



Protecting your data and maintaining compliance in a remote work environment

Agenda

- Challenges with remote work and implications to security/productivity
- Apply sensitivity labels in Teams to protect sensitive data
- Applying data loss prevention in Microsoft Teams
- Restrict Teams experiences for guests and people outside of your organization
- Intelligently identify and act on insider risks
- Enabling simple retention policies
- Discover Teams threaded content

Challenges with
remote work and
implications to
security/productivity

“Due to COVID-19 we accelerated a lot of changes we had scheduled for the year, across all of IT”

“We need to ensure we maintain the same level of productivity, compliance and security for our employees no matter if they are using our corp network or their home one, managed or unmanaged devices”.

Aka.ms/wfhblog



Session objectives

Prevent
Sensitive
information
leakage

**Intelligently
identify and
take action on
insider risks**

**Proactively
manage your
liability and
risk by setting
retention
policies**

Microsoft Information Protection (MIP) is a ***built-in, intelligent, unified*** and ***extensible*** platform and solution to protect sensitive data.

Microsoft Information Protection (MIP)

Key Customer Benefits

Built-in

Built-in labeling and protection experience in Office apps, Microsoft Teams, O365 services, other MS services like Power BI, Edge and Windows

Intelligent

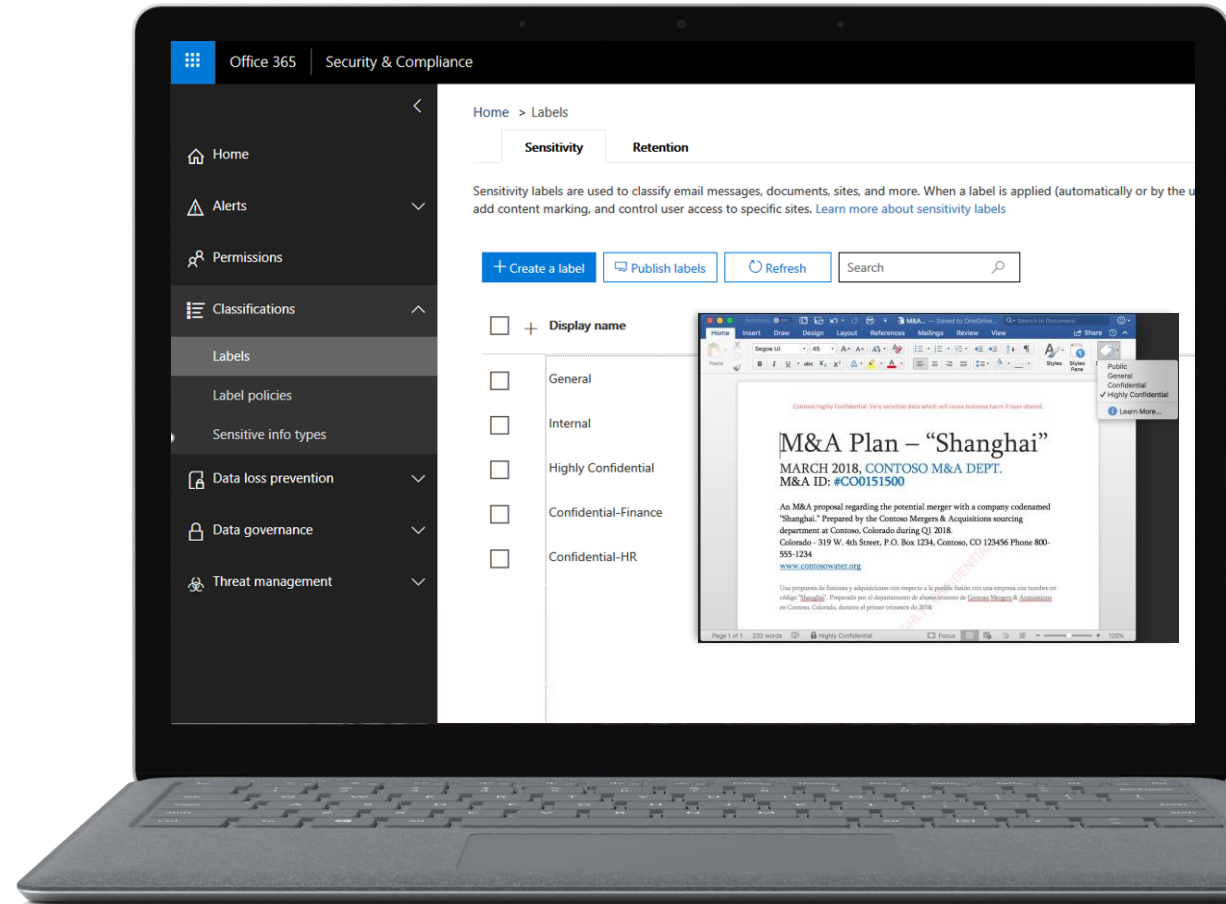
Accuracy and scale in classification via ML based trainable classifiers and exact data match

Unified

Single admin console to configure and manage your policies and view analytics across on-premises, Office apps, M365 services, 3rd party services (via MCAS) and devices

Extensible

MIP development platform extends the protection experience, in a consistent way, to popular non-Microsoft apps and services





Review and monitor sensitive data across your organization

Nadia Fortini – Principal Program Manager



Apply sensitivity labels in Teams to protect sensitive data

Nadia Fortini – Principal Program Manager

Why sensitivity labels for Teams?



