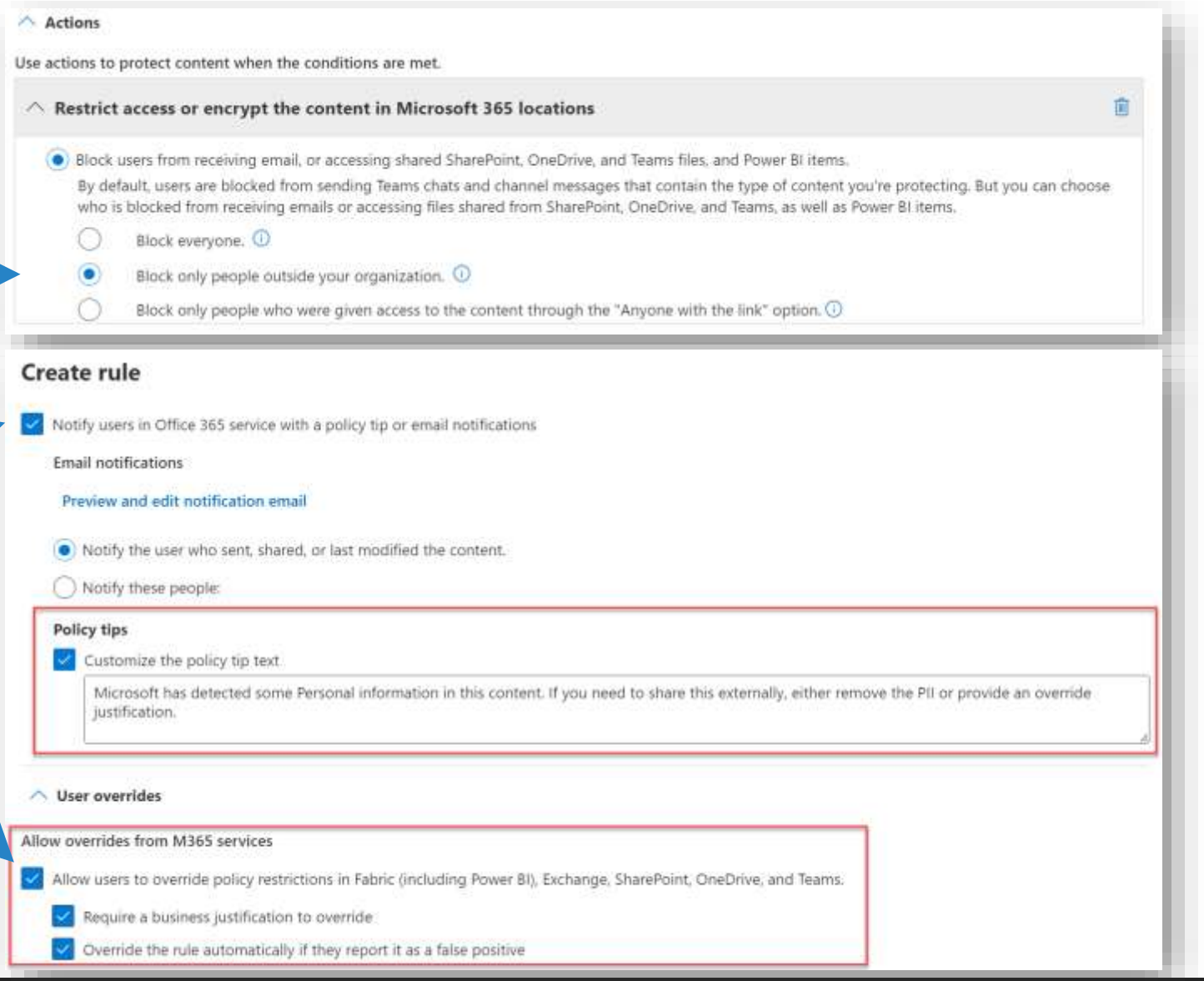
Block it

AND

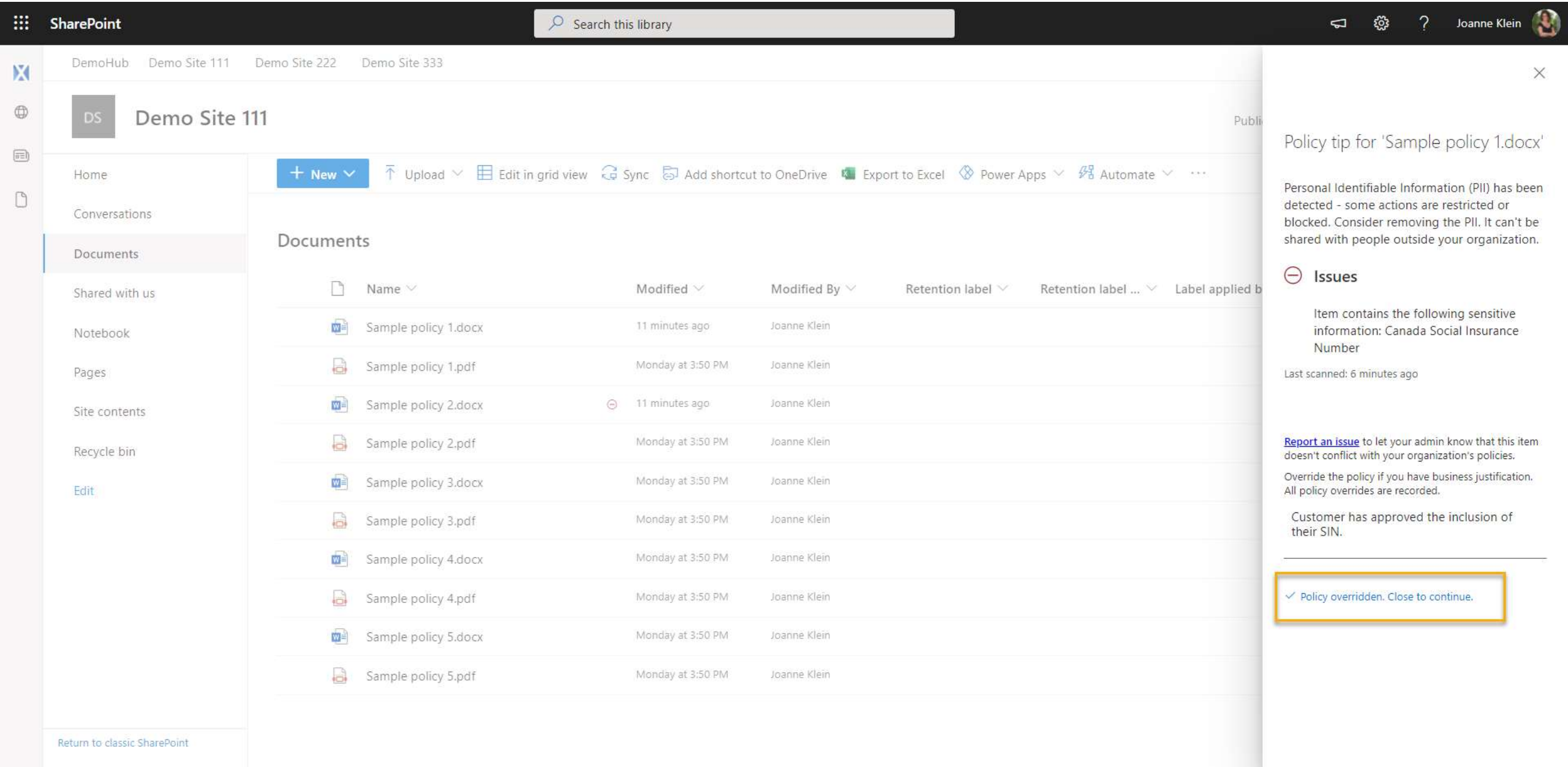
Show policy tip to the end-user

AND

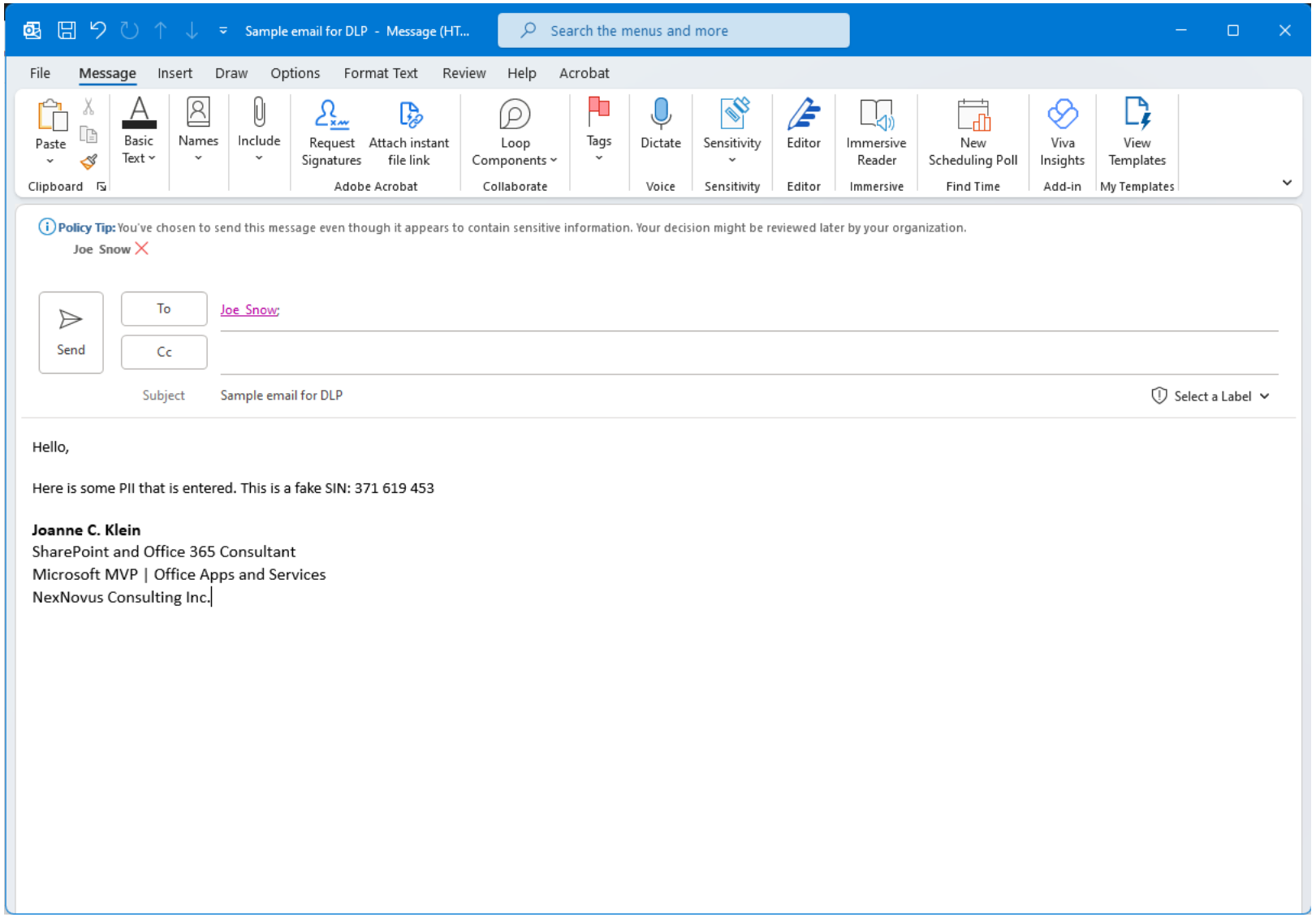
Require an override before allowing the share.



Where end-users see DLP in SharePoint/OneDrive



Sending an email containing PII to an external recipient



Data Loss Prevention

DEMO

A User's risk level informs **Data Loss Prevention**

Adaptive Protection

Detect risky data activity and assign a risk level to the user

Data Loss Prevention

Dynamically apply controls based on a user 's risk level

How can **Data Loss Prevention** help with the "departing, disgruntled employee" scenario?

- DLP policies **automatically adapt** to elevated risk level:

- Other (less risky) users are not blocked

Microsoft Purview
