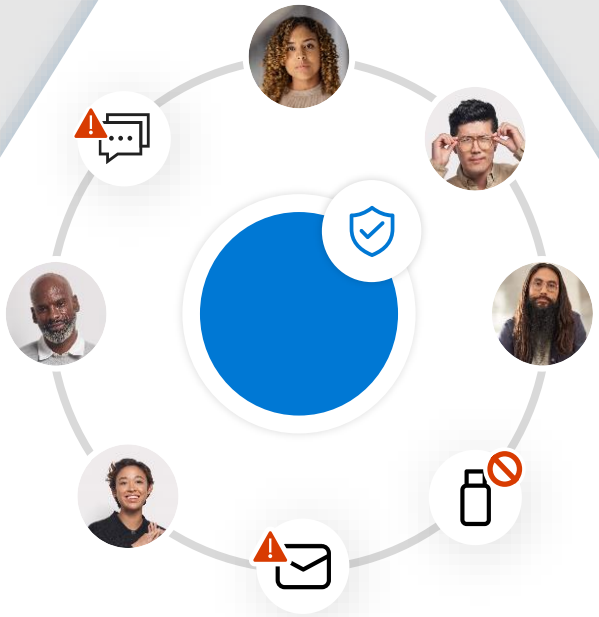
Microsoft Security

Data Security
Let's Protect the Jellyfish

Anela Jaganjac & Ellen van Meurs

Protecting data from unauthorized access, corruption or theft

Information Protection

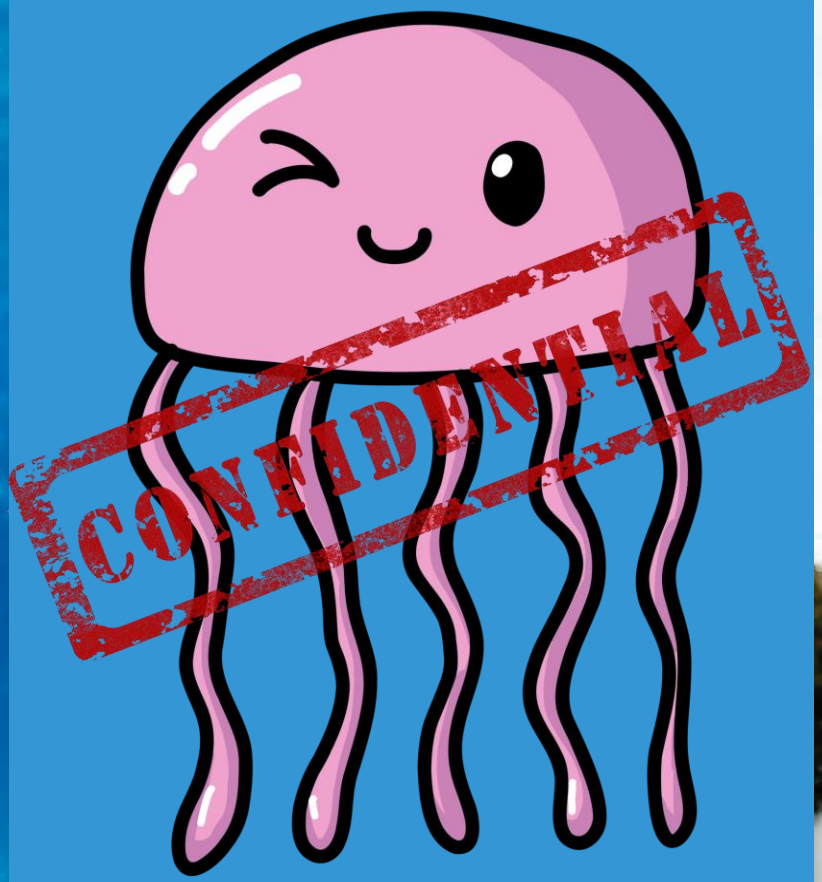


Data Loss Prevention

Insider Risk Management

Microsoft Security

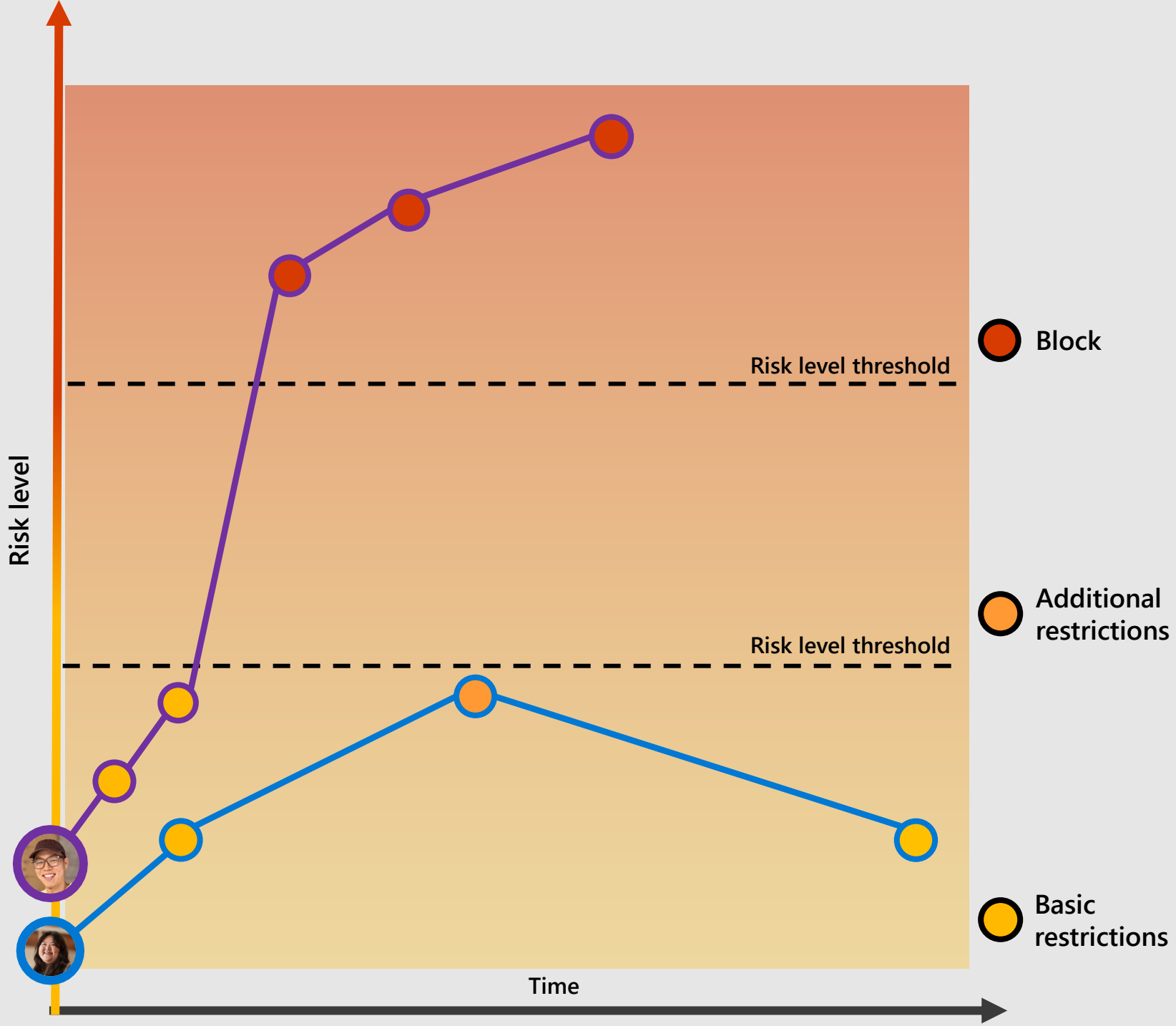

THE GREEN
BATTERY


CONFIDENTIAL


STOP

Resignation and data theft

Adaptive Protection


Risk level
Risk level threshold
Risk level threshold
Time
Block
Additional restrictions
Basic restrictions

- Home
- Compliance Manager
- Data classification
  - Overview
  - Classifiers
  - Content explorer
  - Activity explorer
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials

Solutions

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Data lifecycle management
- Information protection
- Information barriers
- Insider risk management
- Records management
- Privacy risk management

Classifiers

Home

Welcome to the Microsoft Purview compliance portal

Intro | Next steps | Give feedback

Welcome to the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions to help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more. Learn more about the Microsoft Purview compliance portal

Next | Close

What's new ? | Add cards

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers.
Learn more about communication compliance

Recently detected

Communications containing	Instances
All Full Names	760
U.S. Physical Addresses	212
All Physical Addresses	212

Adaptive Protection

Adaptive Protection is ready to go!

What we set up

- An Insider risk policy
- Risk levels for Adaptive Protection
- A DLP policy in test mode.

Head over to **Adaptive Protection** to test it out and refine the features as needed to ensure Adaptive Protection minimizes the risk activities that matter most to your org.

Insider Risk Management

Your policies haven't generated any alerts in the last 30 days

Review and address all policy warnings and recommendations.

Compliance Manager

Your compliance score: 43%

Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information	27 / 81
Control access	87 / 381
Manage devices	0 / 282
Protect against threats	0 / 136
Discover and respond	0 / 69
Manage internal risks	27 / 40

Home
Compliance Manager
Data classification
Overview
Classifiers
Content explorer
Activity explorer
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management

Classifiers

Sensitive info types

Trainable classifiers | Sensitive info types | EDM classifiers

Use built-in or custom classifiers to identify specific categories of content based on existing items in your organization. Once created, classifiers can be used in several compliance solutions to detect related content and classify it, protect it, retain it, and more. Learn more

We're done generating analytics that will allow you to create and test trainable classifiers.

+ Create trainable classifier | Refresh | 109 items | Group

Filters: Language: Any | Type: Any | Name: Any | Status: Any | Filters

Name	Accuracy	Status	Type	Language	Created by	Last modified	Last modified by
Published (109)							
Actuary reports	-	Ready to use	Built-In	English	Microsoft	9/6/2023	Microsoft
Agreements	-	Ready to use	Built-In	English	Microsoft	5/25/2023	Microsoft
Asset Management	-	Ready to use	Built-In	English	Microsoft	9/20/2023	Microsoft
Bank statement	-	Ready to use	Built-In	English	Microsoft	9/20/2023	Microsoft
Budget	-	Ready to use	Built-In	English	Microsoft	5/19/2023	Microsoft
Business plan	-	Ready to use	Built-In	English	Microsoft	1/1/0001	
Completion Certificates	-	Ready to use	Built-In	English	Microsoft	7/14/2023	
Construction specifications	-	Ready to use	Built-In	English	Microsoft	7/14/2023	
Control System and SCADA files	-	Ready to use	Built-In	English	Microsoft	7/11/2023	Microsoft
Corporate Sabotage	-	Ready to use	Built-In	English	Microsoft	9/19/2023	Microsoft
Customer Complaints	-	Ready to use	Built-In	English	Microsoft	3/22/2023	Microsoft
Customer Files	-	Ready to use	Built-In	English	Microsoft	9/20/2023	Microsoft
Discrimination	-	Ready to use	Built-In	English	Microsoft	8/9/2021	

Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Overview
Policies
Alerts
Endpoint DLP settings
Activity explorer
eDiscovery
Data lifecycle management
Information protection
Overview
Labels
Label policies
Auto-labeling
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Extend labeling to assets in the data map ...

When you turn this on, you'll be able to apply your sensitivity labels to files and schematized data assets in Microsoft Purview Data Map and Microsoft Defender for cloud. Learn more

Turn on

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is prote
encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Create auto-labeling policy | Publish label | Edit label | Reorder | Delete label | Refresh

Name	Order	Scope	Created by
Personal	0 - lowest	File, Email	
Public	1	File, Email	
General	2	File, Email	
Confidential	5	File, Email	
Highly Confidential	9	File, Email	
All Employees	10	File, Email	
Specified People	11	File, Email	
Jellyfish	12	File, Email, Meetings, Site, UnifiedGroup	Microsoft CDX
Recipients Only	13	File, Email	Johanna Lorenz
All Employees	14	File, Email	Johanna Lorenz
Anyone (not protected)	15	File, Email	Johanna Lorenz
Project Obsidian	16	File, Email, Site, UnifiedGroup	Johanna Lorenz
Highly Confidential - Jellyfish	17	File, Email, Meetings, Site, UnifiedGroup	Microsoft CDX
Lorem Ipsum	18 - highest	File, Email	Microsoft CDX

Jellyfish

Create sublabel | Create auto-labeling policy | Publish label | ...