Protect with Sensitivity Labels

Control who can access information in Teams

Select if Teams are by default public or private

Regulate access to sensitive Office documents stored in Teams with sensitivity labels

Control access from unmanaged devices

Protect Teams Conversations and Document with a Container Label

Control access to Teams sites and content from unmanaged devices

- Limit or block access to SharePoint, OneDrive, or Teams from [unmanaged devices](#) by selecting one of these options: allow full access from desktop apps, mobile apps, and the web, or limit to web only access, or block access completely.

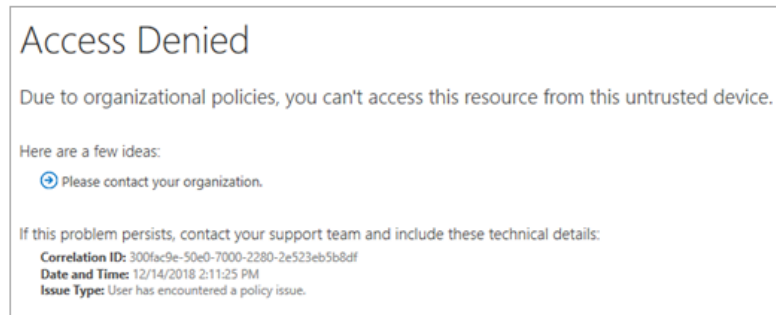


Figure 1. User experience when trying to access Teams from an unmanaged device

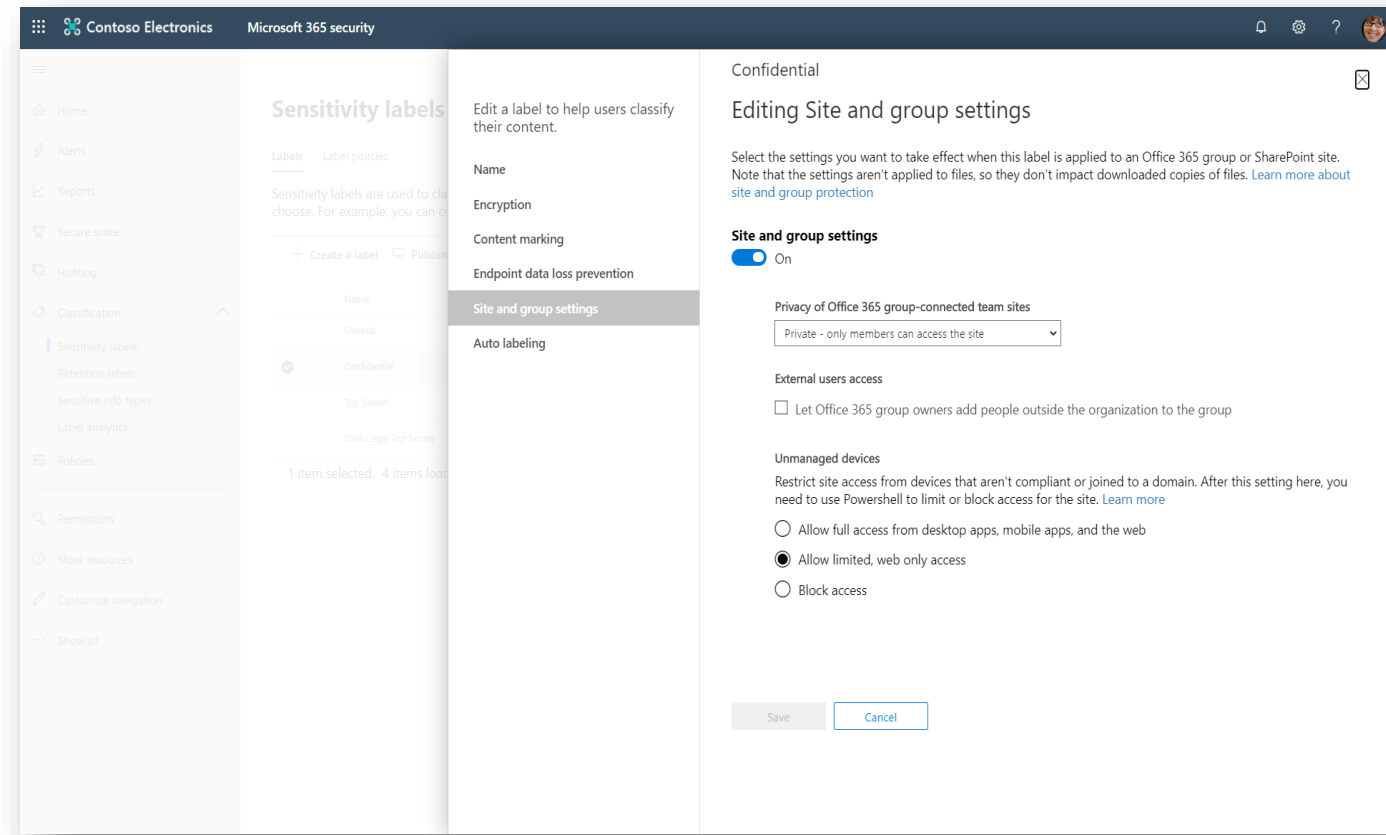


Figure 2. Admin experience on M365 compliance center. Labeling to protect at Teams site level



Applying data loss prevention in Teams

Nadia Fortini – Principal Program Manager

Why Data Loss Prevention for Microsoft Teams?