Data Lifecycle & Records Management

What business problems are we trying to solve with Data Lifecycle and Records Management?

"We need to reduce the risk of over-retaining content."

"We need to retain business records created/stored in our collaboration areas."

"We want to ensure obsolete content is gone so Copilot has better quality data to work with."

Data Lifecycle and Records Management

Retain content

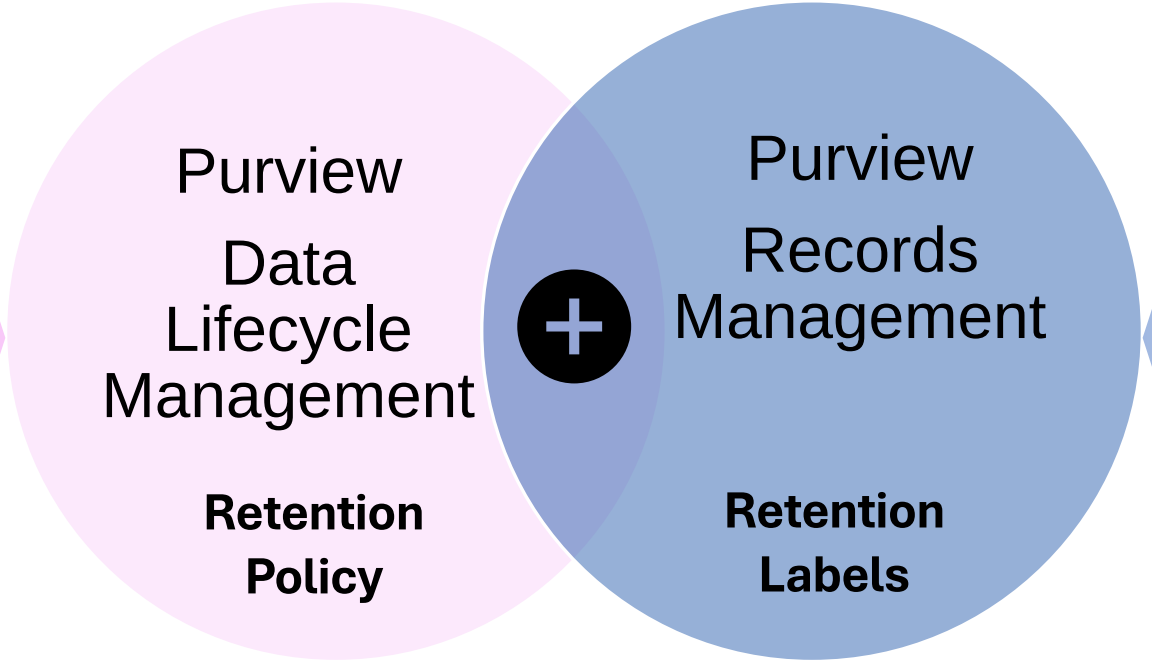
Reduce ROT

Preserve records

Data Lifecycle Management and Records Management are cornerstones of Good Data Governance

Ensure you are retaining content for as long as you are obligated to retain it and removing it as soon as you can.

Over-retaining content can be a risk and contributes to redundant, **obsolete**, and trivial content cluttering your environment.