Name
Jellyfish

Display name
Jellyfish

Description for users
Highly confidential Jellyfish label

Scope
File, Email, Meetings, Site, UnifiedGroup

Encryption
Encryption

Content marking
Watermark: Jellyfish - Highly confidential
Footer: Please use this content only with Jellyfish members

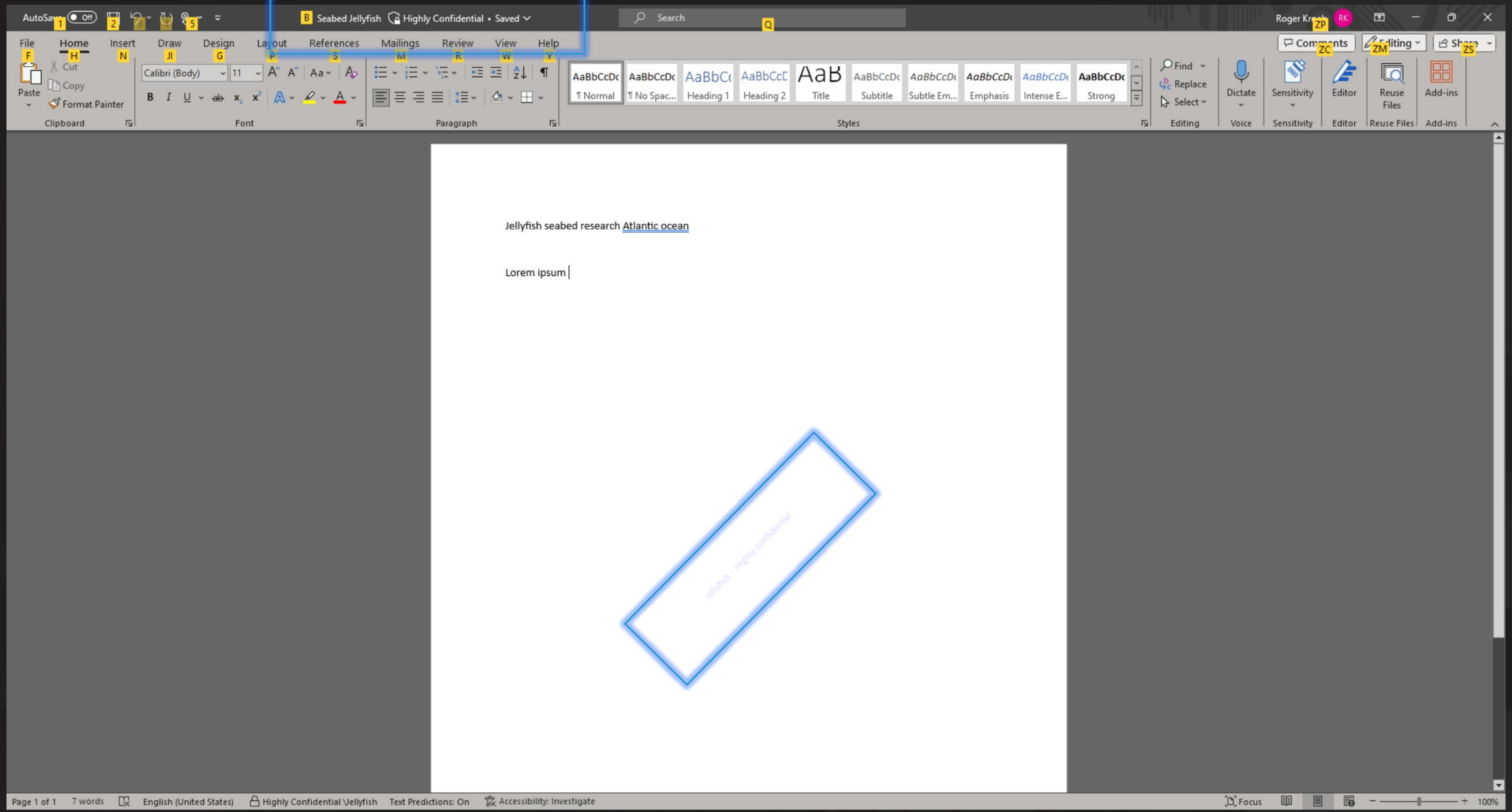
Auto-labeling for files and emails
None

Group settings
Private
Allow external users to be added to the group

Site settings
Allow limited, web-only access
New and existing guests

Meetings settings

Auto-labeling for schematized data assets (preview)
None


Seabed Jellyfish
Highly Confidential • Saved
Search
Roger Kr
File
Home
Insert
Draw
Design
Layout
References
Mailings
Review
View
Help
Comments
Editing
Share
Paste
Cut
Copy
Format Painter
Calibri (Body)
11
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
Dictate
Voice
Sensitivity
Editor
Reuse Files
Add-ins
Jellyfish seabed research Atlantic ocean
Lorem ipsum
Jellyfish - Highly confidential
Page 1 of 1
7 words
English (United States)
Highly Confidential \Jellyfish
Text Predictions: On
Accessibility: Investigate
Focus
100%

image

- Template or custom policy
- **Name**
- Admin units
- Locations
- Policy settings
- Policy mode
- Finish

Name your DLP policy

Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *

Jellyfish Email block with override - Externals

Description

This policy is aimed to protect the oversharing of sensitive information from project Jellyfish with external organizations. Overrides will be audited.

- Template or custom policy
- Name
- Admin units
- **Locations**
- Policy settings
- Policy mode
- Finish

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. Learn more about role group permissions.

View role groups

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

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

Back Next Cancel

- Name
- Admin units
- Locations
- **Advanced DLP rules**
- Policy mode
- Finish

Edit rule

Content contains

Group name *

Default

Group operator

Any of these

Sensitivity labels

Highly Confidential/Jellyfish

Highly Confidential - Jellyfish

Add

Create group

Add condition Add group

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

- (●) Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

  By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

  - (●) Block everyone.
  - ( ) Block only people outside your organization.
- ( ) Encrypt email messages (applies only to content in Exchange)

Add an action

User notifications

Save Cancel

Name
Admin units
Locations
Advanced DLP rules
Policy mode
Finish

Edit rule

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

Email notifications

- Notify the user who sent, shared, or last modified the content.
- Notify these people:
- Customize the email text
- Customize the email subject

Policy tips

Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported

- Customize the policy tip text

The item you are about to send contains sensitive information and is classified as highly confidential. Please state your business justification to allow overriding and continue this activity.

- Show the policy tip as a dialog for the end user before send (available for Exchange workload only)

To help ensure all email messages display the pop-up before they're sent, you must first configure Group Policy Object (GPO) settings to allow for full evaluation. Learn more

- Provide a compliance URL for the end user to learn more about your organization's policies (available for Exchange workload only)

User overrides

Allow overrides from M365 services

- Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.
  - Require a business justification to override
  - Override the rule automatically if they report it as a false positive
  - Require the end user to explicitly acknowledge the override (available for Exchange workload only)

Incident reports

Save Cancel

- Name
- Admin units
- Locations
- Advanced DLP rules
- Policy mode
- Finish

Edit rule

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.
Learn more restricting device activity

Service domain and browser activities

Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

- [x] Upload to a restricted cloud service domain or access from an unallowed browsers — Block
  + Choose different restrictions for sensitive service domains
- [ ] Paste to supported browsers — Audit only
  + Choose different restrictions for sensitive service domains

File activities for all apps

Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

- ( ) Don't restrict file activity
- (•) Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

- [x] Copy to clipboard — Block with ov...
  + Choose different copy to clipboard restrictions
- [x] Copy to a removable USB device — Block with ov...
  + Choose different removable USB device restrictions
- [x] Copy to a network share — Block with ov...

Save Cancel

- Name
- Admin units
- Locations
- Advanced DLP rules
- Policy mode
- Finish

Name your DLP policy

Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *

Project Jellyfish - Exchange Adaptive protection

Description

The business critical of project Jellyfish should be protected with a lot of care and measures.
This DLP policy will help to keep the secret information within the organization and only allow limited access to the information.

Next

Cancel

- Name
- Admin units
- **Locations**
- Advanced DLP rules
- Policy mode
- Finish

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. Learn more about role group permissions.

View role groups

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

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

Back Next Cancel

- Name
- Admin units
- Locations
- **Advanced DLP rules**
- Policy mode
- Finish

Create rule

Use rules to define the t

ent matches many rules, the most restrictive one will be enforced. Learn more about rules.

Name *

DLP - Elevated Block er

Description

Conditions

Define the conditions th

specific content, senders, and recipients that you want the rule to detect. For more complex rules, create groups to exclude or include items. Learn how the condition builder wo

+ Add condition

Actions

Use actions to protect

+ Add an action

User notifications

Use notifications to info

Off

Notifications won't be us

r use of sensitive info.

ams, and On Premises Scanner.

User overrides

Allow overrides from M

Allow overrides fron

SharePoint, OneDrive, and Teams to override policy restrictions.

Incident reports

Use this severity level i

Send an alert to admins

On

Save Cancel

- Content contains
- User's risk level for Adaptive Protection is
- Content is not labeled
- Content is shared from Microsoft 365
- Content is received from
- Sender IP address is
- Header contains words or phrases
- Sender AD Attribute contains words or phras...
- Content character set contains words
- Header matches patterns
- Sender AD Attribute matches patterns
- Recipient AD Attribute contains words or phr...
- Recipient AD Attribute matches patterns
- Recipient is a member of
- Document property is
- Document could not be scanned
- Document or attachment is password protec...
- Has sender overridden the policy tip
- Sender is a member of
- Document didn't complete scanning
- Recipient address contains words
- File extension is
- Recipient domain is
- Recipient is
- Sender is
- Sender domain is
- Recipient address matches patterns
- Document name contains words or phrases
- Document name matches patterns
- Subject contains words or phrases

- Name
- Admin units
- Locations
- Advanced DLP rules
- Policy mode
- Finish

Edit rule

User's risk level for Adaptive Protection is

Risk levels for Adaptive Protection are defined in insider risk management. They determine how risky a user's activity is and can be based on conditions such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. If insider risk management detects that a user matched the risk level condition, the DLP policy will enforce any actions you configure below. Learn more about risk levels for Adaptive Protection

Elevated risk level

AND

Content contains

Group name *

Default

Group operator: Any of these

Sensitive info types

Project Jellyfish — High confidence — Instance count 1 to Any

Sensitivity labels

Highly Confidential - Jellyfish

Highly Confidential/Jellyfish

Add

Create group

Add condition Add group

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

Save Cancel

- Name
- Admin units
- Locations
- **Advanced DLP rules**
- Policy mode
- Finish

Edit rule

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

- (•) Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

  By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

  - (•) Block everyone.
  - ( ) Block only people outside your organization.
- ( ) Encrypt email messages (applies only to content in Exchange)

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

- [x] **Email notifications**
  - (•) Notify the user who sent, shared, or last modified the content.
  - ( ) Notify these people:
  - [ ] Customize the email text
  - [ ] Customize the email subject
- [x] **Policy tips**

Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported

- [x] Customize the policy tip text

Please be aware you are sharing sensitive information to potential unauthorized users.

- [x] Show the policy tip as a dialog for the end user before send (available for Exchange workload only)

Save Cancel

- Name
- Admin units
- Locations
- **Advanced DLP rules**
- Policy mode
- Finish

Edit rule

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

Email notifications

- Notify the user who sent, shared, or last modified the content.
- Notify these people:
- Customize the email text
- Customize the email subject

Policy tips

Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported

- Customize the policy tip text

Please be aware you are sharing sensitive information to potential unauthorized users.

- Show the policy tip as a dialog for the end user before send (available for Exchange workload only)

To help ensure all email messages display the pop-up before they're sent, you must first configure Group Policy Object (GPO) settings to allow for full evaluation. Learn more

- Provide a compliance URL for the end user to learn more about your organization's policies (available for Exchange workload only)

User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

Incident reports

Use this severity level in admin alerts and reports: Low

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

Save Cancel

Favorites
Inbox 9
Sent Ite...
Drafts 2
Deleted ...
Add favo...

Folders
Inbox 9
Drafts 2
Sent Ite...
Deleted ...
Junk Em...
Archive
Notes
Convers...
RSS Feeds
Create n...