Prevent Data Loss

Identify and monitor risky sharing activities

Educate users with in-context guidance to make the right decisions

Enforce data use policies upon content without inhibiting productivity

Integrates with classification & labeling to detect and protect data @ egress



Restrict Teams experiences for guests and people outside your organization

Nadia Fortini – Principal Program Manager

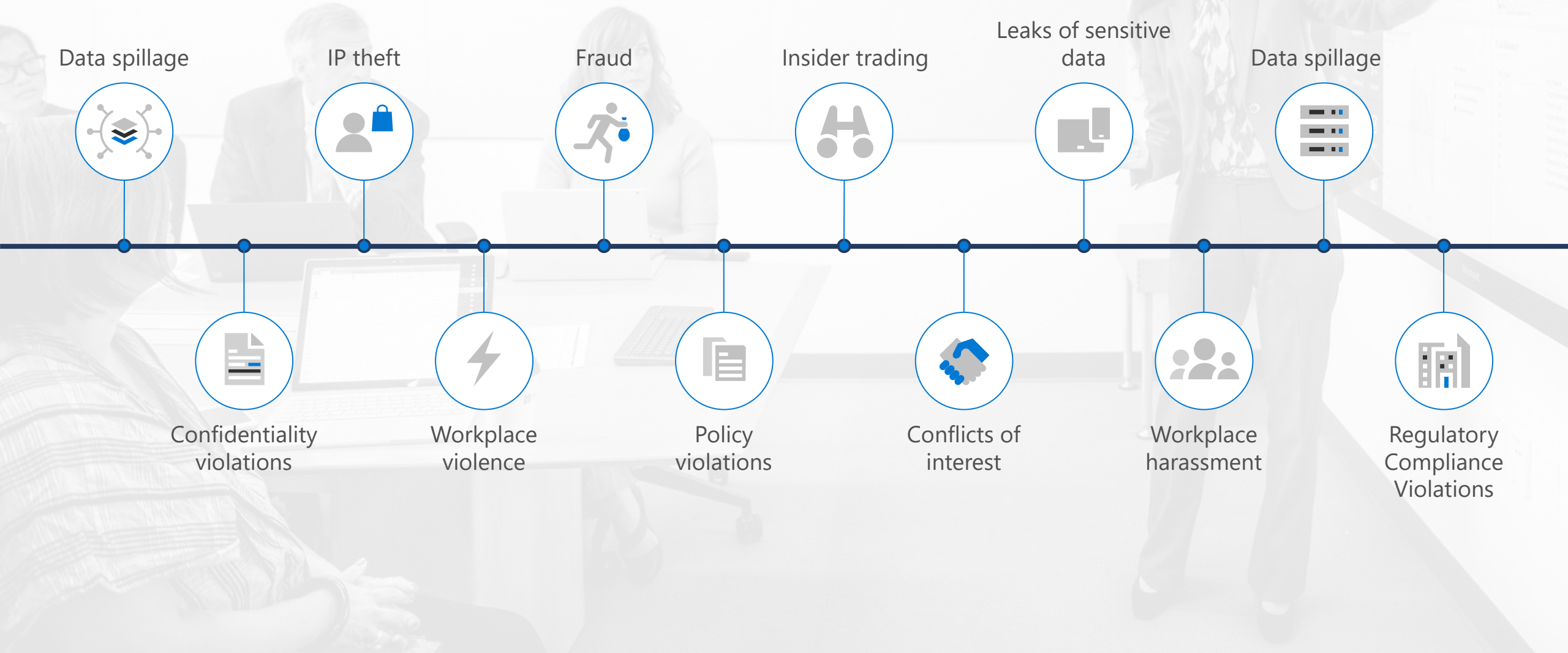


INSIDER RISK MANAGEMENT

Manage risks within your organization



Organizations face a broad range of risks from insiders



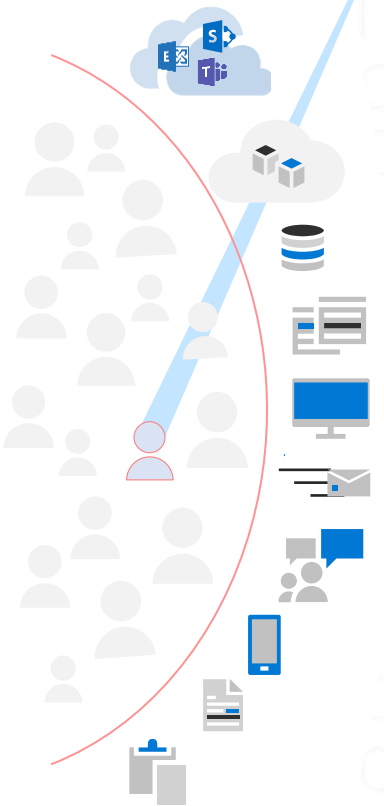
Organizations using a fractured approach for insider risks

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 | <ul style="list-style-type: none"> • Configuration requires scripting (engineering led 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 | <ul style="list-style-type: none"> • Requires deployment of endpoint agents and on-prem servers • Management of agents is complex • Scale and performance issues with agent-based model | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • Low visibility into content • Low sentiment analysis • Low understanding of content sensitivity | <ul style="list-style-type: none"> • Low visibility into content • Low sentiment analysis • Limited signal correlation • Low understanding of content sensitivity | <ul style="list-style-type: none"> • Low visibility into content • Low sentiment analysis • Limited signal correlation • Prone to high-false positive rate |
| Narrow workflows | <ul style="list-style-type: none"> • No integrated workflow beyond SOC | <ul style="list-style-type: none"> • No integrated workflow beyond SOC | <ul style="list-style-type: none"> • No integrated workflow beyond SOC |