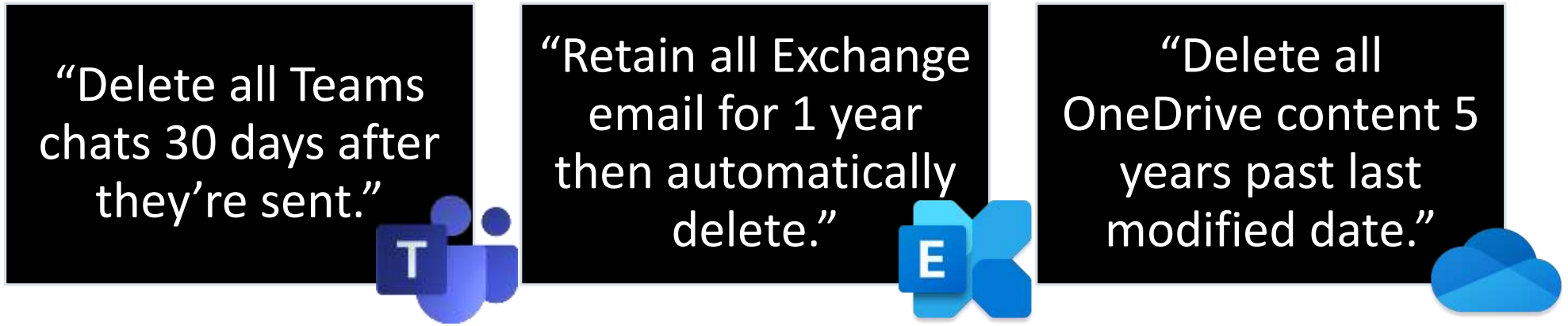
Records have value to an organization and serve as evidence of business transactions, decisions, or activities and are typically **retained for a specified period** to meet legal, regulatory, operational, or historical requirements.

These 2 Purview features help to provide governance to ground an organization's content, so Copilot has better information to leverage.

What is a retention policy?

It applies retention settings to **everything** in a "location" such as an Exchange mailbox, SharePoint site*, or OneDrive site.

- Examples I've seen with my customers:



They help reduce ROT (redundant, obsolete, trivial) content across your tenant

They reduce your data footprint (and therefore data risk)

Recommend to **use them alongside retention labels** for exceptions in SharePoint and Exchange

End user is (mostly) unaware that a retention policy is in effect

**Any kind of SharePoint site (can be connected to a Microsoft Team or Viva Engage community, but doesn't have to be)*

What is a retention label?

It applies retention settings to **individual items** (file, email) stored in Exchange, SharePoint*, and OneDrive to meet your organization's legal, regulatory, and business requirements.

Once applied to an item, end users can see it, apply it, and in some cases, remove it.

It typically aligns to the record codes in your retention schedule. Examples:

Retention Label name	What it does once applied to a document…
Contract	Retains the document for 2 years past contract end date; then reviewed before deletion.
Board meeting minutes	Retains permanently.
Insurance assessments	Retains for 5 years past last modified and automatically deleted.

Only 1 retention label can be applied to an item at a time

They are published or auto-applied to content with a retention label policy

**Any kind of SharePoint site (can be connected to a Microsoft Team or Viva Engage community, but doesn't have to be)*

Data Lifecycle & Records Management

DEMO

Applying Retention Labels across SharePoint, Teams, and Viva Engage

There are **many** ways to apply a retention label to your content.

All the options you choose become part of your overall retention design and implementation.

Manually apply the label

1. Manually apply a retention label to a file

Default the label

2. Default the label based on the library, folder, or document set the file is stored in

Auto-apply the label

3. Managed properties (uses KQL queries)
4. Words and Phrases
5. Sensitive Information Types (SITs)
6. Pre-trained and custom Trainable Classifiers
7. Code / Script
8. SharePoint Premium document models

Example: auto-apply a retention label based on your SharePoint information architecture

SharePoint content types and metadata can be used to auto-apply a retention label to content in SharePoint (any type of site, including a site backing a Microsoft Team or Viva Engage Community)

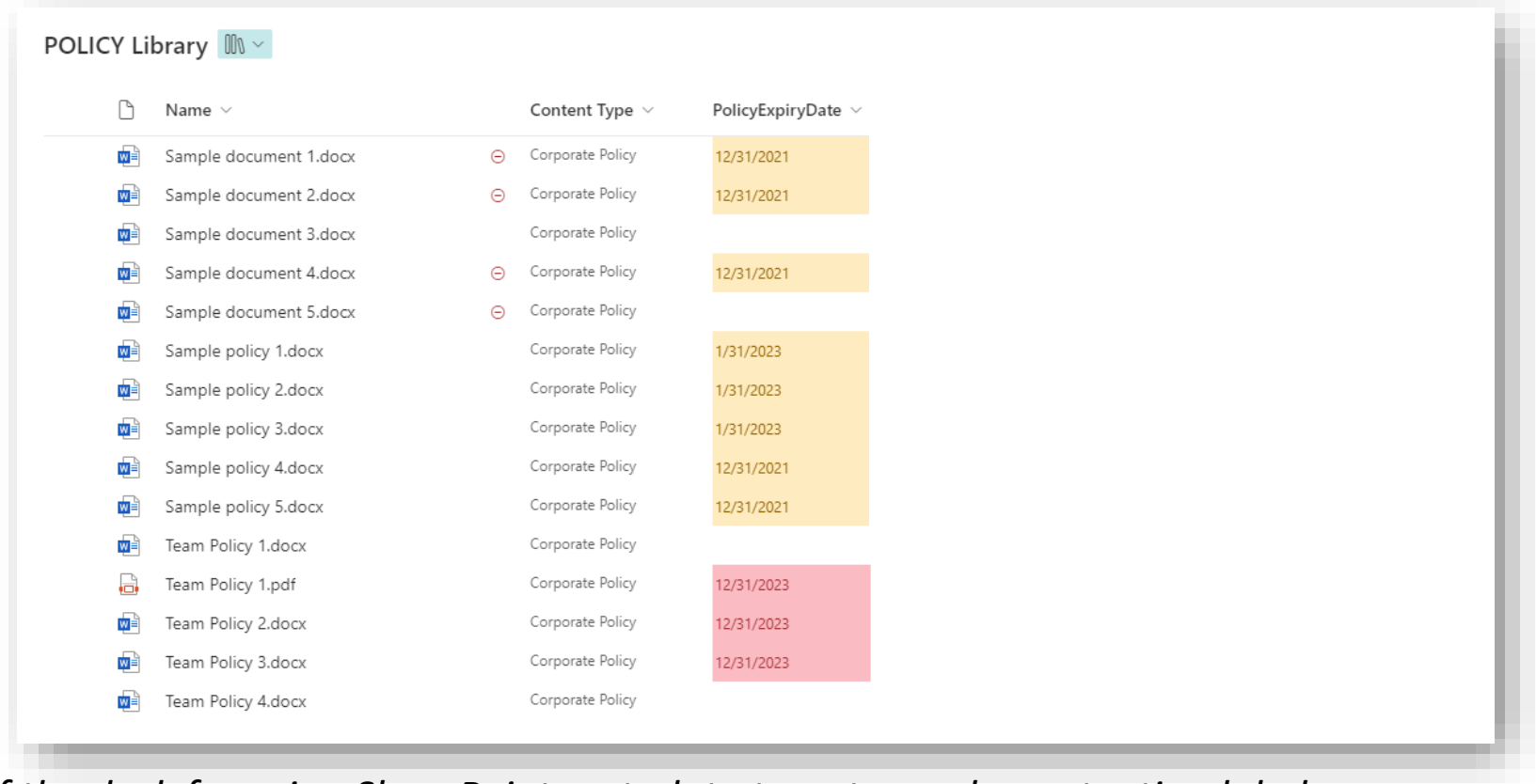
EXAMPLE:

"START RETENTION WHEN A CORPORATE POLICY IS EXPIRED"

KQL in the retention label policy:

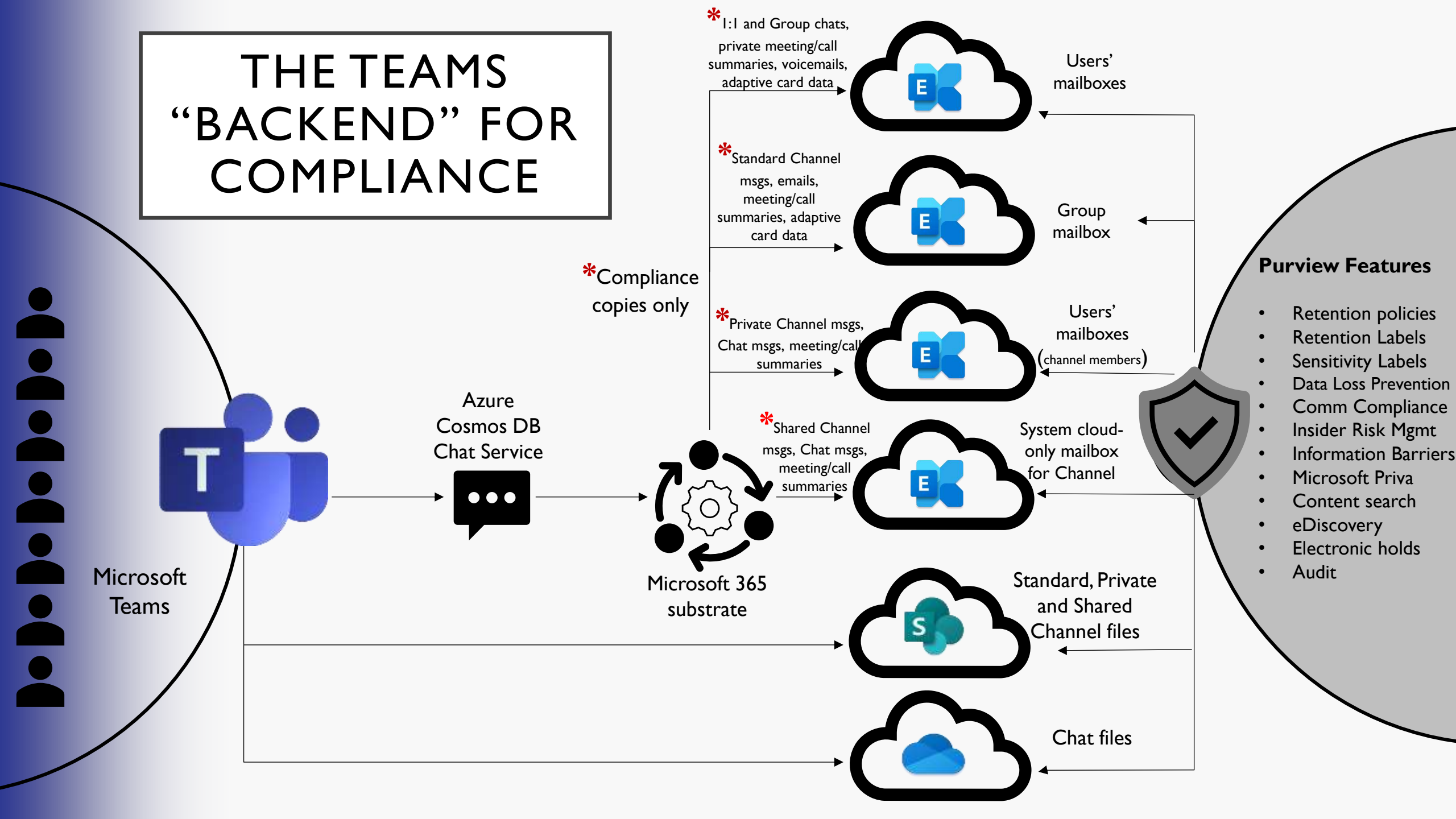
ContentType:"Corporate Policy" AND PolicyExpiryDate<TODAY

TODAY was 01/01/2022 in this example



Download my tip sheets at the end of the deck for using SharePoint metadata to auto-apply a retention label.

THE TEAMS "BACKEND" FOR COMPLIANCE



THE VIVA ENGAGE "BACKEND" FOR COMPLIANCE

*User messages and community messages where user is @ mentioned, storyline posts

Users' mailboxes

*Compliance copies only if Viva Engage network is configured in native mode

*Community messages

Group mailbox

Yammer data store

Viva Engage

Microsoft 365 substrate

Community files

User message files

Purview Features*

- Retention policies
- Retention Labels
- Sensitivity Labels
- Data Loss Prevention
- Comm Compliance
- Insider Risk Mgmt
- Information Barriers
- Microsoft Priva
- Content search
- eDiscovery
- Electronic holds
- Audit

***Not all Purview services available for Viva Engage**

Jane deletes “her” Team files from SharePoint.

Adaptive Protection in Data Lifecycle Management

No risk
Minor risk

Moderate Risk

No action when user deletes content

Elevated Risk

User deletes content

Policy preserves the data

File can be restored if needed

User is dynamically added to a Data Lifecycle Management policy that preserves any data they delete

How can **Data Lifecycle and Records Management** help with this scenario?

- A **retention policy** can ensure deleted content is preserved (without Jane knowing).

- Due to Jane's elevated risk, a **retention label** is auto-applied to any SP/Teams files she deletes ensuring the files are preserved.

Back to Jane Doe's activities… how can Purview help?

Jane Doe

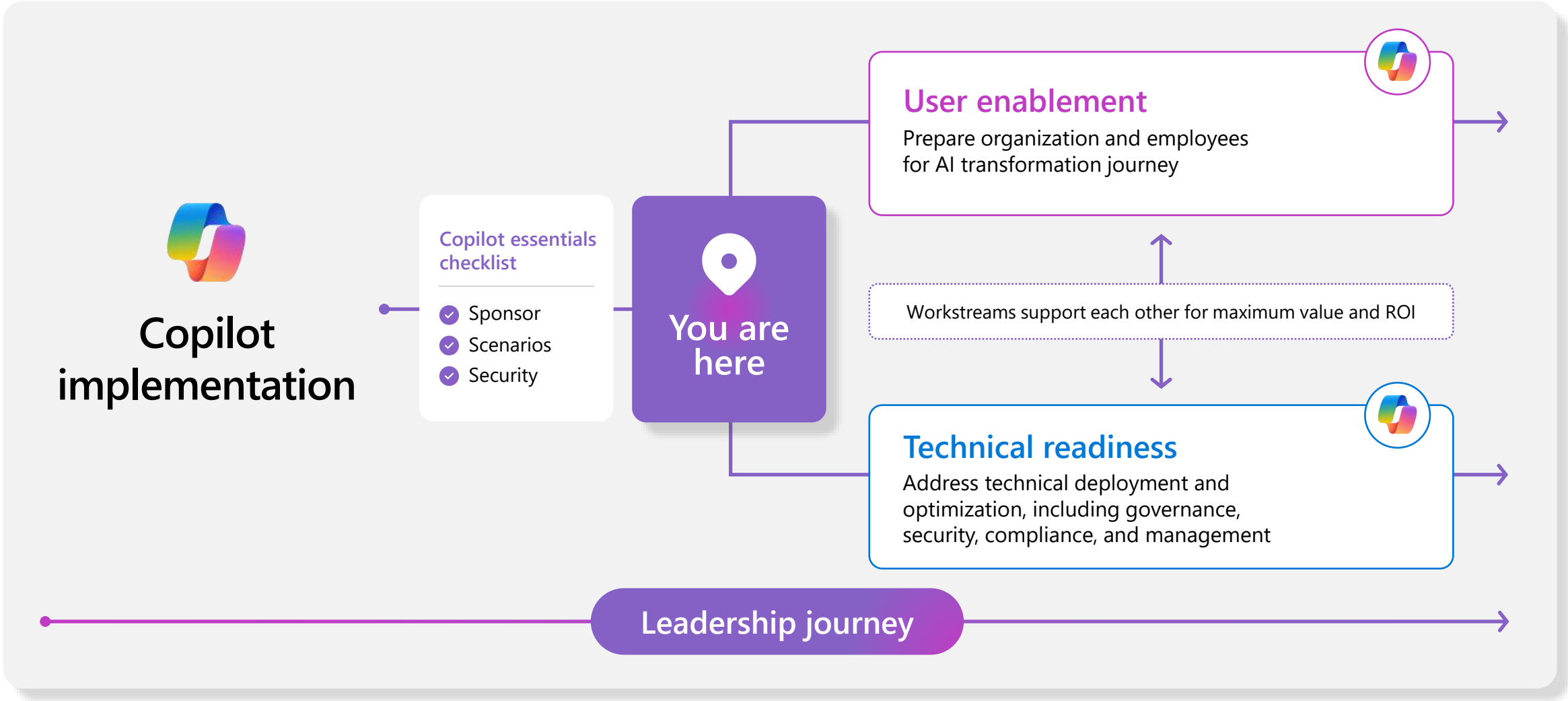
Trusted employee for 5 years

Prior to resigning, Jane downloads confidential files to USB.	Jane hands in her official resignation to HR.	Jane continues to exfiltrate files to her Dropbox and email.	Jane deletes the files from SharePoint including recycle bins.	Jane was successful at exfiltrating several sensitive documents.
Classify data with **Information Protection.** Apply protection controls to sensitive content.	Use **Insider Risk Management** to evaluate Jane's data-related activity and assign a risk level using **Adaptive Protection**.	Use Jane's risk level to block some of her risky activity with **Data Loss Prevention.**	Use **Data Lifecycle Management** and **Adaptive Protection** to protect against malicious activity.	Escalate the **Insider Risk Management** case to legal team with **eDiscovery Premium**.