Focused Other Filter

WeTransfer
Seabed Jellyfish.docx s... Fri 4:56 PM
Thanks for using WeTransfer! Your fil...

WeTransfer
Your code is: 701901 Fri 4:54 PM
Your code is: 701901 This code will b...

This week

Microsoft Outlook
Collaboration partne... Thu 1:13 PM
Delivery has failed to these recipient...

Microsoft CDX
Issuance of Hold notif... Thu 8:50 AM
TO: Roger Kroch This is the issuance ...

Microsoft Viva
Welcome to your digest Tue 9/26
Private to you Hi, Roger Kroch, Welc...

Last week

Linda Stolp
Jellyfish bugs Wed 9/20
No preview is available.

Linda Stolp
Jellyfish Electrical co... Wed 9/20
No preview is available.

Send this email during your work hours: Mon, Oct 02 at 8:00 AM Schedule send | Dismiss

Policy tip: The item you are about to send contains sensitive information and is classified as highly confidential. Please state your business justification to allow overriding and continue this activity. Show details

The following recipient is outside your organization: evanmeurs@microsoft.com. Remove recipient

Send

To evanmeurs@microsoft.com

Bcc

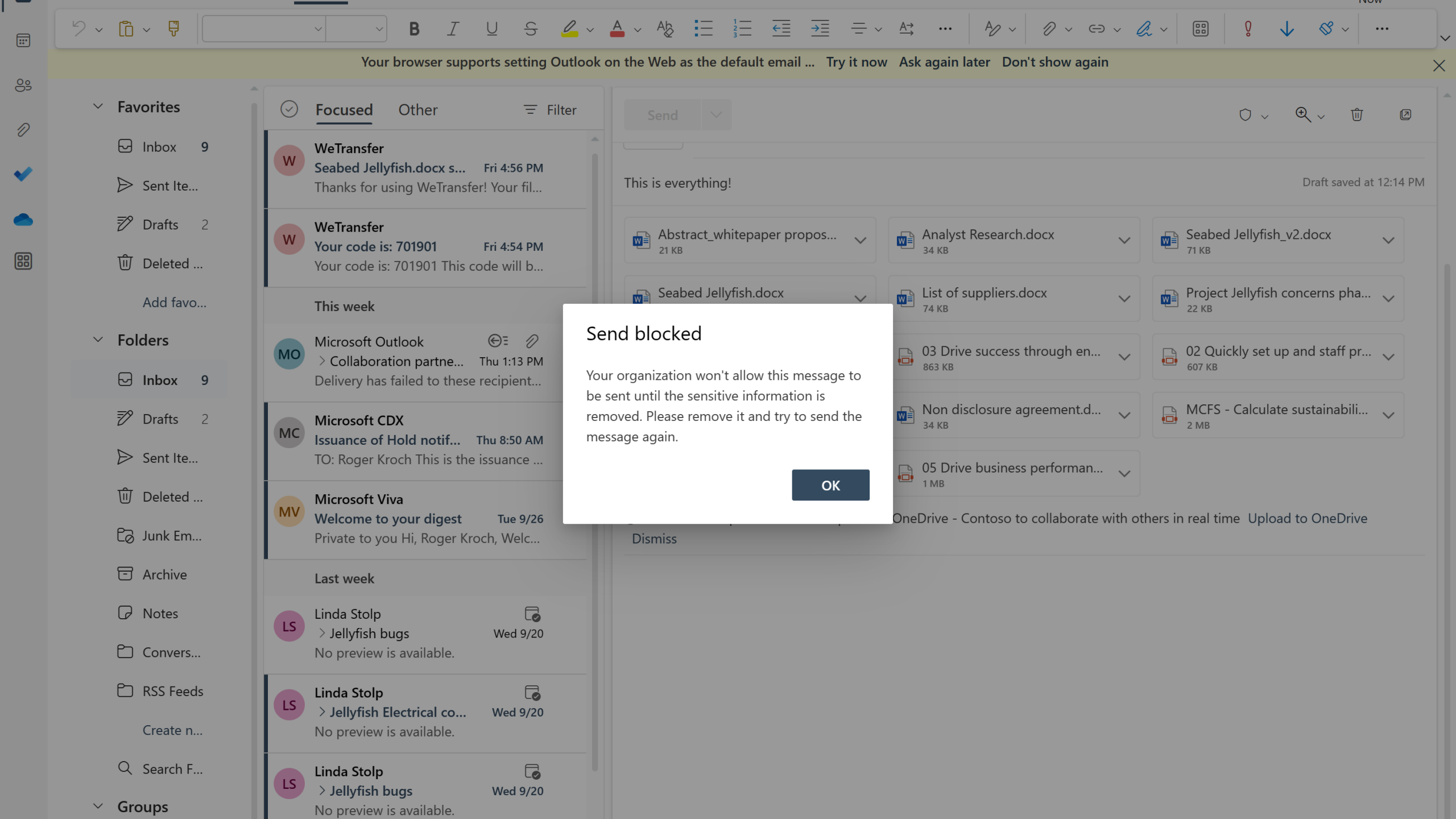
Cc

This is everything!

Draft saved at 12:14 PM

Abstract_whitepaper propos... 21 KB	Analyst Research.docx 34 KB	Seabed Jellyfish_v2.docx 71 KB
Seabed Jellyfish.docx 71 KB	List of suppliers.docx 74 KB	Project Jellyfish concerns pha... 22 KB
Document.docx 71 KB	03 Drive success through en... 863 KB	02 Quickly set up and staff pr... 607 KB
Regulatory Requirements Re... 185 KB	Non disclosure agreement.d... 34 KB	MCFS - Calculate sustainabili... 2 MB
Architecture design.docx 12 KB	05 Drive business performan... 1 MB	

No more multiple file versions. Upload to OneDrive - Contoso to collaborate with others in real time Upload to OneDrive
Dismiss


Your browser supports setting Outlook on the Web as the default email ... Try it now Ask again later Don't show again
Favorites
Inbox 9
Sent Ite...
Drafts 2
Deleted ...
Add favo...
Folders
Inbox 9
Drafts 2
Sent Ite...
Deleted ...
Junk Em...
Archive
Notes
Convers...
RSS Feeds
Create n...
Search F...
Groups
Focused
Other
Filter
WeTransfer
Seabed Jellyfish.docx s... Fri 4:56 PM
Thanks for using WeTransfer! Your fil...
WeTransfer
Your code is: 701901 Fri 4:54 PM
Your code is: 701901 This code will b...
This week
Microsoft Outlook
Collaboration partne... Thu 1:13 PM
Delivery has failed to these recipient...
Microsoft CDX
Issuance of Hold notif... Thu 8:50 AM
TO: Roger Kroch This is the issuance ...
Microsoft Viva
Welcome to your digest Tue 9/26
Private to you Hi, Roger Kroch, Welc...
Last week
Linda Stolp
Jellyfish bugs Wed 9/20
No preview is available.
Linda Stolp
Jellyfish Electrical co... Wed 9/20
No preview is available.
Linda Stolp
Jellyfish bugs Wed 9/20
No preview is available.
Send
This is everything!
Draft saved at 12:14 PM
Abstract_whitepaper propos... 21 KB
Analyst Research.docx 34 KB
Seabed Jellyfish_v2.docx 71 KB
Seabed Jellyfish.docx
List of suppliers.docx 74 KB
Project Jellyfish concerns pha... 22 KB
03 Drive success through en... 863 KB
02 Quickly set up and staff pr... 607 KB
Non disclosure agreement.d... 34 KB
MCFS - Calculate sustainabili... 2 MB
05 Drive business performan... 1 MB
OneDrive - Contoso to collaborate with others in real time Upload to OneDrive
Dismiss
Send blocked
Your organization won't allow this message to be sent until the sensitive information is removed. Please remove it and try to send the message again.
OK

Calibri 12

Favorites
Inbox 9
Sent Ite...
Drafts 3
Deleted ...
Add favo...
Folders
Inbox 9
Drafts 3
Sent Ite...
Deleted ...
Junk Em...
Archive
Notes
Convers...
RSS Feeds
Create n...
Search F...

Focused Other Filter

WeTransfer
Seabed Jellyfish.docx s... Fri 4:56 PM
Thanks for using WeTransfer! Your fil...

WeTransfer
Your code is: 701901 Fri 4:54 PM
Your code is: 701901 This code will b...

This week

Microsoft Outlook
Collaboration partne... Thu 1:13 PM
Delivery has failed to these recipient...

Microsoft CDX
Issuance of Hold notif... Thu 8:50 AM
TO: Roger Kroch This is the issuance ...

Microsoft Viva
Welcome to your digest Tue 9/26
Private to you Hi, Roger Kroch, Welc...

Last week

Linda Stolp
Jellyfish bugs Wed 9/20
No preview is available.

Linda Stolp
Jellyfish Electrical co... Wed 9/20
No preview is available.

Linda Stolp
Jellyfish bugs Wed 9/20

Your organization automatically applied the Sensitivity: Highly Confidential - Jellyfish

Policy tip: The item you are about to send contains sensitive information and is classified as highly confidential. Please state your business justification to allow overriding and continue this activity. Show details

The following recipient is outside your organization: evanmeurs@microsoft.com. Remove recipient

Send

To evanmeurs@microsoft.com Bcc

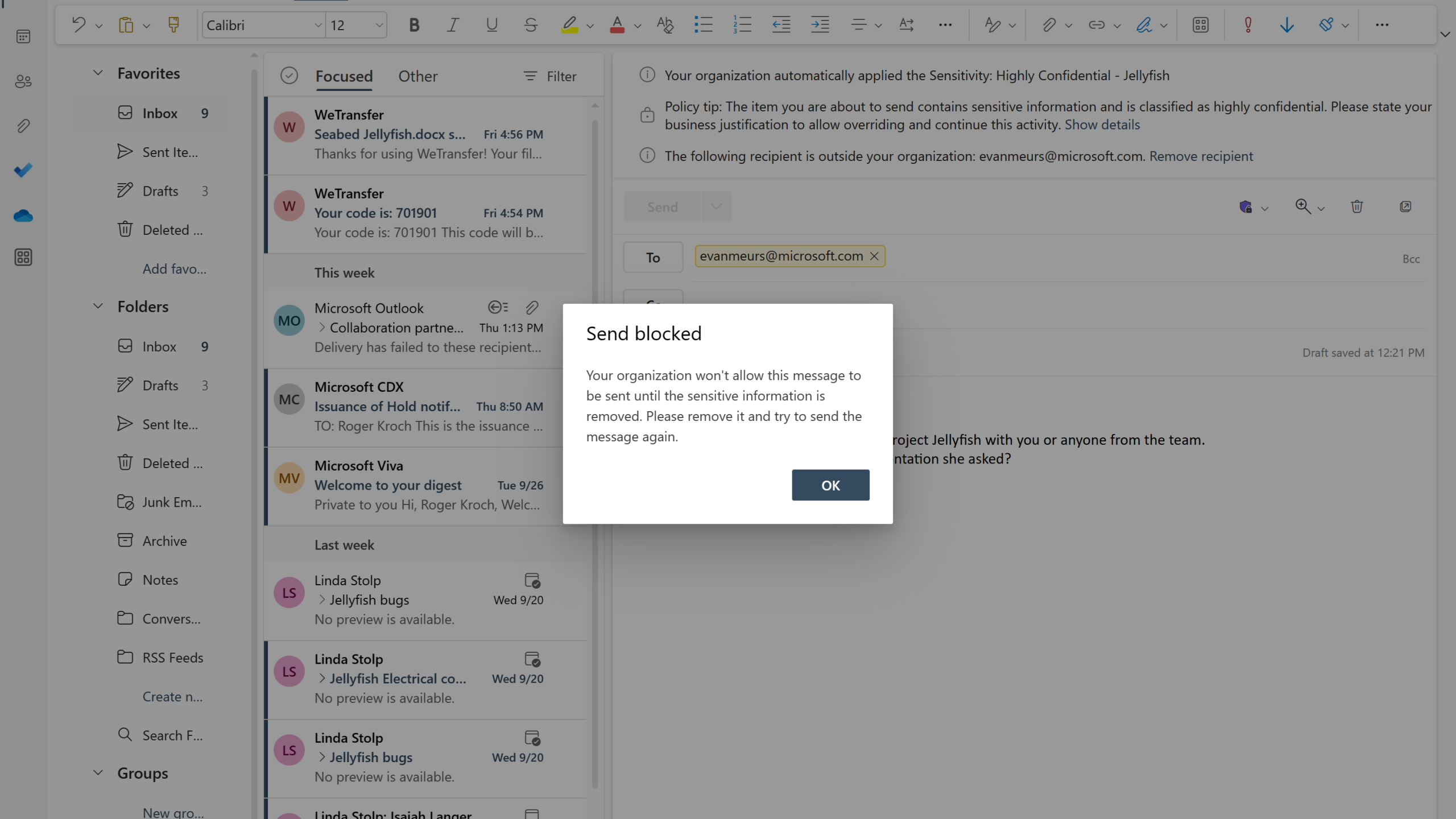
Cc

Communication block Draft saved at 12:21 PM

Hi Ellen,

I am not able to send anything related to Project Jellyfish with you or anyone from the team.
Could you send Anna the required documentation she asked?