Insider Risk Management

Identify and take action on critical insider threats

Rich Insights via tailored templates

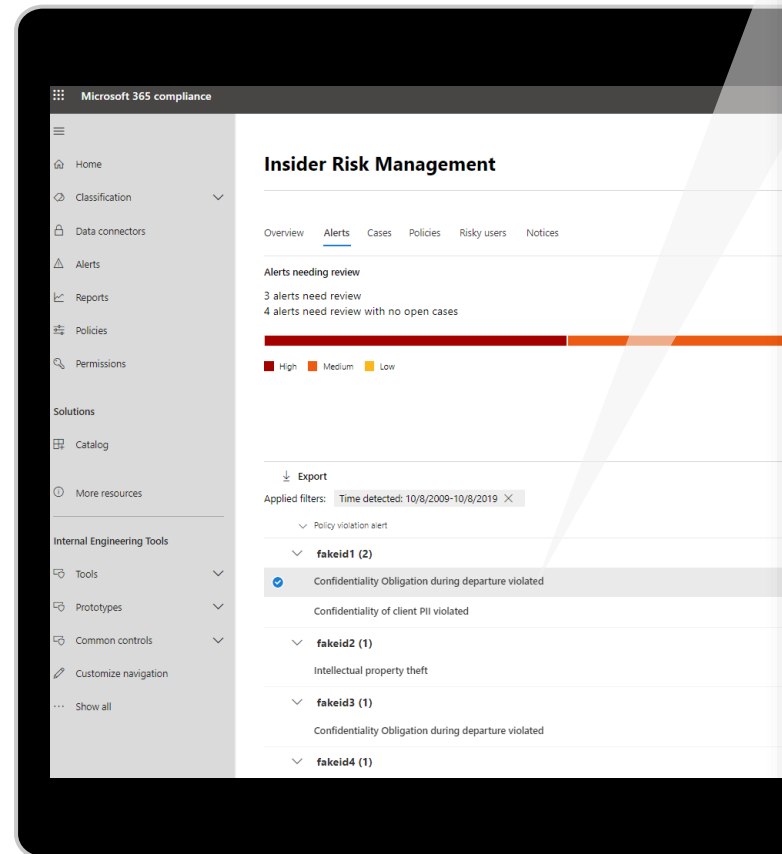
Machine learning correlates native¹ and third-party signals to identify insider risks

Privacy built-in

Anonymity controls ensure data about risks is appropriately managed

End-to-end investigations

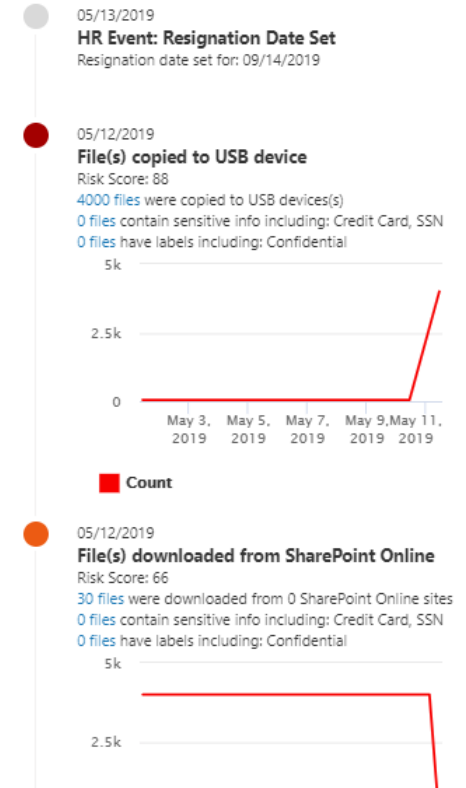
Integrated investigation workflows allow for collaboration across IT, HR and legal



Confidentiality Obligation

Overview User activity User profile

History of recent user activity



1. Teams, SharePoint Online, Exchange Online, OneDrive for Business and Windows 10



Insider Risk Demo



Communication Compliance

Detect code-of-conduct
violations in communications



Organization needs for company communications

Corporate Policies

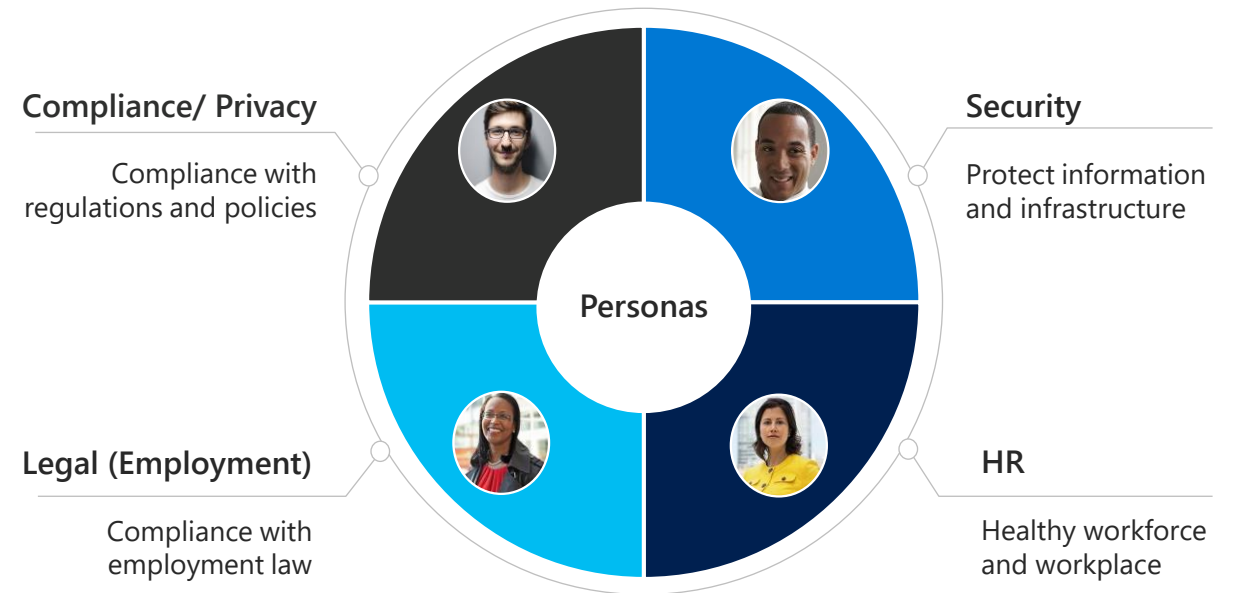
Comply with ethical use and corporate standards