Microsoft Purview data security

Copilot for Microsoft 365

Copilot for Microsoft 365 implementation



User enablement

Essentials for Copilot success

Nominate and activate your Copilot executive sponsors, in partnership with your AI Council

Accelerate your business impact by defining highest value scenarios

Define your path to secure your data for compliance and peace of mind

Copilot for Microsoft 365

Implementation overview

	Get ready	Onboard & engage	Deliver impact	Extend & optimize
USER ENABLEMENT	**User Enablement Workstream** Secure exec sponsorship, create AI Council, and define RAI principles Identify success owners, Champions, and early adopter cohorts Detail high value scenarios and personas Be intentional with assignment and concentrate seats Define success criteria, KPIs, and success measurement plan	Complete User Enablement Strategy training Define user experience and feedback strategy Design and deploy training and engagement community (Center of Excellence/Champion Platform) Launch employee communications and Champion program Onboard executives and user cohorts Deliver user Champions and support staff training	Review success measures and user survey results Conduct feedback and reporting analysis Deliver extended training and adoption support Identify additional optimization scenarios Iterate user experience strategy Gather and amplify success stories	Extend to new high value scenarios Deliver business process transformation with Copilot Studio, plugins, and connectors Drive group and cross-organizational productivity and innovation Understand custom line of business opportunities
TECHNICAL READINESS	**Technical Readiness Workstream** Perform the Copilot for Microsoft 365 Optimization Assessment Address data security, governance, and data access questions Build shared Copilot for Microsoft 365 implementation plan with User Enablement team	Ensure appropriate Data Security controls are in place Prepare your organization for Copilot for Microsoft 365 with setup guide: deploy Microsoft 365 apps, if needed; assign licenses Assign permissions by role to provide access to the Copilot for Microsoft 365 usage report	Establish service management plan Analyze Copilot for Microsoft 365 usage reports and the Microsoft Copilot Dashboard to observe user adoption, retention, and engagement	Design, build, and publish plugins to deliver unique experiences Build your own copilots

Source: Copilot Success Kit – Microsoft Adoption

“Technical readiness”

Copilot for Microsoft 365

Implementation overview

	Get ready	Onboard & engage	Deliver impact	Extend & optimize
USER ENABLEMENT	**User Enablement Workstream** Secure exec sponsorship, create AI Council, and define RAI principles Identify success owners, Champions, and early adopter cohorts Detail high value scenarios and personas Be intentional with assignment and concentrate seats Define success criteria, KPIs, and success measurement plan	Complete User Enablement Strategy training Define user experience and feedback strategy Design and deploy training and engagement community (Center of Excellence/Champion Platform) Launch employee communications and Champion program Onboard executives and user cohorts Deliver user Champions and support staff training	Review success measures and user survey results Conduct feedback and reporting analysis Deliver extended training and adoption support Identify additional optimization scenarios Iterate user experience strategy Gather and amplify success stories	Extend to new high value scenarios Deliver business process transformation with Copilot Studio, plugins, and connectors Drive group and cross-organizational productivity and innovation Understand custom line of business opportunities
TECHNICAL READINESS	**Technical Readiness Workstream** Perform the Copilot for Microsoft 365 Optimization Assessment Address data security, governance, and data access questions Build shared Copilot for Microsoft 365 implementation plan with User Enablement team	Ensure appropriate Data Security controls are in place Prepare your organization for Copilot for Microsoft 365 with setup guide: deploy Microsoft 365 apps, if needed; assign licenses Assign permissions by role to provide access to the Copilot for Microsoft 365 usage report	Establish service management plan Analyze Copilot for Microsoft 365 usage reports and the Microsoft Copilot Dashboard to observe user adoption, retention, and engagement	Design, build, and publish plugins to deliver unique experiences Build your own copilots

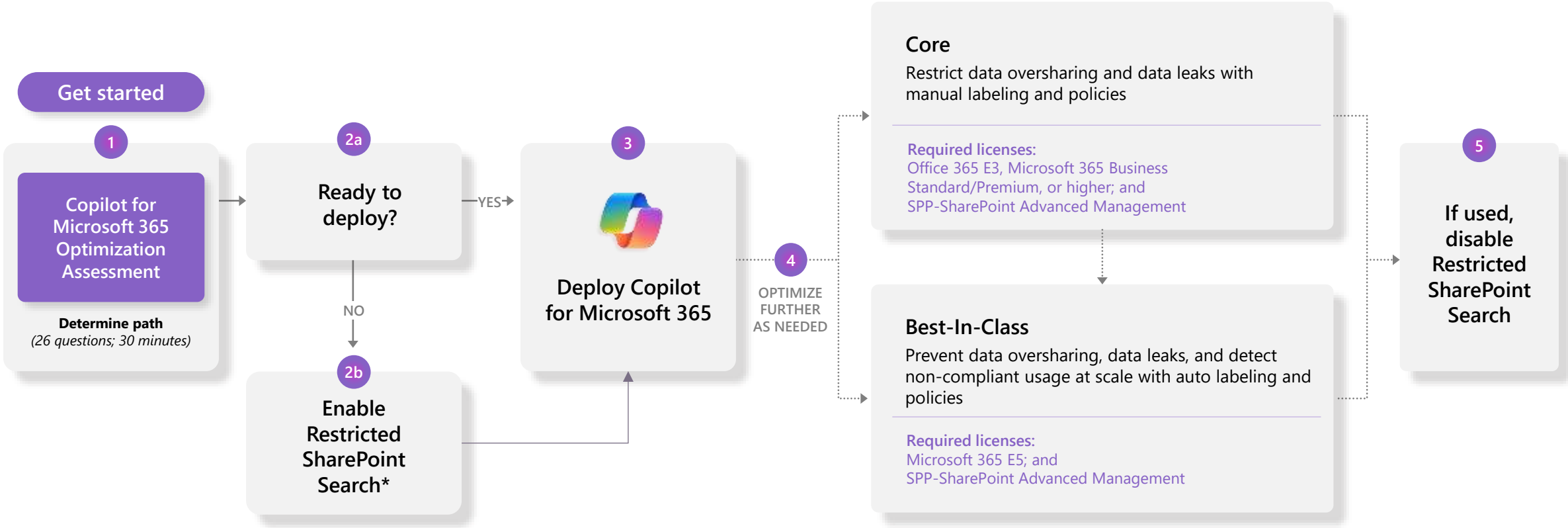
You are here

Onboard & engage

Ensure appropriate Data Security controls are in place

Apply appropriate Data Security controls

Get started quickly and continue to optimize along the way



Link: [M365 Copilot - Solution Assessments Program (microsoft.com)]

*Restricted SharePoint Search will limit Copilot for Microsoft 365 experiences and organization-wide search. It is a temporary option which gives you time to address oversharing concerns while getting started on your Copilot journey.