RK


Calibri
12
Favorites
Inbox 9
Sent Ite...
Drafts 3
Deleted ...
Add favo...
Folders
Inbox 9
Drafts 3
Sent Ite...
Deleted ...
Junk Em...
Archive
Notes
Convers...
RSS Feeds
Create n...
Search F...
Groups
New gro...
Focused
Other
Filter
WeTransfer
Seabed Jellyfish.docx s... Fri 4:56 PM
Thanks for using WeTransfer! Your fil...
WeTransfer
Your code is: 701901 Fri 4:54 PM
Your code is: 701901 This code will b...
This week
Microsoft Outlook
Collaboration partne... Thu 1:13 PM
Delivery has failed to these recipient...
Microsoft CDX
Issuance of Hold notif... Thu 8:50 AM
TO: Roger Kroch This is the issuance ...
Microsoft Viva
Welcome to your digest Tue 9/26
Private to you Hi, Roger Kroch, Welc...
Last week
Linda Stolp
Jellyfish bugs Wed 9/20
No preview is available.
Linda Stolp
Jellyfish Electrical co... Wed 9/20
No preview is available.
Linda Stolp
Jellyfish bugs Wed 9/20
No preview is available.
Linda Stolp: Isaiah Langer
Your organization automatically applied the Sensitivity: Highly Confidential - Jellyfish
Policy tip: The item you are about to send contains sensitive information and is classified as highly confidential. Please state your business justification to allow overriding and continue this activity. Show details
The following recipient is outside your organization: evanmeurs@microsoft.com. Remove recipient
Send
To
evanmeurs@microsoft.com
Bcc
Draft saved at 12:21 PM
roject Jellyfish with you or anyone from the team.
ntation she asked?
Send blocked
Your organization won't allow this message to be sent until the sensitive information is removed. Please remove it and try to send the message again.
OK

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

Choose a policy template

Policy templates specify the conditions and indicators that define the risk activities you want to be alerted to.

Data theft

- Data theft by departing users

Data leaks

- Data leaks
- Data leaks by priority users
- Data leaks by risky users

Security policy violations (preview)

- Security policy violations (preview)
- Security policy violations by departing users (preview)
- Security policy violations by risky users (preview)
- Security policy violations by priority users (preview)

Health record misuse (preview)

- Health record misuse (preview)

Risky browser usage (preview)

- Risky browser usage (preview)

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.

Prerequisites

DLP policy OPTIONAL

Devices onboarded OPTIONAL

To detect activity on devices, you must have devices onboarded to the compliance portal. Devices onboarded

Physical badging connector OPTIONAL

Physical badging connector configured to periodically import access events to priority physical locations. Set up badging connector

Triggering event

- User performs selected exfiltration activities that exceed specific thresholds.
- User performs an activity matching specified DLP policy.

Activities detected 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**
- Triggering event
- Indicators
- Finish

Decide whether to prioritize content

You can prioritize content based on factors like where it's stored and how it's classified. Risk scores are increased for any activity that contains priority content, which in turn increases the chance of generating a high severity alert. Learn about the benefits of prioritizing content

- (●) **I want to prioritize content**
  Choose what to prioritize. You'll add the specific items in the next step.
  - [x] Sharepoint sites
  - [x] Sensitivity labels
  - [x] Sensitive info types
  - [ ] File extensions
  - [ ] Trainable classifiers
- ( ) **I don't want to prioritize content right now**
  You can return to this step after the policy is created

Back Next Cancel

Policy template
Name and description
Users and groups
Content to prioritize
Triggering event
Trigger thresholds
Indicators
Finish

Choose thresholds for triggering events

Each triggering event you specified uses built-in thresholds to start scoring activity for users included in this policy. Thresholds are based on the number of events recorded for an activity per day. However, you can bypass these built-in thresholds and define your own.

- ( ) Apply built-in thresholds (recommended)
- (•) Choose your own thresholds

Sending email with attachments to recipients outside the organization

- [x] Total number of activities
  50 per day
- [x] Number of activities for emails containing sensitive info types
  20 per day
- [x] Number of activities for emails matching priority content
  10 per day
- [x] Number of activities performed in which target is unallowed domain
  3 per day
- [x] Activity is above user's usual activity for the day

Reset to defaults

Sharing SharePoint files with people outside the organization

- [x] Total number of activities
  28 per day
- [x] Number of activities for files containing sensitive info types
  10 per day
- [x] Number of activities for files matching priority content
  5 per day
- [x] Number of activities performed in which target is unallowed domain

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

Indicators

The following indicators are used to generate alerts for the activity detected by the policy template you selected. Learn more

Total indicators selected: 32/47

Unable to select some indicators? This is because they're currently turned off in your organization. To make them available to select, you can turn them on now.

Choose indicators

Office indicators (28/28)

- [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 OneDrive
- [x] Syncing content from OneDrive
- [x] Downloading content from SharePoint
- [x] Syncing content from SharePoint
- [x] Adding people outside organization to priority SharePoint sites
- [x] Downgrading sensitivity labels applied to SharePoint files
- [x] Removing sensitivity labels from SharePoint files
- [x] Removing sensitivity labels from SharePoint sites
- [x] Accessing sensitive or priority SharePoint files
- [x] Granting access to sensitive or priority SharePoint resources to people outside organization
- [x] Requesting access to sensitive or priority SharePoint resources
- [x] Deleting of SharePoint files
- [x] Deleting of SharePoint files from first stage recycling bin
- [x] Deleting of SharePoint files from second stage recycling bin
- [x] Deleting of SharePoint folders

Policy template
Name and description
Users and groups
Content to prioritize
Triggering event
Indicators
Detection options
Indicator thresholds
Finish

Activity insights over past 10 days (preview)

Insights based on users and activities included in this policy

Approximately 0 users exceeded lowest daily thresholds for at least one activity

Top 3 activities where users exceeded lowest daily thresholds

Activity	Users
Sharing SharePoint files with people outside the organization	0
Downloading content from OneDrive	0
Accessing sensitive or priority SharePoint files	0

Downloading content from Teams

100 to 250 events per day generates low severity alerts

250 to 500 events per day generates medium severity alerts

500 > 500 events per day generates high severity alerts

No data available

Reset to defaults

Sending Teams messages that contain sensitive info types

20 to 50 events per day generates low severity alerts

50 to 200 events per day generates medium severity alerts

200 > 200 events per day generates high severity alerts

No data available

Reset to defaults

Adding users outside the organization to a Teams private channel

20 to 50 events per day generates low severity alerts

50 to 200 events per day generates medium severity alerts

200 > 200 events per day generates high severity alerts

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

Review settings and finish

Review the settings for your insider risk policy. The policy will take effect immediately after you create it, but may take up to 24 hours to start generating alerts. We recommend letting your users know how these changes will impact them.

Policy template

Data leaks

Edit policy type

Policy name and description

Project Jellyfish data theft and leakage
This policy discovers the potential theft and/or leakage of highly sensitive data related to this domain of the organization.

Edit policy name and description

Users and groups

All

Edit users and groups

Content to prioritize

https://m365x98433645.sharepoint.com/sites/safety
https://m365x98433645.sharepoint.com/sites/RecordsManagementAdmins
https://m365x98433645.sharepoint.com/sites/contosoteam
https://m365x98433645.sharepoint.com/sites/ProjectJellyfish
Project Jellyfish
Highly Confidential\Jellyfish
Highly Confidential - Jellyfish

Edit content to prioritize

Triggering event

Built-in data leak trigger

Edit triggers

Policy indicators

37/69 selected
No customized thresholds

Edit policy indicators

Back Submit Cancel

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

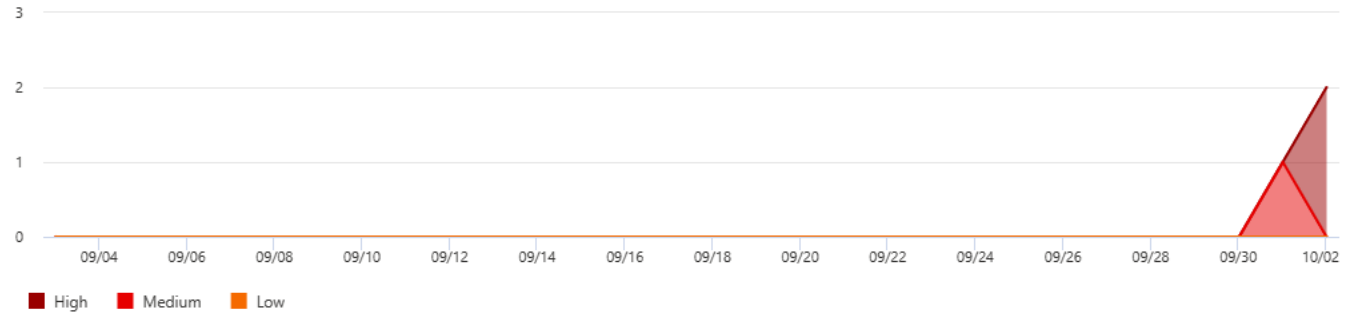
Insider risk management

Overview | Alerts | Cases | Policies | Users | Forensic evidence | Notice templates | Adaptive protection (preview)

Total alerts that need review

High	Medium	Low
2	0	0

Open alerts over past 30 days



Average time to resolve alerts

High severity alerts
Resolution time not available

Medium severity alerts
Resolution time not available

Low severity alerts
Resolution time not available

Alerts summary

100% of alerts still need review

Export | 2 items | Alerts tutorial | Search | Filter

ID	Users	Alert	Status	Alert severity	Time detected	Assigned to	Case	Case status	Risk factors
bbbf7e99	#Anonymized#EAAAA...	Adaptive Protection policy for Insider ...	Needs review	High	19 hours ago	Unassigned		No case	Activities include
ba4a7eab	#Anonymized#EAAAA...	Adaptive Protection policy for Insider ...	Needs review	High	2 days ago	Unassigned		No case	Activities include

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(ba4a7eab) Adaptive Protection policy for Insider Risk Management

Assign | Needs review | Confirm all alerts & create case | Dismiss alert

What will these actions do?

High Risk score: 75/100 Alert created on Sep 30, 2023 (UTC)

Activity that generated this alert

Reduce alerts for this activity

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Triggering event

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

User details

#Anonymized#EAAAACqvzjrIc0TQmxem82YeYYQxq+6xKeT4A+hp0peWBuDEjb+S556okDpjspc1FyjWxGaIV2mQiXnY5+Q0FRLCGao=

View all details

User alert history

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

All risk factors | Activity explorer | User activity

All risk factors for this user's activity

Top exfiltration activities

10 exfiltration activities

File shared externally from SPO 6
Email sent to external recipient 4

View all exfiltration activity

Cumulative exfiltration activities

No cumulative exfiltration activities detected

View all cumulative exfiltration activities

Sequences of activity

5 sequence activities

View all sequence activity

Unusual activity for this user

No activity is considered unusual for this user

View all unusual activity

Priority content

Unallowed domains

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Priority content

⚠ **12 activities include events with priority content**

View all priority content activity

Unallowed domains

No activity includes events with unallowed domains

View all unallowed domain activity

Content detected

Top labels

4 with sensitivity labels

Label	Number of activit...
General\Anyone (unrestricted)	2
Personal	1
Confidential\Anyone (unrestrict...	1

Top sensitive info types

4 with sensitive info ty...

Sensitive info type	Number of activit...
Project Jellyfish	2
All Medical Terms And Conditio...	1
Project Olivine	1

Classifiers

No Classifiers detected

Top Keywords

12 with keywords dete...