Risk Management

Identify risks and support a healthy workforce

Regulatory Compliance

Implement oversight process for industry standards



Communication Compliance

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



Intelligent customizable templates

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



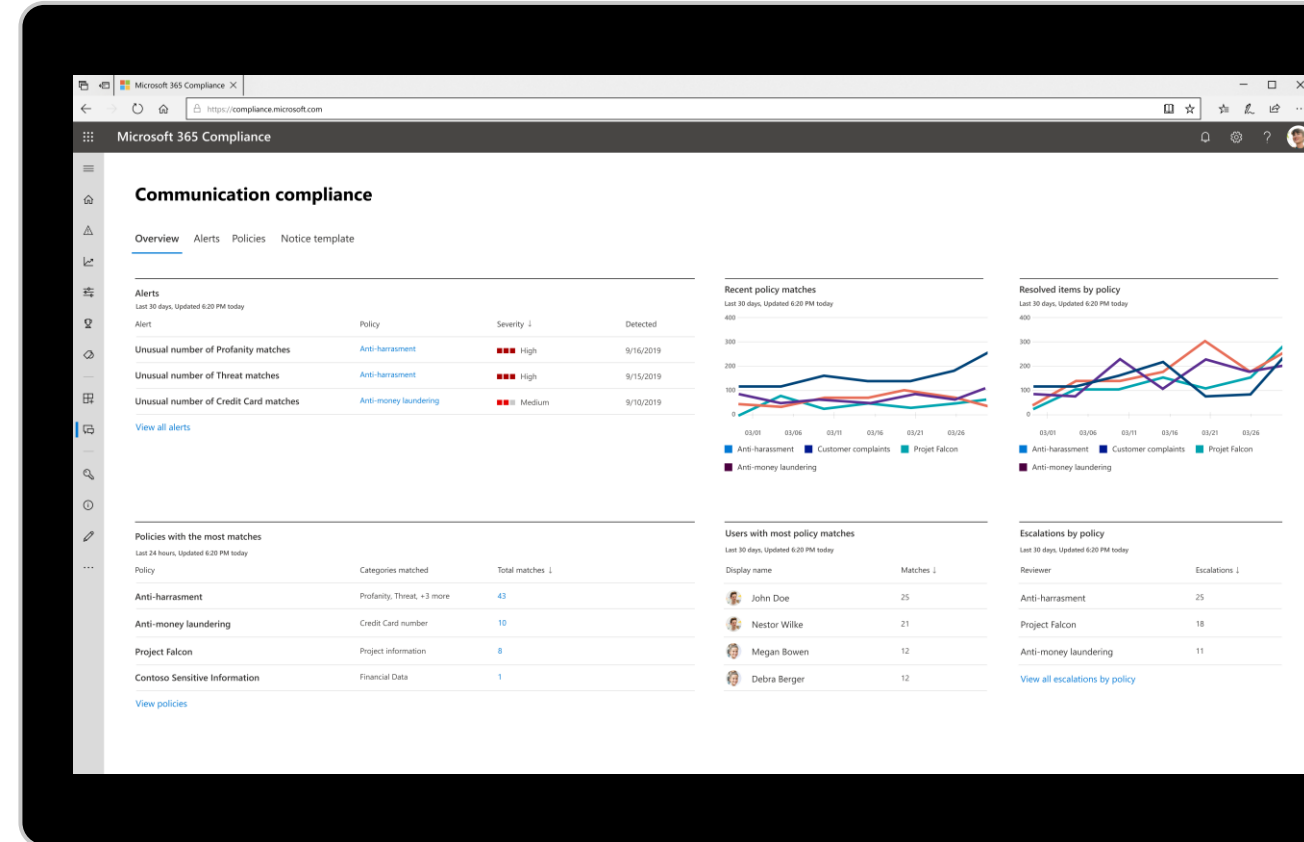
Support employee health and safety

Minimize the impact of risks by detecting threatening language in a timely manner