Securing and governing Copilot for Microsoft 365

Baseline

Copilot for Microsoft 365
+ Office 365 E3

- Multi-factor authentication
- Audit logging

Core

Copilot for Microsoft 365
+ Microsoft 365 E3
+ SharePoint Advanced Management

- Conditional Access
- Manual sensitivity labels
- Data loss prevention policies
- Advanced SharePoint sitewide access controls and reporting
- Unified endpoint management

Best-in-class

Copilot for Microsoft 365
+ Microsoft 365 E5
+ SharePoint Advanced Management

- Conditional Access based on identity risk
- Automatically apply sensitivity labels
- Automatically remove inactive content
- Prevent data leak on endpoint devices
- Detect non-compliant usage

Restricted SharePoint Search

Now generally available: Rollout started June 2024

This is intended as a temporary solution to give you time to review and audit site permissions, while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management.

- **Restricted SharePoint Search** is designed for organizations particularly concerned about unintentional oversharing of content
- When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content

PREREQUISITES

- Available to tenants with Copilot for Microsoft 365 subscriptions
- Activation requires Global/Tenant/SharePoint admin rights

IMPACT

Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site
- Users' OneDrive for Business, chats they are part of, emails they send and receive, calendars to which they have access, etc.
- Files that are shared with, and accessed by users
- Content from users' frequently visited sites

Turning on Restricted SharePoint Search does not affect the site's index or associated DLP and labeling policies.

Access this blog for more info.

Microsoft Purview AI Hub 

Purview AI Hub

Helps with your technical readiness for Copilot for Microsoft 365

Prerequisites to help with insights:

- Onboarded devices to Purview
- Install Purview browser extension (Edge and Chrome)
  - Extension reads your browsing history, manages “my downloads”, communicates with cooperating native applications

With your consent, it will create these Purview policies:

1. **Endpoint DLP policy**

   Detects sensitive info in prompts and responses in other AI assistants

2. **Endpoint DLP policy**

   Uses Adaptive Protection to warn risky users uploading sensitive info to other AI assistants

3. **Comm Compliance policy**

   Detects sensitive info in prompts and responses in Copilot for M365

4. **Insider Risk Mgmt policy**

   Detects when users browse to other AI assistants

5. **Sensitivity Label policy (and labels)!!**

   Creates sensitivity labels and policy for all users

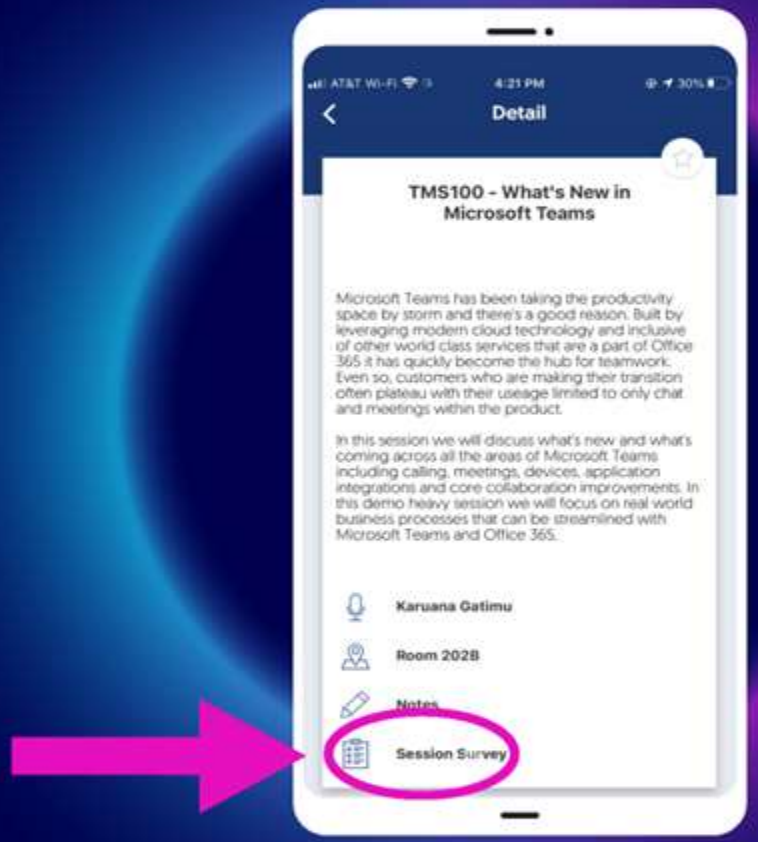
AI Hub (preview)

DEMO

Take-Home guidance

Compliance take-home guidance

Information Protection	Data Loss Prevention	Data Lifecycle and Records Management	Insider Risk Solutions
Apply a container-based sensitivity label to Sites/Teams/Groups. Make it required and better yet… incorporate it into a provisioning solution. Set a default sensitivity label on document libraries where it makes sense. (Incorporate into a provisioning solution if you can) Gradually move from manual to recommending/auto-applying sensitivity labels to files/emails based on conditions you define (you may not start with this on day one).	Sensitivity Labels + Data Loss Prevention = “Better together” Data Loss Prevention is a complimentary control to sensitivity labels. Examples: - If a sensitivity label is downgraded, a DLP policy can still prevent a user from sharing/sending it externally if sensitive content remains in the file/email - A sensitivity label can be a condition in a DLP policy for Exchange email and SharePoint/OneDrive files.	Leverage existing SharePoint information architecture and trainable classifiers to automate the application of retention labels. Retention policies and retention labels are complimentary controls, and are meant to work together: - Apply retention policies for broad coverage - Apply retention labels for more targeted retention requirements Work with your records managers to determine the SharePoint/Teams architecture impacts based on their retention schedules’ mapping into Microsoft Purview. Example: Which SharePoint sites/Microsoft Teams will labels be published to? Incorporate these controls into a provisioning solution.	Establish privacy controls such as pseudonymization. Audit the investigators. Engage stakeholders across org: Legal, Risk, Compliance, Internal Audit, HR, Corp Comms, Cybersecurity, IT. Establish clear policies/ procedures for the use/monitoring of electronic communications in your org and clearly communicate to staff (consider the “Terms of Use” Entra ID feature). Make employees your first line of defense by establishing regular data security & protection training. Configure Adaptive Protection to auto-assign user risk levels.



How was the session?

Search for **365 EduCon** in the App Store or Google Play

Fill out the Session Surveys in the **365 EduCon App** and be eligible to win **PRIZES!**

365 EduCon
Microsoft 365 Conference

THANK YOU!