Keyword	Number of instan...
abstract	4
proposal	4
whitepaper	4

Top SharePoint sites

6 with SharePoint sites

Site name	Number of activit...
https://m365x98433645-my.sh...	6

SharePoint labels

No SharePoint labels d...

Top Recipients

4 with recipients

User	Items shared
ajaganjac@microsoft.com	3
evanmeurs@microsoft.com	1

Top Recipient domains

4 with destination dom...

Domain	Items shared
microsoft.com	4

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(ba4a7eab) Adaptive Protection policy for Insider Risk Management

Megan Bowen | Needs review | Confirm all alerts & create case | Dismiss alert

What will these actions do?

High Risk score: 75/100 Alert created on Sep 30, 2023 (UTC)

Activity that generated this alert

Reduce alerts for this activity

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Triggering event

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

User details

#Anonymized#EAAAACqvzjrIc0TQmxem82YeYYQxq+6xKeT4A+hp0peWBuDEjb+S556okDpjspc1FyjWxGaIV2mQiXnY5+Q0FRLCGao=

View all details

User alert history

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

All risk factors | Activity explorer | User activity

Filter:
Show: Only scored activity in this alert
Risk factor: Any
Review status: All
Sort by

(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Confidential\Anyone (unrestricted)

(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people

Export | 39 items | Reset columns | Choose columns | Save this view | Views

Filter | Reset | Filters

Activity: Any | Date (UTC): 3/2/2023-10/2/2023

Date (UTC)	Activity	File name	Item type	Object ID	Workload
Sep 30, 2023 10:13 AM	File accessed on SPO	Document.docx	File	https://m365x98433645-my....	OneDrive
Sep 30, 2023 10:13 AM	File accessed on SPO	Seabed Jellyfish_v2.docx	File	https://m365x98433645-my....	OneDrive
Sep 30, 2023 10:12 AM	File downloaded from OneDrive	Project Jellyfish concerns ph...	File	https://m365x98433645-my....	OneDrive
Sep 30, 2023 10:12 AM	File downloaded from OneDrive	Seabed Jellyfish.docx	File	https://m365x98433645-my....	OneDrive
Sep 30, 2023 10:12 AM	File downloaded from OneDrive	Analyst Research.docx	File	https://m365x98433645-my....	OneDrive
Sep 30, 2023 10:12 AM	File downloaded from OneDrive	Architecture design.docx	File	https://m365x98433645-my....	OneDrive

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

#Anonymized#EAAAAOgvvx3oa1g6JNG7MCUC2CzbLjWpAdDj3eQWmSKW/Wp/yigYjQQCd6A696ncCM0zpniVwy9MLSJhO63BrazZokU=

View all details

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

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

(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Confidential\Anyone (unrestricted)

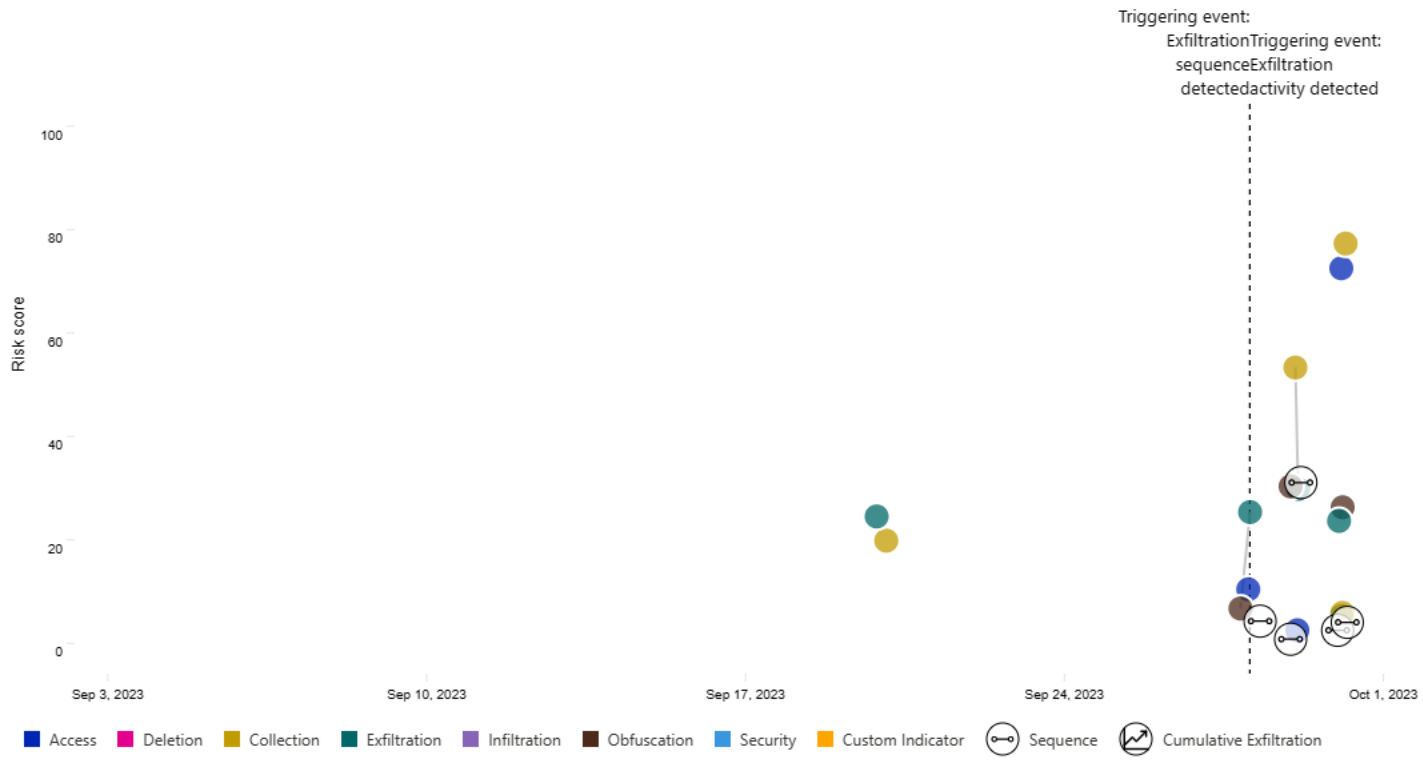
(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org

Exfiltration: Emails with attachments sent outside the organization
Sep 30, 2023 (UTC) | Risk score: 5/100
1 email: sent to 1 recipient outside the organization
1 email: containing sensitive info, including: Project Jellyfish, Project Olivine

Access: Sensitive SharePoint files accessed
Sep 30, 2023 (UTC) | Risk score: 75/100
3 events: Sensitive files accessed from 1 SharePoint site
3 events: Files that have labels applied, including: Highly Confidential - Jellyfish, Highly Confidential\Jellyfish
3 events: Sites that have labels applied, including:

Obfuscation: Labels of sensitive files downgraded on SharePoint

User activity scatter plot 6 Months | 3 Months | **1 Month**



Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

#Anonymized#EAAAAOgvvx3oa1g6JNG7MCUC2CzbLjWpAdDj3eQWmSKW/Wp/yigYjQQCd6A696ncCM0zpniVwy9MLSJhO63BrazZokU=

View all details

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

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

(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Confidential\Anyone (unrestricted)

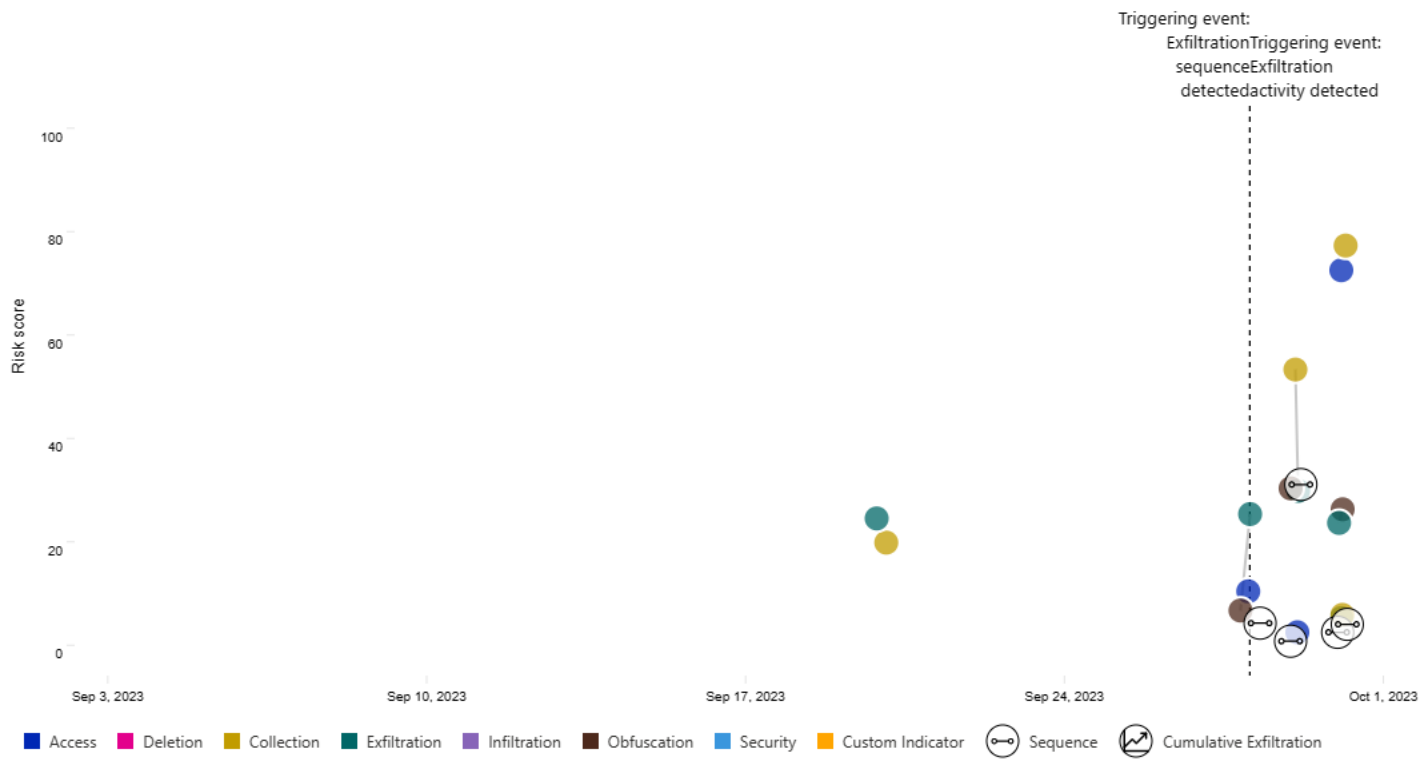
Exfiltration: SharePoint files shared
Sep 30, 2023 (UTC) | Risk score: 25/100
2 events: Files shared
2 events: Files that have labels applied, including: General\Anyone (unrestricted)

Obfuscation: Labels of sensitive files downgraded on SharePoint
Sep 30, 2023 (UTC) | Risk score: 25/100
3 events: Labels of SharePoint files downgraded
3 events: Files that have labels applied, including: Confidential\Anyone (unrestricted), Highly Confidential - Jellyfish

(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org

Exfiltration: Emails with attachments sent outside the organization
Sep 30, 2023 (UTC) | Risk score: 5/100
1 email: sent to 1 recipient outside the organization

User activity scatter plot 6 Months | 3 Months | **1 Month**



Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

#Anonymized#EAAAAOgvvx3oa1g6JNG7MCUC2CzbLjWpAdDj3eQWmSKW/Wp/yigYjQQCd6A696ncCM0zpniVwy9MLSJhO63BrazZokU=

View all details

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

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

(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Confidential\Anyone (unrestricted)