Flexible remediation workflows

Remediation workflows to quickly act on violations





Communication Compliance Demo

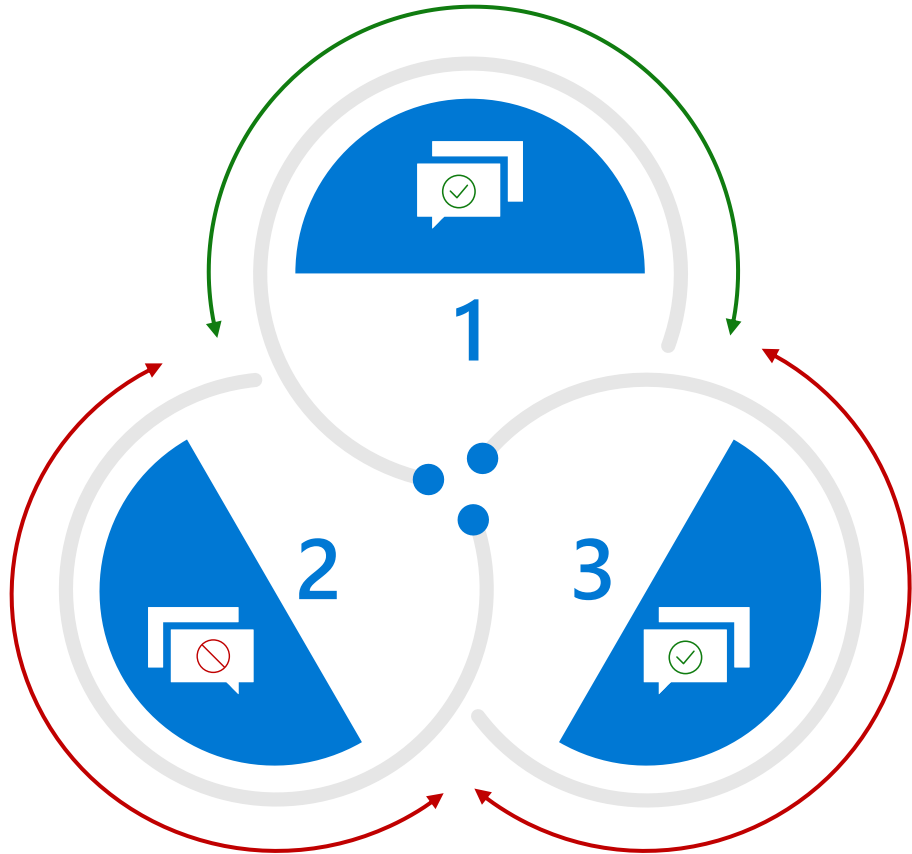


Information Barriers

Restrict communication between risky user groups



Information Barriers – Need



Microsoft 365 provides powerful communication and collaboration capabilities

Communication Restrictions

Avoid conflicts of interest to conform to regulations (like Finance)

Limit communication between users based on their roles (like Education)

Restrict interaction with groups working on sensitive projects

Information barriers provide essential safeguards for communication and collaboration

Information Barriers

Define segments and configure policies to segment to restrict communication



SEGMENTS

are sets of users defined by filters based on user account attributes or AAD group membership



INFORMATION BARRIER POLICIES

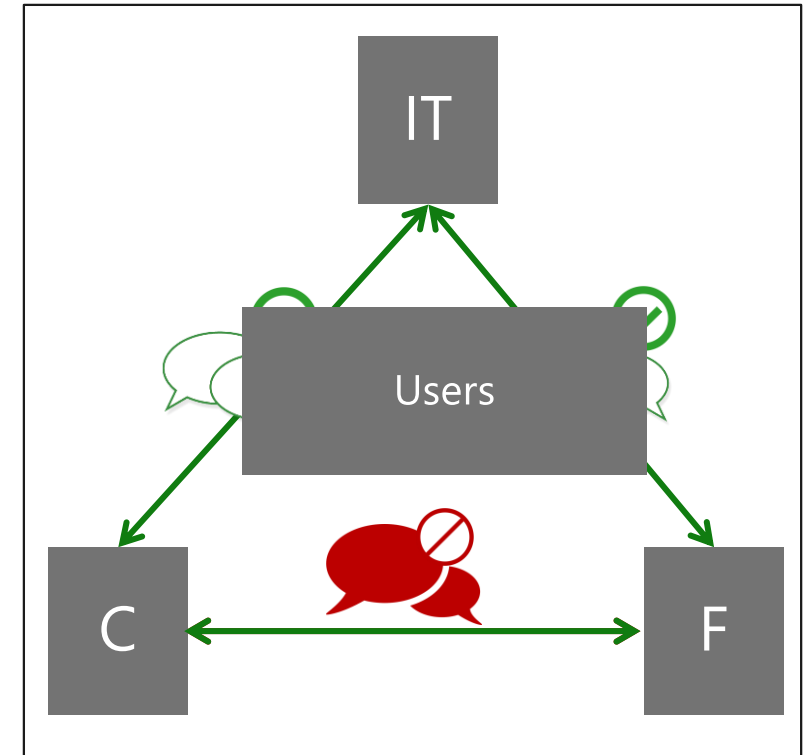
determine communication limits or restrictions between segments

- "Block" policies to prevent one segment from communicating with certain other segments (or)
- "Allow" policies to allow one segment to communicate with only certain other segments



POLICY APPLICATION

is done after all information barrier policies are defined, and you are ready to apply them in your organization.