@DanielGlenn

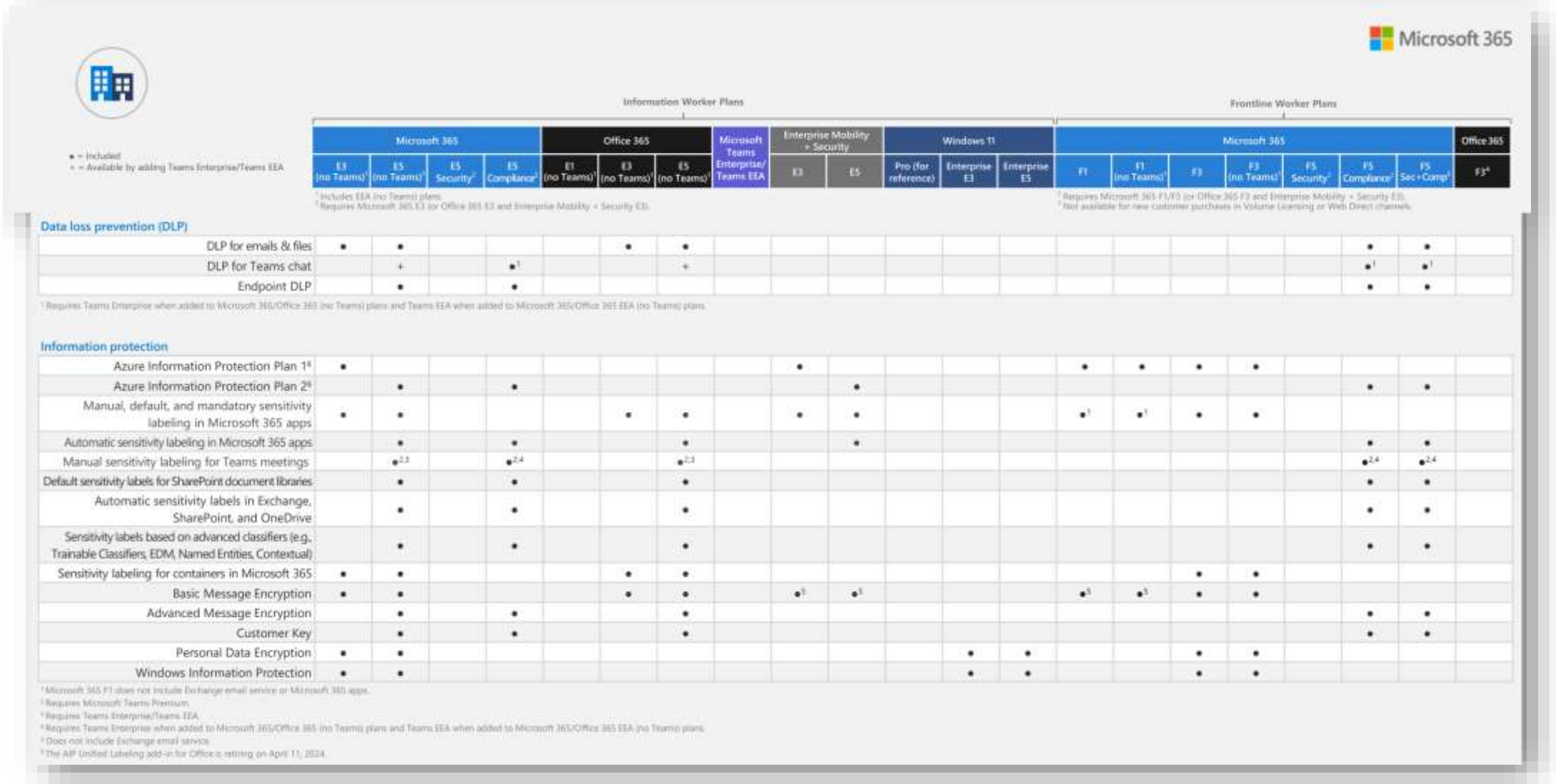
DanielGlenn.com

@JoanneCKlein

JoanneCKlein.com

Licensing for Information Protection and DLP

Microsoft's official resource: https://aka.ms/ComplianceSD (has a downloadable PDF)



Microsoft 365

• = Included
+ = Available by adding Teams Enterprise/Teams EEA

	Information Worker Plans													Frontline Worker Plans							
	Microsoft 365				Office 365			Microsoft Teams Enterprise/ Teams EEA	Enterprise Mobility + Security		Windows 11			Microsoft 365							Office 365
	E3 (no Teams)[1]	E5 (no Teams)[1]	E5 Security[2]	E5 Compliance[2]	E1 (no Teams)[1]	E3 (no Teams)[1]	E5 (no Teams)[1]		E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F1 (no Teams)[1]	F3	F3 (no Teams)	F5 Security[2]	F5 Compliance[2]	F5 Sec+Comp[2]	F3[4]
Data loss prevention (DLP)																					
DLP for emails & files	•	•				•	•												•	•	
DLP for Teams chat		+		•[3]			+												•[3]	•[3]	
Endpoint DLP		•		•															•	•	
Information protection																					
Azure Information Protection Plan 1[4]	•								•					•	•	•	•				
Azure Information Protection Plan 2[4]		•		•						•									•	•	
Manual, default, and mandatory sensitivity labeling in Microsoft 365 apps	•	•				•	•		•	•				•[3]	•[3]	•	•				
Automatic sensitivity labeling in Microsoft 365 apps		•		•			•			•									•	•	
Manual sensitivity labeling for Teams meetings		•[2,3]		•[2,4]			•[2,3]												•[2,4]	•[2,4]	
Default sensitivity labels for SharePoint document libraries		•		•			•												•	•	
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive		•		•			•												•	•	
Sensitivity labels based on advanced classifiers (e.g., Trainable Classifiers, EDM, Named Entities, Contextual)		•		•			•												•	•	
Sensitivity labeling for containers in Microsoft 365	•	•				•	•									•	•				
Basic Message Encryption	•	•				•	•		•[5]	•[5]				•[5]	•[5]	•	•				
Advanced Message Encryption		•		•			•												•	•	
Customer Key		•		•			•												•	•	
Personal Data Encryption	•	•										•	•			•	•				
Windows Information Protection	•	•										•	•			•	•				

[1] Includes EEA (no Teams) plans.
[2] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).
[3] Requires Teams Enterprise when added to Microsoft 365/Office 365 (no Teams) plans and Teams EEA when added to Microsoft 365/Office 365 EEA (no Teams) plans.
[4] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).
[5] Not available for new customer purchases in Volume Licensing or Web Direct channels.

[1] Microsoft 365 F1 does not include Exchange email service or Microsoft 365 apps.
[2] Requires Microsoft Teams Premium.
[3] Requires Teams Enterprise/Teams EEA.
[4] Requires Teams Enterprise when added to Microsoft 365/Office 365 (no Teams) plans and Teams EEA when added to Microsoft 365/Office 365 EEA (no Teams) plans.
[5] Does not include Exchange email service.
[6] The AIP Unified Labeling add-in for Office is retiring on April 11, 2024.

Info Protection and DLP Capabilities for GCC and GCC High

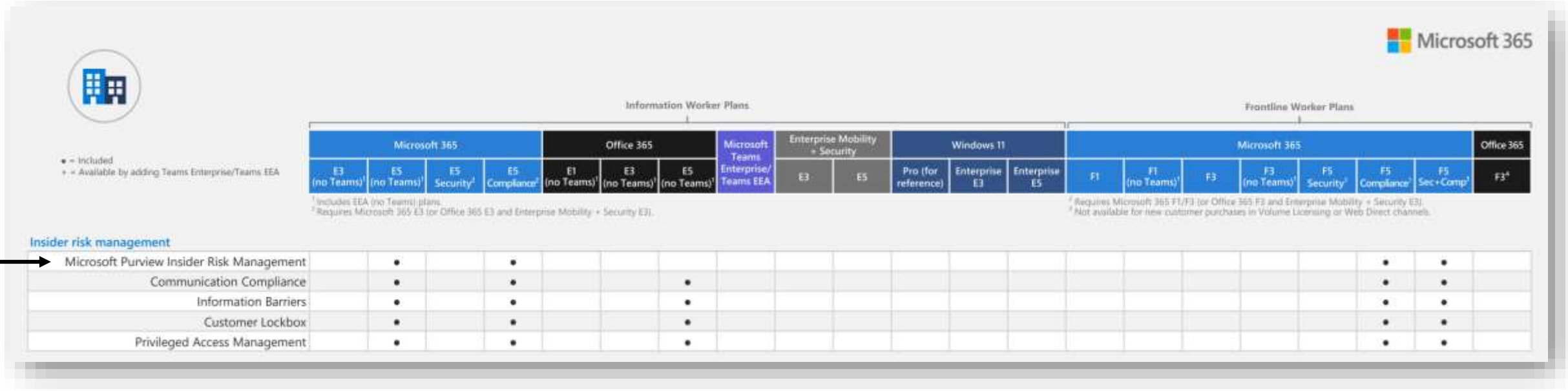
Area	Feature	GCC Status
Data protection		
Sensitive information types	Exact data match	Available
	Named entities sensitive information types and policy authoring templates	In development
Sensitivity labeling	Unified labeling client and scanner	Available
	Application of a "default label" to an unlabeled file uploaded to a SharePoint Online document library	In development
	Apply default label policies to ensure documents being edited	In development
	Automatic classification and labeling for Exchange Online, SharePoint Online, and OneDrive for Business	Available
	Automatic classification and labeling for Office app (Word, Excel, PowerPoint, Outlook) across platforms (web, Android, iOS, Windows, and Mac)	Available
	Automatic classification and labeling for Office clients (Mobile)	On engineering backlog
	Automatic classification and labeling for Teams, Microsoft 365 Groups, and SharePoint sites	Available
	Auto-labeling policies support overwriting manual label and encrypting mail received from any organization	Available
	Co-authoring on Microsoft Purview Information Protection encryption documents	Available
	Enhanced simulations and location support for auto-labeling in SharePoint Online and OneDrive for Business	Available
	Extend built-in sensitivity labels to assets in Azure with Microsoft Azure Purview	In development
	Granular conditional access policies via "Sensitivity labels" for SharePoint Online sites	On engineering backlog
	Mandatory labels	Available
	Manual labels	Available
	New conditions for auto-labeling in Exchange Online	In development