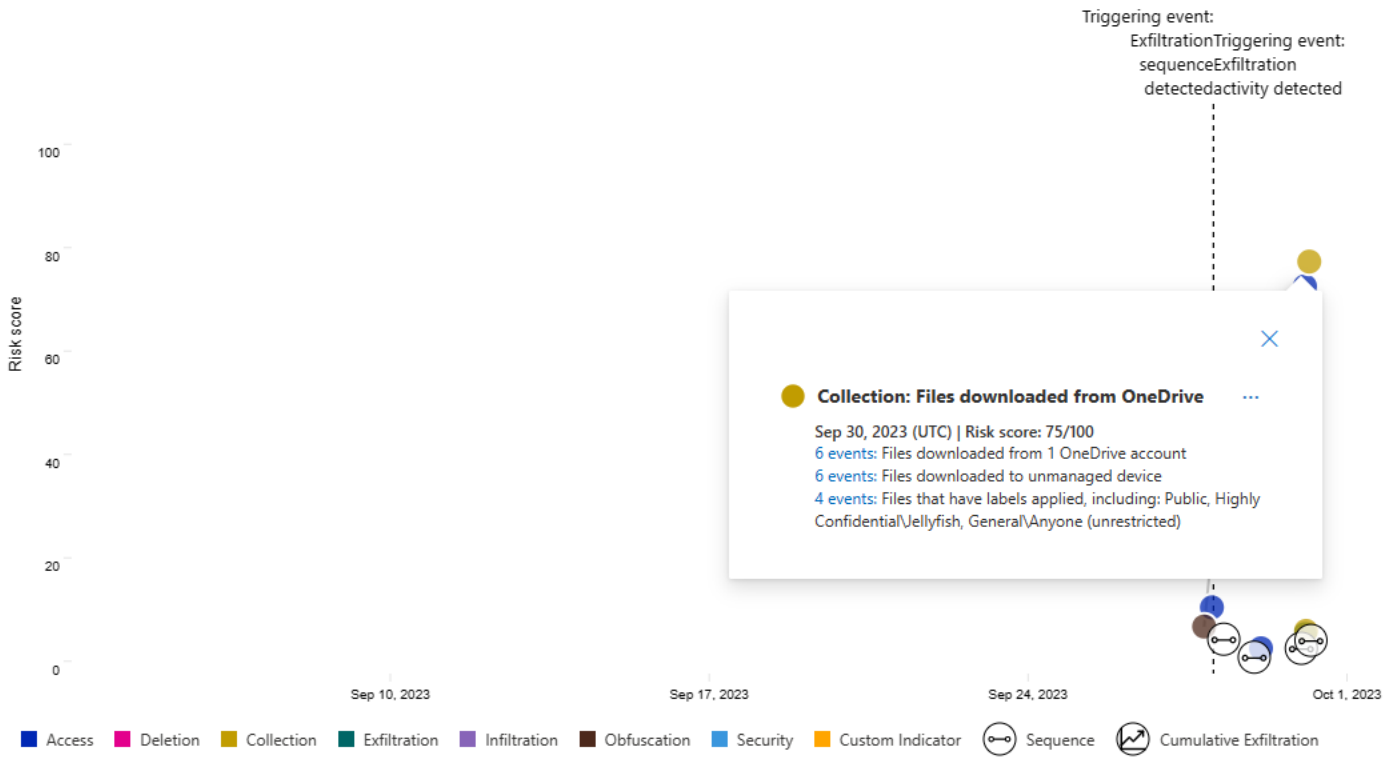
Exfiltration: SharePoint files shared
Sep 30, 2023 (UTC) | Risk score: 25/100
2 events: Files shared
2 events: Files that have labels applied, including: General\Anyone (unrestricted)

Obfuscation: Labels of sensitive files downgraded on SharePoint
Sep 30, 2023 (UTC) | Risk score: 25/100
3 events: Labels of SharePoint files downgraded
3 events: Files that have labels applied, including: Confidential\Anyone (unrestricted), Highly Confidential - Jellyfish

(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org

Exfiltration: Emails with attachments sent outside the organization
Sep 30, 2023 (UTC) | Risk score: 5/100
1 email: sent to 1 recipient outside the organization

User activity scatter plot 6 Months | 3 Months | **1 Month**



Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

#Anonymized#EAAAAOgvvx3oa1g6JNG7MCUC2CzbLjWpAdDj3eQWmSKW/Wp/yigYjQQCd6A696ncCM0zpniVwy9MLSJhO63BrazZokU=

View all details

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

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

(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Confidential\Anyone (unrestricted)

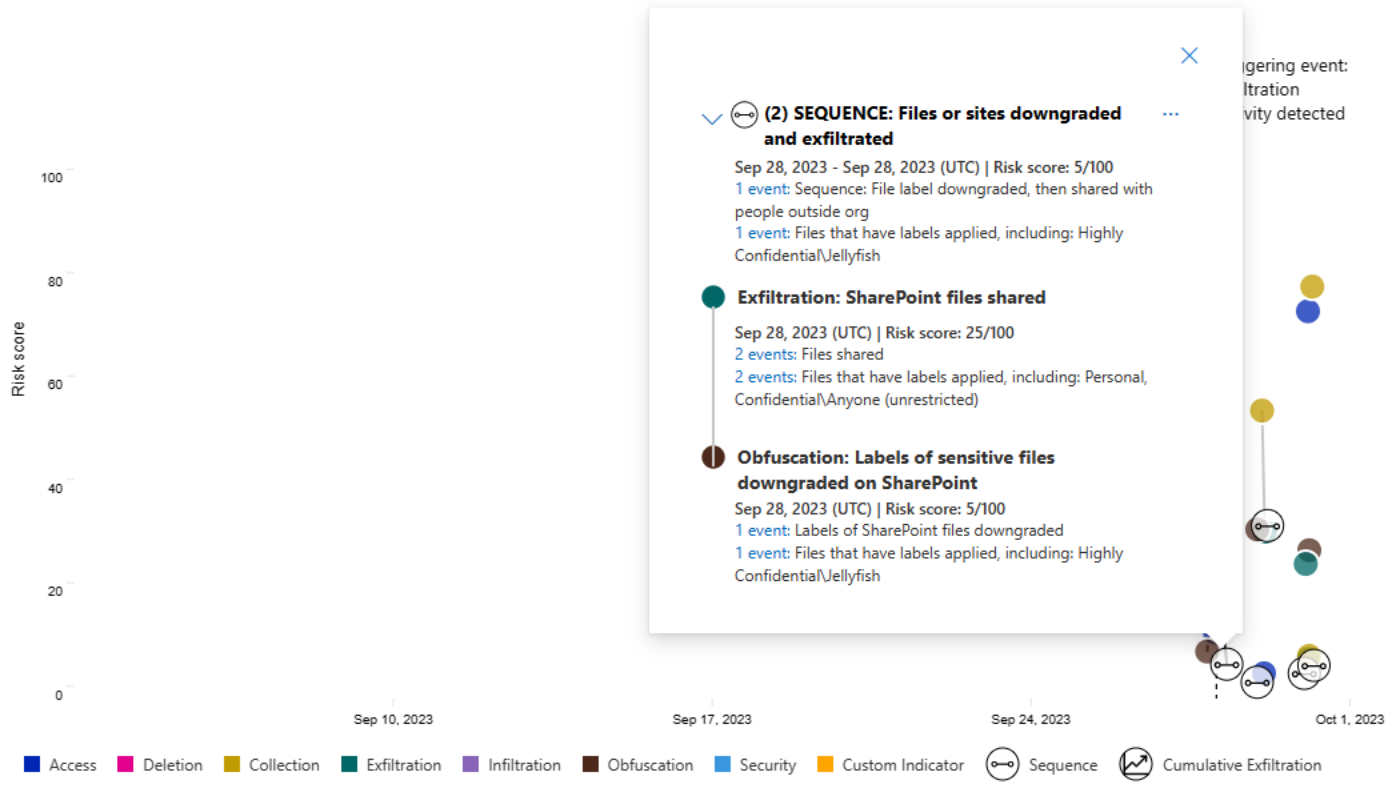
Exfiltration: SharePoint files shared
Sep 30, 2023 (UTC) | Risk score: 25/100
2 events: Files shared
2 events: Files that have labels applied, including: General\Anyone (unrestricted)

Obfuscation: Labels of sensitive files downgraded on SharePoint
Sep 30, 2023 (UTC) | Risk score: 25/100
3 events: Labels of SharePoint files downgraded
3 events: Files that have labels applied, including: Confidential\Anyone (unrestricted), Highly Confidential - Jellyfish

(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org

Exfiltration: Emails with attachments sent outside the organization
Sep 30, 2023 (UTC) | Risk score: 5/100
1 email: sent to 1 recipient outside the organization

User activity scatter plot 6 Months | 3 Months | **1 Month**



(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 28, 2023 - Sep 28, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Highly Confidential\Jellyfish

Exfiltration: SharePoint files shared
Sep 28, 2023 (UTC) | Risk score: 25/100
2 events: Files shared
2 events: Files that have labels applied, including: Personal, Confidential\Anyone (unrestricted)

Obfuscation: Labels of sensitive files downgraded on SharePoint
Sep 28, 2023 (UTC) | Risk score: 5/100
1 event: Labels of SharePoint files downgraded
1 event: Files that have labels applied, including: Highly Confidential\Jellyfish

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Sep 29, 2023 (UTC)

This user performed exfiltration activity.

#Anonymized#EAAAAOgvvx3oa1g6JNG7MCUC2CzbLjWpAdDj3eQWmSKW/Wp/yigYjQQCd6A696ncCM0zpniVwy9MLSJhO63BrazZokU=

View all details

Last 30 days

Adaptive Protection policy for Insider Ris... 1 alert

View full user history

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

(2) SEQUENCE: Files or sites downgraded and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: File label downgraded, then shared with people outside org
1 event: Files that have labels applied, including: Confidential\Anyone (unrestricted)

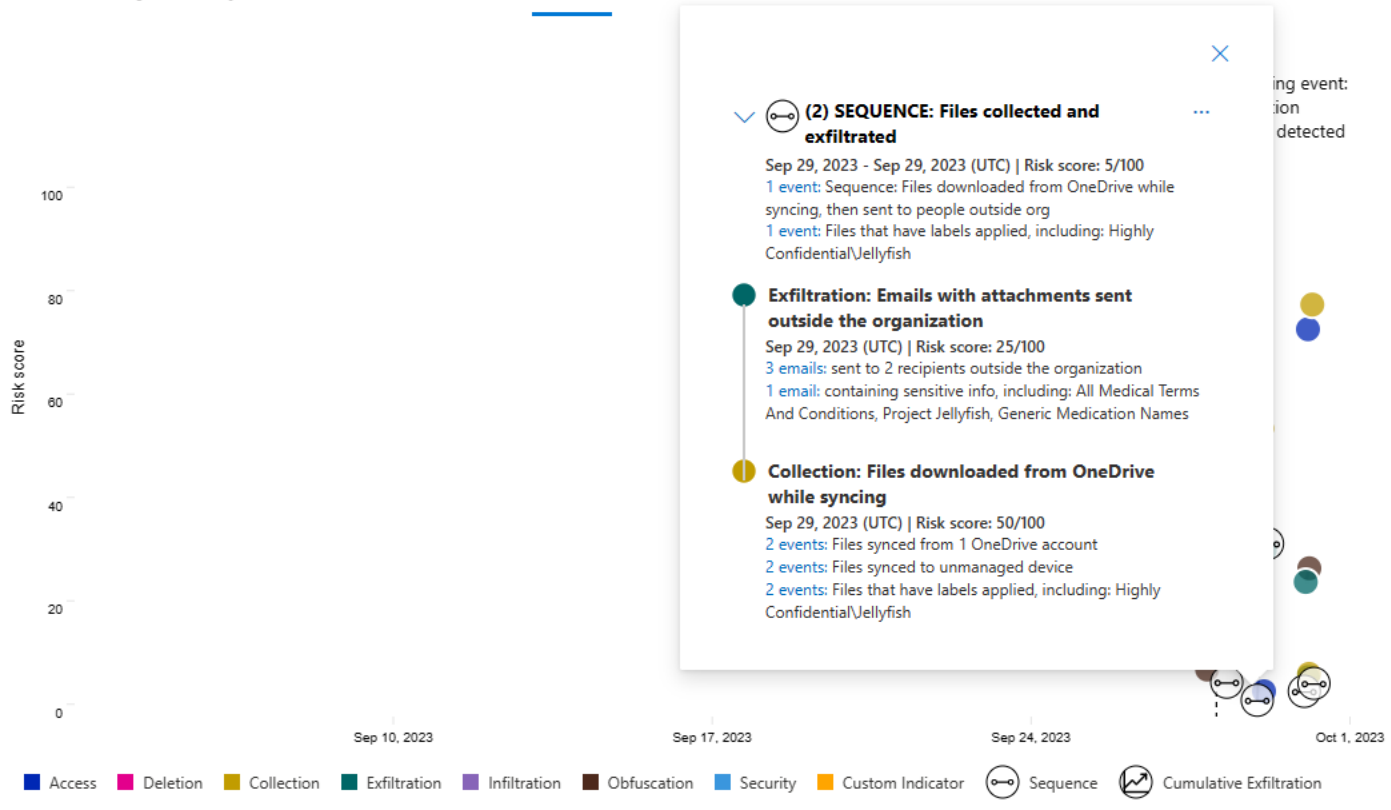
Exfiltration: SharePoint files shared
Sep 30, 2023 (UTC) | Risk score: 25/100
2 events: Files shared
2 events: Files that have labels applied, including: General\Anyone (unrestricted)