- Home
- Users
 - Active users
 - Contacts
 - Guest users
 - Deleted users
- Groups
 - Groups (selected)
 - Deleted groups
 - Shared mailboxes
- Billing
- Setup
- Health
- Admin centers
 - Security
 - Compliance
 - Customize navigation
 - Show all

Add a group Refresh Edit name and description Edit email addresses Delete group

| Group name ↑ | Group email | Type | Sync stat... | Teams status |
|---------------------|---|-------------------|--------------|--------------|
| Generate CC msgs | generateccmsgs@M365x525973.onmicrosof | Office 365 | ☰ | |
| Group AB | GroupAB@M365x525973.onmicrosoft.com | Office 365 | ☰ | |
| Group M | GroupM@M365x525973.onmicrosoft.com | Office 365 | ☰ | |
| Leadership | leadership@M365x525973.onmicrosoft.com | Office 365 | ☰ | |
| Legal Team | LegalTeam@M365x525973.OnMicrosoft.com | Distribution list | ☰ | |
| Mark 8 Project Team | Mark8ProjectTeam@M365x525973.onmicro: | Office 365 | ☰ | 👤 |
| ML | ML@M365x525973.onmicrosoft.com | Office 365 | ☰ | |
| Northwind Traders | Traders@M365x525973.OnMicrosoft.com | Distribution list | ☰ | |
| Operations | operations@M365x525973.onmicrosoft.com | Office 365 | ☰ | |
| Paralegals | Paralegals@M365x525973.onmicrosoft.com | Distribution list | ☰ | |
| Project Falcon | Falcon@M365x525973.OnMicrosoft.com | Distribution list | ☰ | |
| Retail | Retail@M365x525973.onmicrosoft.com | Office 365 | ☰ | 👤 |
| Sales and Marketing | SalesAndMarketing@M365x525973.onmicrc | Office 365 | ☰ | 👤 |
| Sales Planning | SalesPlanning@M365x525973.onmicrosoft.c | Office 365 | ☰ | 👤 |
| Sales Team | SalesTeam@M365x525973.OnMicrosoft.com | Distribution list | ☰ | |
| sg-Engineering | | Security | ☰ | |
| sg-Executive | | Security | ☰ | |
| sg-Finance | | Security | ☰ | |
| sg-HR | | Security | ☰ | |



Group AB

Private group • 5 members

General Members Settings Microsoft Teams

Owners (1)

Adele Vance
AdeleV@M365x525973.OnMicrosoft.com

[View all and manage owners](#)

Members (5)

| | |
|--|---|
| Alex Wilber AlexW@M365x525973.OnMicrosoft.com | Allan Deyoung AllanD@M365x525973.OnMicrosoft.com |
|--|---|

| | |
|---|--|
| Adele Vance AdeleV@M365x525973.OnMicrosoft.com | Bianca Pisani BiancaP@M365x525973.OnMicrosoft.com |
|---|--|

Brian Johnson (TAILSPIN)
BrianJ@M365x525973.onmicrosoft.com

[View all and manage members](#)

- Home
- Users
 - Active users
 - Contacts
 - Guest users
 - Deleted users
- Groups
 - Deleted groups
 - Shared mailboxes
- Billing
- Setup
- Health
- Admin centers
 - Security
 - Compliance
 - Customize navigation
 - Show all

Add a group Refresh Edit name and description Edit email addresses Delete group

| Group name ↑ | Group email | Type | Sync stat... | Teams status |
|---------------------|---|-------------------|--------------|--------------|
| Generate CC msgs | generateccmsgs@M365x525973.onmicrosof | Office 365 | ☁ | |
| Group AB | GroupAB@M365x525973.onmicrosoft.com | Office 365 | ☁ | |
| Group M | GroupM@M365x525973.onmicrosoft.com | Office 365 | ☁ | |
| Leadership | leadership@M365x525973.onmicrosoft.com | Office 365 | ☁ | |
| Legal Team | LegalTeam@M365x525973.OnMicrosoft.com | Distribution list | ☁ | |
| Mark 8 Project Team | Mark8ProjectTeam@M365x525973.onmicro: | Office 365 | ☁ | 📱 |
| ML | ML@M365x525973.onmicrosoft.com | Office 365 | ☁ | |
| Northwind Traders | Traders@M365x525973.OnMicrosoft.com | Distribution list | ☁ | |
| Operations | operations@M365x525973.onmicrosoft.com | Office 365 | ☁ | |
| Paralegals | Paralegals@M365x525973.onmicrosoft.com | Distribution list | ☁ | |
| Project Falcon | Falcon@M365x525973.OnMicrosoft.com | Distribution list | ☁ | |
| Retail | Retail@M365x525973.onmicrosoft.com | Office 365 | ☁ | 📱 |
| Sales and Marketing | SalesAndMarketing@M365x525973.onmicrc | Office 365 | ☁ | 📱 |
| Sales Planning | SalesPlanning@M365x525973.onmicrosoft.c | Office 365 | ☁ | 📱 |
| Sales Team | SalesTeam@M365x525973.OnMicrosoft.com | Distribution list | ☁ | |
| sg-Engineering | | Security | ☁ | |
| sg-Executive | | Security | ☁ | |
| sg-Finance | | Security | ☁ | |
| sg-HR | | Security | ☁ | |



Group M

Private group • 2 members

General Members Settings Microsoft Teams

Owners (1)

Megan Bowen
MeganB@M365x525973.OnMicrosoft.com

[View all and manage owners](#)

Members (2)

| | |
|---|--|
| Megan Bowen MeganB@M365x525973.OnMicrosoft.com | Miriam Graham MiriamG@M365x525973.OnMicrosoft.com |
|---|--|

[View all and manage members](#)



Information Barriers Demo



Enabling simple retention (or deletion) policies

Roberto Yglesias

Information Governance

Intelligently govern data across your environment to reduce risk



Streamlined administration

Single place to apply policies across services, native connectors to bring in 1st and 3rd party content