Analytics	Data classification analytics: Overview and Content Explorer	Available
	Auditing and analytics in Office apps	Available
	Activity explorer includes Power BI sensitivity label data	Available
	Activity explorer built-in filters	Available
	Activity explorer user experience improvements	Available
	Activity explorer Power BI sensitivity label data	Available
	Activity explorer security reader role updated	Available
	Content explorer includes Teams data	In development
	Machine learning classifiers with auto labeling on Office apps/client side	Available
Microsoft Purview Data Loss Prevention	Alerts dashboard and alerting experience	Available
	Data surfaced in Activity Explorer	Available
	Endpoint data loss prevention	Available
	Files (SPO/ODB) and email	Available
	Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) integration	Available
	On-premises scanner	Available
	Solution overview page	Available
	Teams chat and channel conversations	Available

Reference: Current GCC capabilities for Info Protection and DLP

Licensing for Insider Risk Management

Microsoft's official resource: https://aka.ms/ComplianceSD (has a downloadable PDF)



Microsoft 365

• = Included
+ = Available by adding Teams Enterprise/Teams EEA

	Information Worker Plans												Frontline Worker Plans							
	Microsoft 365				Office 365			Microsoft Teams Enterprise/ Teams EEA	Enterprise Mobility + Security		Windows 11			Microsoft 365						Office 365
	E3 (no Teams)[1]	E5 (no Teams)[1]	E5 Security[2]	E5 Compliance[2]	E1 (no Teams)[1]	E3 (no Teams)[1]	E5 (no Teams)[1]		E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F1 (no Teams)[1]	F3	F3 (no Teams)[1]	F5 Security[2]	F5 Compliance[2]	F5 Sec+Comp[2]	F3[4]
Insider risk management																					
Microsoft Purview Insider Risk Management		•		•															•	•	
Communication Compliance		•		•			•												•	•	
Information Barriers		•		•			•												•	•	
Customer Lockbox		•		•			•												•	•	
Privileged Access Management		•		•			•												•	•	

[1] Includes EEA (no Teams) plans.
[2] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).
[3] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).
[4] Not available for new customer purchases in Volume Licensing or Web Direct channels.

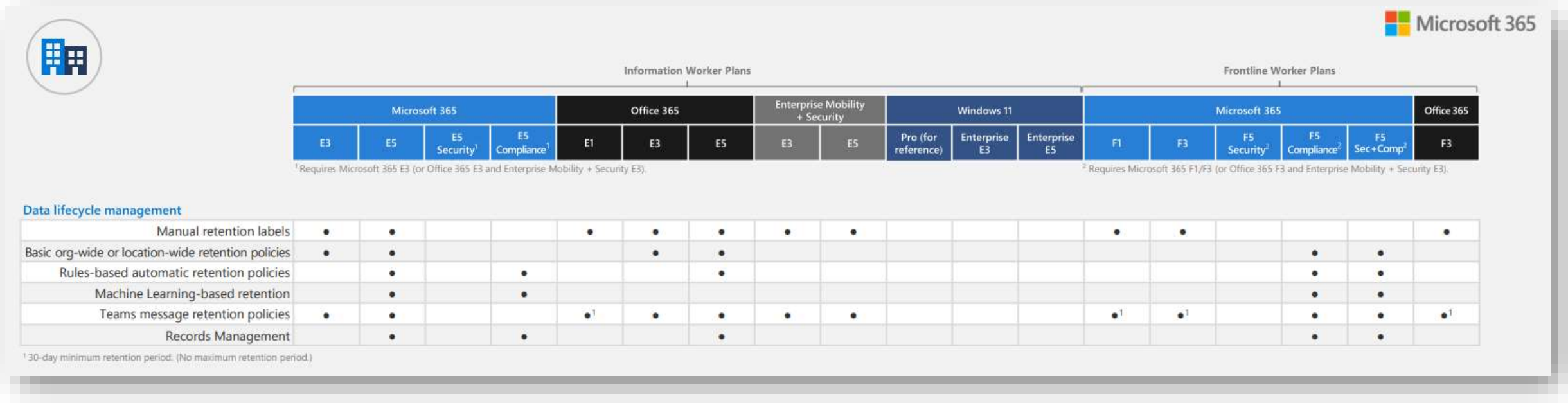
For insider risk management, you will need one of these for each user that is included in a policy and activity is being monitored…

E5/A5/G5 OR **E5/A5/G5/F5 Compliance** OR **E5/A5/G5/F5 Insider Risk Management** OR **F5 Security & Compliance**

Licensing for Data Lifecycle and Records Management

2 trusted resources I use:

- https://aka.ms/ComplianceSD (Microsoft official resource with a downloadable PDF)
- https://m365maps.com (Aaron Dinnage - @AaronDinnage)



Microsoft 365

	Information Worker Plans									Frontline Worker Plans					
	Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 11			Microsoft 365					Office 365
	E3	E5	E5 Security[1]	E5 Compliance[1]	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security[2]	F5 Compliance[2]	F5 Sec+Comp[2]	F3
Data lifecycle management																		
Manual retention labels	•	•			•	•	•	•	•				•	•				•
Basic org-wide or location-wide retention policies	•	•				•	•									•	•	
Rules-based automatic retention policies		•		•			•									•	•	
Machine Learning-based retention		•		•												•	•	
Teams message retention policies	•	•			•[1]	•	•	•	•				•[1]	•[1]		•	•	•[1]
Records Management		•		•			•									•	•	

[1] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).

[1] 30-day minimum retention period. (No maximum retention period.)

For features that are "automated", you will need one of these for each user benefiting from the service…
E5/A5/G5/F5 OR **E5/A5/G5/F5 Compliance** OR **E5/A5/G5/F5 Information Protection and Governance** OR **F5 Security & Compliance**

"Some tenant services are not currently capable of limiting benefits to specific users. Efforts should be taken to limit the service benefits to licensed users."

DLM/RM Capabilities for GCC and GCC High

Microsoft Purview Data Lifecycle Management (formerly Information Governance)	Adaptive scopes for retention and labeling policies	Available
	Apply retention label action at end of retention period	In development
	Apply default retention labels for SharePoint, OneDrive for Business libraries, folders, and document sets; Exchange inboxes; and Office 365 Groups	Available
	Configure option to block the ability to edit metadata for records	In development
	Disable unlocking of records	In development
	Email Archiving	Available
	Import PST	Available
	Manual non-record retention labels	Available
	Preservation lock	Available
	Retention improvements for SharePoint Online and OneDrive for Business	Available
	Retention label deletion behavior change in SharePoint	Available
	Retention policies to entire organization; specific locations or users; automatically based on specific condition (for example, keywords or sensitive information); and based on an event	Available
	Retention policies for Teams (chat)	Available
	Retention policies for Teams meeting recording	Available
	Retention policies for Teams private channels	Available

Records management	Ability to delete a record label	Available
	Allow record label to start "unlocked" for manual records declaration	In development
	Apply a record label manually	Available
	Apply default record labels for SharePoint, OneDrive for Business libraries, folders, and document sets; and Office 365 groups	Available
	Apply record policies automatically based on specific conditions (for example, keywords or sensitive information); and based on an event	Available
	Apply record policies automatically with trainable classifiers	In development
	Disable unlocking of records	Available
	Disposition review	Available
	File plan manager	Available
	Multi-stage disposition review	Rolling out
	Outlook client support for Records Management	Available
	Power Automate integration	On engineering backlog
	Proof of disposal	Available
	Records versioning	Available
	Regulatory records	Available

Reference: Current GCC capabilities for DLM/RM