Obfuscation: Labels of sensitive files downgraded on SharePoint
Sep 30, 2023 (UTC) | Risk score: 25/100
3 events: Labels of SharePoint files downgraded
3 events: Files that have labels applied, including: Confidential\Anyone (unrestricted), Highly Confidential - Jellyfish

(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org

Exfiltration: Emails with attachments sent outside the organization
Sep 30, 2023 (UTC) | Risk score: 5/100
1 email: sent to 1 recipient outside the organization

User activity scatter plot 6 Months | 3 Months | **1 Month**



(2) SEQUENCE: Files collected and exfiltrated
Sep 29, 2023 - Sep 29, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org
1 event: Files that have labels applied, including: Highly Confidential\Jellyfish

Exfiltration: Emails with attachments sent outside the organization
Sep 29, 2023 (UTC) | Risk score: 25/100
3 emails: sent to 2 recipients outside the organization
1 email: containing sensitive info, including: All Medical Terms And Conditions, Project Jellyfish, Generic Medication Names

Collection: Files downloaded from OneDrive while syncing
Sep 29, 2023 (UTC) | Risk score: 50/100
2 events: Files synced from 1 OneDrive account
2 events: Files synced to unmanaged device
2 events: Files that have labels applied, including: Highly Confidential\Jellyfish

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(ba4a7eab) Adaptive Protection policy for Insider Risk Management

Megan

High Risk score: 75/100 Alert created on Sep 30, 2023 (UTC)

Activity that generated this alert Reduce alerts for this activity

Data Collection: Files downloaded from OneDrive
75/100 **High severity** | Sep 30, 2023 (UTC)
6 events: Files downloaded from 1 OneDrive account
6 events: Files downloaded to unmanaged device
4 events: Files that have labels applied, including: Public, Highly Confidential\Jellyfish, General\Anyone (unrestricted)
Factors that impacted risk score:
Includes priority content (1 event)

Note: 1 other activity has the same risk score of 75/100

View all activity

Triggering event
Sep 29, 2023 (UTC)
This user performed exfiltration activity.

User det
#Anonymiz
LjWpAdDj3
zpniVwy9M
View all det

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

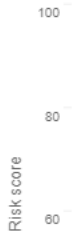
Confidential\Anyone (unrestricted), Highly Confidential - Jellyfish

(2) SEQUENCE: Files collected and exfiltrated
Sep 30, 2023 - Sep 30, 2023 (UTC) | Risk score: 5/100
1 event: Sequence: Files downloaded from OneDrive while syncing, then sent to people outside org

Exfiltration: Emails with attachments sent outside the organization
Sep 30, 2023 (UTC) | Risk score: 5/100
1 email: sent to 1 recipient outside the organization
1 email: containing sensitive info, including: Project Jellyfish, Project Olivine

Collection: Files downloaded from OneDrive while syncing
Sep 30, 2023 (UTC) | Risk score: 5/100

User activity scatter plot 6 Months | 3 Months | 1 Month



User alert history

Total alerts
1 alert needs review

Newest to oldest

This alert: Adaptive Protection policy for Insider Risk Management

Oct 1, 2023 (UTC)
Alert severity increased
Alert ID: ba4a7eab
Severity: High
Case ID:

Sep 30, 2023 (UTC)
Alert severity increased
Alert ID: ba4a7eab
Severity: Medium
Case ID:

Sep 30, 2023 (UTC)
Alert created
Alert ID: ba4a7eab
Severity: Low
Case ID:

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(fe785bc8) Jellyfish investigation 0014

Active High 75 risk score

Megan Bowen Resolve case Case actions

Case overview Alerts User activity Activity explorer Content explorer Case notes Contributors

About this case

Case information

Status
Active

Case created on
02/10/2023, 17:37:17

User details

User's risk score
75/100

Email
#Anonymized#EAAAAHbMefyWko/mtKx6q6MsojiHcsktZWE

Alerts

Policy matches	ID	Status	Severity	Time detected
Adaptive Protection policy for Inside...	ba4a7eab	Confirmed	High	2 days ago

View all details

Content detected

Top labels

4 with sensitivity labels

Label	Number of activities
General\Anyone (unrestricted)	2
Personal	1
Confidential\Anyone (unrestrict...	1

Top sensitive info types

4 with sensitive info types

Sensitive info type	Number of activities
Project Jellyfish	2
All Medical Terms And Conditio...	1
Project Olivine	1

Classifiers

No Classifiers detected

Top Keywords

12 with keywords detected

Keyword	Number of instances
abstract	4
proposal	4
whitepaper	4

Top SharePoint sites

SharePoint labels

Top Recipients

Top Recipient domains

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(fe785bc8) Jellyfish investigation 0014

Active High 75 risk score

Megan Bowen Resolve case Case actions

Case overview Alerts User activity Activity explorer **Content explorer** Case notes Contributors

Examine the emails and files captured by the policies included in this case. Learn more

Last Updated Today

Filter Reset Filters

Group Choose columns Export all file names 1 of 10 selected

	Subject/Title	Date (UTC)	File class	Sender/Author	Recipients	Sensitivit
☐	More...	Sep 30, 2023 7:17 ...	Email	Roger Kroch <Rog...	ajaganjac@micros...	
☐	Analyst Research.d...	Sep 30, 2023 7:16 ...	Attachment	Irvin Sayers		
☐	Architecture design...	Aug 28, 2023 5:03 ...	Attachment	Roger Kroch		
☐	Non disclosure agr...	Oct 30, 2020 12:56 ...	Document	rogerkroch@m365...		
☐	Check this out	Sep 29, 2023 1:24 P...	Email	Roger Kroch <Rog...	evanmeurs@micro...	
☑	Abstract_whitepap...	Sep 30, 2023 10:04 ...	Document	rogerkroch@m365...		Confiden
☐	item.fs		Email			
☐	Check this	Sep 29, 2023 1:27 P...	Email	Roger Kroch <Rog...	ajaganjac@micros...	

Abstract_whitepaper proposal.docx

Source view

Word Accessibility Mode Print Find Immersive Reader

Title: Project Jellyfish: Harnessing Marine Minerals for Sustainable Battery Energy

Abstract:
Project Jellyfish is an innovative research initiative aimed at exploring the untapped potential of marine minerals for sustainable energy storage solutions. As the world faces the growing challenges of energy security and environmental sustainability, this research project seeks to leverage the rich mineral resources found in the depths of our oceans to develop advanced battery technologies. By focusing on the extraction and utilization of marine minerals, Project Jellyfish aims to contribute to the development of cleaner, more efficient, and environmentally friendly energy storage systems.

1. Introduction
The demand for energy storage solutions has risen significantly in recent years due to the increasing integration of renewable energy sources and the electrification of various sectors. Traditional lithium-ion batteries, while effective, face challenges related to resource availability, environmental impact, and energy density. Project Jellyfish proposes a novel approach by harnessing minerals from the sea to address these issues.

2. Objectives
- To identify and characterize marine minerals suitable for battery applications.
- To develop sustainable and cost-effective extraction methods for marine minerals.
- To design and optimize battery prototypes using marine-mineral-derived materials.

Page 1 of 2 88% Give Feedback to Microsoft

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(fe785bc8) Jellyfish investigation 0014

Active High 75 risk score

Megan Bowen **Resolve case** Case actions

- Send email notice
- Escalate for investigation
- Automate
- Share
- Manage pseudonymize
- Learn more about insider risk cases

Case overview Alerts User activity A Case notes Contributors

About this case

Case information

Status
Active

Case created on
02/10/2023, 17:37:17

#Anonymized#EAAAADdQMUWlos+z1tUWEM2vEldfSCY/q(

View all details

Alerts

Policy matches	ID	Status	Severity	Time detected
Adaptive Protection policy for Inside...	ba4a7eab	Confirmed	High	2 days ago

Content detected

Top labels

4 with sensitivity labels

Label	Number of activities
General\Anyone (unrestricted)	2
Personal	1
Confidential\Anyone (unrestrict...	1

Top sensitive info types

4 with sensitive info types

Sensitive info type	Number of activities
Project Jellyfish	2
All Medical Terms And Conditio...	1
Project Olivine	1

Classifiers

No Classifiers detected

Top Keywords

12 with keywords detected

Keyword	Number of instances
abstract	4
proposal	4
whitepaper	4

Top SharePoint sites

SharePoint labels

Top Recipients

Top Recipient domains

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Overview
Policies
Alerts
Endpoint DLP settings
Activity explorer
eDiscovery
Data lifecycle management
Information protection
Overview
Labels
Label policies
Auto-labeling
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests
Settings
More resources
Customize navigation

(fe785bc8) Jellyfish investigation 0014

Active High 75 risk score

Megan Bowen Resolve case Case actions

Case overview | Alerts | User activity | Activity explorer | Content explorer | Case notes | Contributors

About this case

Case information

Status
Active

Case created on
02/10/2023, 17:37:17

User details

User's risk score
75/100

Email
RogerKroch@M365x98433645.onmicrosoft.com

Alerts

Policy matches	ID	Status	Severity	Time detected
Adaptive Protection policy for Inside...	ba4a7eab	Confirmed	High	3 days ago

View all details

Content detected

Top labels

4 with sensitivity labels

Label	Number of activities
General\Anyone (unrestricted)	2
Personal	1
Confidential\Anyone (unrestrict...	1

Top sensitive info types

4 with sensitive info types

Sensitive info type	Number of activities
Project Jellyfish	2
All Medical Terms And Conditio...	1
Project Olivine	1

Classifiers

No Classifiers detected

Top Keywords

12 with keywords detected

Keyword	Number of instances
abstract	4
proposal	4
whitepaper	4

Top SharePoint sites

SharePoint labels

Top Recipients

Top Recipient domains

Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions

Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

(fe785bc8) Jellyfish investigation 0014

Active High 75 risk score

Megan Bowen Resolve case Case actions

Case overview Alerts User activity Activity explorer Content explorer Case notes Contributors

About this case

Case information

Status
Active

Case created on
02/10/2023, 17:37:17

User details

User's risk score
75/100

Email
#Anonymized#EAAAADdQMUWlos+z1tUWEM2vEldfSCY/q

Alerts

Policy matches

Adaptive Protection policy for Inside...

View all details

Content detected

Top labels

4 with sensitivity labels

Label	Number of activities
General\Anyone (unrestricted)	2
Personal	1
Confidential\Anyone (unrestrict...	1

Top sensitive info types

4 with sensitive info types

Sensitive info type	Number of activities
Project Jellyfish	2
All Medical Terms And Conditio...	1
Project Olivine	1

Classifiers

No Classifiers det

Top SharePoint sites

SharePoint labels

Top Recipients

Escalate for investigation

Create an eDiscovery (Premium) case for this user and notify any admins who have the eDiscovery Manager and eDiscovery Administrators roles assigned.

Name *
Jellyfish investigation 0013

Custodian
#Anonymized#EAAAAIp8dXVC9Yly8NNvAHmLCbCW4q69S0liHE3MY6XYCIhSQkEqiVVsq4yv

Source
Insider risk management

Note *
Investigate Jellyfish related activities

Save Cancel

Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Standard
Premium
User data search
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources
Customize navigation

Overview | Data sources | Collections | Review sets | Communications | Hold | Processing | Exports | Jobs | Settings

Start your case by setting up people as custodians to quickly identify and preserve data sources with which they are associated. Learn more

Add data source | Refresh | 0 items | Search | Filter | Group | Customize columns

Name	Source type	Status	Hold	Indexing job status	Index date

Tell us where to look

We'll try to ensure you can search these locations quickly. Don't forget to put them on hold to preserve their contents.