Automation at scale

Automatically and intelligently classify with trainable classifiers to retain or delete data to reduce risk



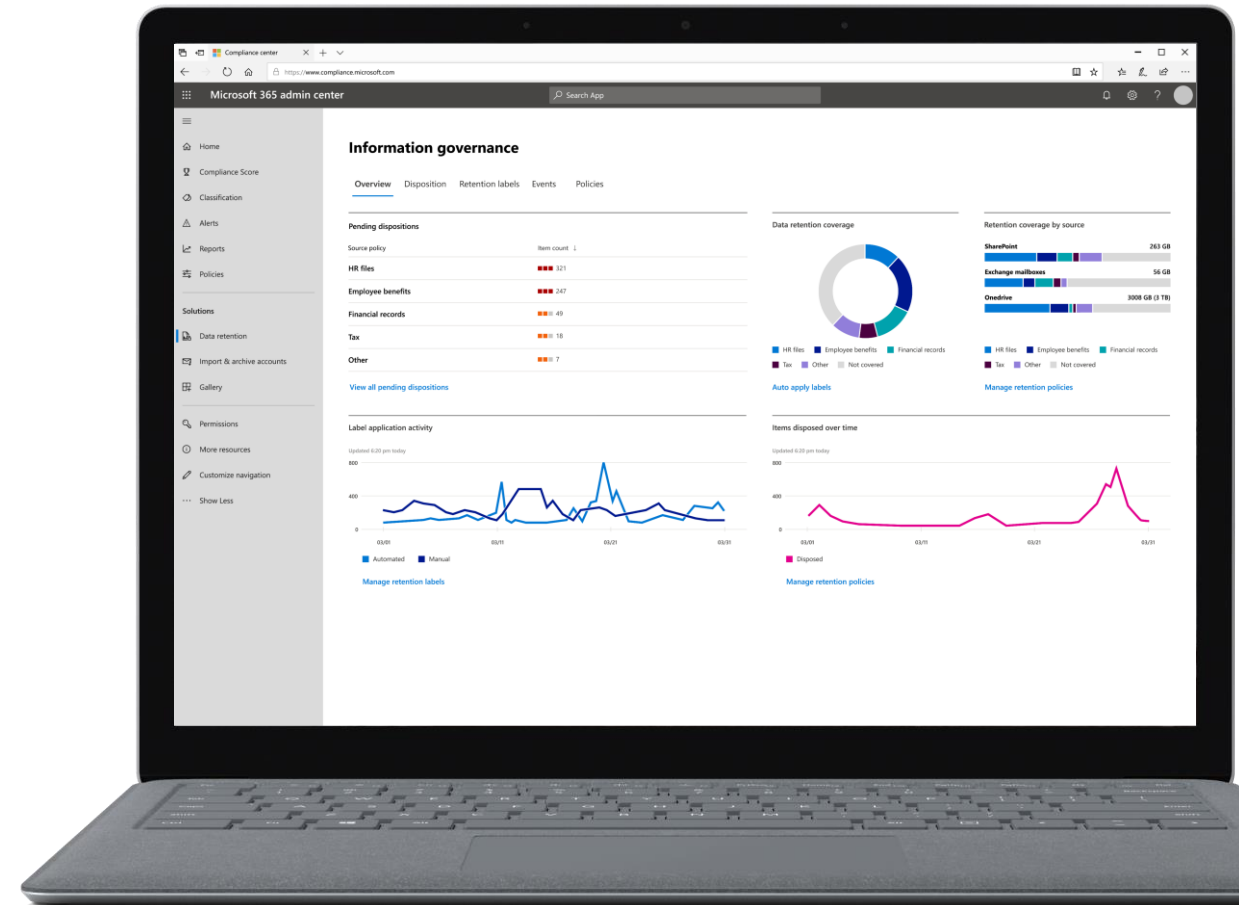
Tailored workflows

Simplify business processes with actionable insights and remediation flows



Records Management

Modernize records management and scale it to meet regulations





Discovering Teams threaded content

Iram Arras



Do more, **in-place**
eDiscovery in
Microsoft 365



Cost reduction

Lower cost per
custodian average



Efficiency

Review relevant Office 365 and
non-Office 365 content faster

Reduce
collection activities



Security

Export matter-relevant
content

Logging and auditing
from one place

Take action today to reduce your risk



Explore these capabilities with a [Microsoft 365 E5 trial](#)



Classify and label sensitive data with [Microsoft Information Protection](#)



Implement [Insider Risk Management and Communication Compliance](#) to reduce insider risks



Get ahead of the ever-evolving compliance landscape with [Compliance Score](#)


Resources

Managed by the MIP and Compliance CXE Team

- ✓ Tech Community Resources – <https://aka.ms/MIPC/CommunityResources>
- ✓ Webinars – <https://aka.ms/MIPC/Webinars>
- ✓ Previews – <https://aka.ms/MIPC/Previews>
- ✓ Blog – <https://aka.ms/MIPblog> & <https://aka.ms/CompBlog>
- ✓ Yammer – <https://aka.ms/MIPC/AskMIPTeam>
- ✓ <https://twitter.com/MIPnews> using the tag #MicrosoftIP

Webinar survey - aka.ms/wfhwebinarsurvey – help us improve! 😊



A collection of colorful geometric shapes including a blue circle, a green triangle, a yellow vertical bar, an orange semi-circle, a blue ring, a green square, and a large orange circle with yellow dashed lines radiating from it.

Thank you!
Stay healthy, stay safe, stay
secured and stay connected!

The Microsoft team 😊