Add a custodial data source

Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Standard
Premium
User data search
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources
Customize navigation

eDiscovery (Pre

Overview

Start your case b

Add data sourc

Name

New custodian

- **Identify custodian**
- Hold settings
- Review

Select custodian

Identify new custodians from your organization's active directory

RK Roger Kroch × Please type minimum 3 characters to get the mailbox list.

Expand each custodian to view and add locations.

Custodian	Count	Clear	Edit
Roger Kroch			
Mailboxes	1/1 (Default)	Clear	Edit
OneDrives	1/1 (Default)	Clear	Edit
Exchange	1		Edit
SharePoint	33		Edit
Teams	0		Edit
Yammer	0		Edit

Next

Cancel

Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Standard
Premium
User data search
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources
Customize navigation

Overview Data sources Collections Review sets Communications Hold Processing Exports Jobs Settings

Manage and automate legal hold notifications, escalations, and reminders in one place.Learn more

New communication Download list Refresh 0 items Search Filter Group Customize columns

Name	Status	Last modified	Custodians	Hold acknowledged

Tell custodians their data is on hold

When you notify custodians, you can request them to acknowledge receipt of the notice through a portal.

New communication

New Communication

- Name Communication
- **Define Portal Content**
- Set Notifications - Required
- Set Notifications - Optional
- Custodians
- Review your settings

Define Portal Content

Define the content of your hold notice here. This content will be emailed to your custodians and also be made accessible through their personal custodian portal. After assigning custodians to this notice, you can also create and send templated emails to improve response rates and ensure that your custodians have the most up-to-date information.

Insert: Display name | Acknowledgement link | Portal link | Issuing officer email | Issuing date

electronic data and documents) be preserved, and all routine destruction or discarding of any such documents or data, whether pursuant to formal company policies or otherwise, be suspended until further notice. This includes turning off any "autodelete" functions and ensuring that back-up tapes are preserved and not overwritten or deleted. If you have a question about whether something needs to be preserved, err on the side of preserving it until advised otherwise by legal counsel.

This policy applies to all such documents whether kept at the office, at off-site storage facilities, or at your home. It includes not only formal company documents, but also materials such as handwritten notes, drafts, calendars, and the like. In addition, if anyone under your supervision has custody or control of such documents or data and it is not listed as a recipient of this memorandum, please forward it to them immediately. If you know of others who should receive this memorandum, or if you know of documents beyond our control that should be preserved, please notify {{IssuingOfficerEmail}} immediately.

Detailed instructions regarding the procedures for collection of documents will follow shortly and will be designed to minimize disruption of your daily business activities. Until such instructions are provided, all documents and files should be maintained as they are kept in the ordinary course of business.

The subpoena should not be discussed outside of any discussions necessary for document preservation and compliance, or in communications with company counsel. There should be no discussions with third parties.

We require that you acknowledge this notice by clicking the link below.

Back Next Cancel

New Communication

- Name Communication
- Define Portal Content
- **Set Notifications - Required**
- Set Notifications - Optional
- Custodians
- Review your settings

Set Notifications - Required

Issuance*

Edit

Recipient: All custodians
Cc:
Bcc:
Subject: Issuance of Hold notification
Body: TO: {{DisplayName}}
This is the issuance of the hold notification.
The hold notification is attached.
{{IssuingOfficerEmail}}

Reissue*

Edit

Recipient: All custodians
Cc:
Bcc:
Subject: Reissue of the Hold Notification
Body: {{DisplayName}}
This is the reissue of the hold notification.
The hold notification is attached.
{{IssuingOfficerEmail}}

Release*

Edit

Recipient: All custodians
Cc:
Bcc:
Subject: Release of Hold Notification
Body: {{DisplayName}}
This is the release of the hold notification.
The hold notification is attached.
{{IssuingOfficerEmail}}

Back Next Cancel

View activity

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: Show results for all activities

Users: Roger Kroch

File, folder, or site: Add all or part of a file name. folder name or URL

View all activities

Start date: Mon May 01 2023 Start time: 00:00

End date: Fri Sep 29 2023 End time: 00:00

Searching for activities that occurred over 90 days ago only returns activities from users who are assigned the appropriate licensing for long-term audit log retention. Also, results might be impacted by the retention duration of any audit log retention policies. For example, if you have a policy set up to retain activity for 6 months, and you search for activity from one year ago, you'll only see related activity from the past 6 months.

Search Clear all

Export 150 items Filter

Date	IP address	User	Activity	Item	Detail
Sep 26, 2023 8:16 AM	2603:10b6:a03:18e::30	RogerKroch@M365x98433645.onmicrosoft.com	Created mailbox item		
Sep 20, 2023 4:11 PM	2a01:110:8012:1010:3990:2b6a:d7a9:f82c	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	00000003-0000-0000-c000-000000000000	
Sep 20, 2023 4:11 PM	2a01:110:8012:1013:398d:2b6a:d7a9:f82c	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	00000002-0000-0ff1-ce00-000000000000	
Sep 20, 2023 4:11 PM	2a01:110:8012:1013:398d:2b6a:d7a9:f82c	RogerKroch@M365x98433645.onmicrosoft.com	Applied sensitivity label		
Sep 20, 2023 5:09 PM	2603:10b6:a03:48a::19	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 20, 2023 4:21 PM	2a01:110:8012:1012:398e:2b6a:d7a9:f82c	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	00000003-0000-0000-c000-000000000000	
Sep 20, 2023 4:22 PM	2a01:110:8012:1012:398e:2b6a:d7a9:f82c	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	00000003-0000-0000-c000-000000000000	

View activity

Export

150 items Filter

Date	IP address	User	Activity	Item	Detail
Oct 2, 2023 4:22 PM	2603:10b6:a03:18e::30	RogerKroch@M365x98433645.onmicrosoft.com	Created mailbox item		
Oct 3, 2023 11:03 AM	2603:10b6:a03:4ce::11	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:24 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Applied sensitivity label		
Sep 30, 2023 12:20 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Applied sensitivity label		
Sep 30, 2023 12:20 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Updated sensitivity Label		
Sep 30, 2023 12:19 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Applied sensitivity label		
Sep 30, 2023 12:16 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Applied sensitivity label		
Sep 30, 2023 12:25 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:24 PM	2603:10b6:930:51::5	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:23 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:22 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:24 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Sent message		
Sep 30, 2023 12:24 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Moved messages to Deleted Items folder		
Sep 30, 2023 12:24 PM		RogerKroch@M365x98433645.onmicrosoft.com	DlpRuleMatch	<CYYPR11MB8307EFEFDE5E50D16CA35D95D9C7A...	
Sep 30, 2023 12:24 PM		RogerKroch@M365x98433645.onmicrosoft.com	MipLabel	<CYYPR11MB8307EFEFDE5E50D16CA35D95D9C7A...	
Sep 30, 2023 12:24 PM		RogerKroch@M365x98433645.onmicrosoft.com	MipLabel	<CYYPR11MB8307EFEFDE5E50D16CA35D95D9C7A...	
Sep 30, 2023 12:19 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:23 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Created mailbox item		
Sep 30, 2023 12:20 PM		RogerKroch@M365x98433645.onmicrosoft.com	MipLabel	<CYYPR11MB8307E0B444016741C4EF75A5D9C7A...	

Export

150 items Filter

Date	IP address	User	Activity	Item	Detail
Sep 30, 2023 12:19 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Created mailbox item		
Sep 30, 2023 12:20 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Sent message		
Sep 30, 2023 12:18 PM	2603:10b6:930:51::5	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:18 PM		RogerKroch@M365x98433645.onmicrosoft.com	DlpRuleMatch	<CYYPR11MB83076A7A37D9ADDEFABB2910D9C7A...	
Sep 30, 2023 12:18 PM		RogerKroch@M365x98433645.onmicrosoft.com	MipLabel	<CYYPR11MB83076A7A37D9ADDEFABB2910D9C7A...	
Sep 30, 2023 12:18 PM		RogerKroch@M365x98433645.onmicrosoft.com	MipLabel	<CYYPR11MB83076A7A37D9ADDEFABB2910D9C7A...	
Sep 30, 2023 12:18 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:18 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	Sent message		
Oct 1, 2023 8:21 AM	2603:10b6:a03:531::11	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:20 PM	52.108.80.19	rogerkroch@m365x98433645.onmicrosoft.com	Accessed file	Regulatory Requirements Review.pptx	Accessed from "Documents/Project Je...
Oct 1, 2023 8:21 AM	2603:10b6:a03:531::11	RogerKroch@M365x98433645.onmicrosoft.com	Accessed mailbox items		Mail Items Accessed
Sep 30, 2023 12:25 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	00000003-0000-0000-c000-000000000000	
Sep 30, 2023 12:11 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	00000003-0000-0000-c000-000000000000	
Sep 30, 2023 12:11 PM	2a02:a420:18:f700:c4a2:66b3:7ff2:1f03	RogerKroch@M365x98433645.onmicrosoft.com	User logged in	4765445b-32c6-49b0-83e6-1d93765276ca	
Sep 30, 2023 9:14 AM	77.160.101.91	RogerKroch@M365x98433645.onmicrosoft.com	SensitivityLabelPolicyMatched	https://m365x98433645-my.sharepoint.com/person...	
Sep 30, 2023 9:13 AM	77.160.101.91	RogerKroch@M365x98433645.onmicrosoft.com	SensitivityLabeledFileOpened	C:\Users\Roger Koch\AppData\Local\Microsoft\Win...	
Sep 30, 2023 9:13 AM	77.160.101.91	RogerKroch@M365x98433645.onmicrosoft.com	SensitivityLabeledFileRenamed	C:\Users\Roger Koch\AppData\Local\Microsoft\Win...	
Sep 30, 2023 9:12 AM	77.160.101.91	rogerkroch@m365x98433645.onmicrosoft.com	Accessed file	Analyst Research.docx	Accessed from "Documents/Project Je...
Sep 30, 2023 9:09 AM	77.160.101.91	rogerkroch@m365x98433645.onmicrosoft.com	Downloaded files to computer	Seabed Jellyfish_v2.docx	
Sep 30, 2023 8:53 AM		ROGERKROCH@M365X98433645.ONMICROSOFT.COM	DLPRuleMatch	402870e6-3921-4ce6-99aa-9c3ec27541a9	
Sep 30, 2023 8:50 AM	77.160.101.91	rogerkroch@m365x98433645.onmicrosoft.com	Uploaded file	Seabed Jellyfish_v2.docx	Uploaded to "Documents/Project Jelly...
Sep 30, 2023 8:49 AM	77.160.101.91	rogerkroch@m365x98433645.onmicrosoft.com	Accessed file	Analyst Research.docx	Accessed from "Documents/Project Je...

Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Standard
Premium
User data search
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources
Customize navigation

Overview Data sources Collections Review sets Communications Hold Processing Exports Jobs Settings

New collection Refresh 0 items Search Filter Group Customize columns

Name	Review set	Status	Query text	Last run time	Estimate status	Preview status

Start searching for relevant data

Prepare and run your query to find the items you want to collect.

New collection

New collection

- Name and description
- Custodial data sources
- Non-custodial data sources
- Additional locations
- **Search query**
- Review your collection

Define your search query

Use the query builder or editor to define your search. Learn more about queries

Query language-country/region: None

Use new query builder

Query builder

KQL editor

Filters Clear all

AND

Size (in bytes) | Greater than | 1

Add filter Add subgroup

Back Next Save and close Cancel

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Standard
Premium
User data search
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

eDiscovery (Premium) > Cases > Jellyfish investigation 0013

Overview Data sources Collections Review sets Communications H

New collection Refresh

Name	Review set	Status
Search for Jellyfish specific demo	Jellyfish demo review set	Committ
Search for Jellyfish demo		Estimate

Search for Jellyfish specific demo

Committed

Updated 02/10/2023, 17:56:01

Review search statistics and samples to determine if you want to rerun, edit, review, or export the collection.

Summary | Data sources | Search statistics | Collection options

Collection overview

Understand how the items were found, retrieved, and processed as part of this collection.

Locations with hits

We **searched 181 locations,** and found **36 locations with hits.**

36 mailboxes and 0 sites had search hits.

97 locations failed to be searched during estimate.

To learn more, view failed locations report

Pre-collection estimates

1.835 items (~129.07 MB) had search hits.

2 items were partially indexed and weren't fully searched. You can add these items to a review set for inspection.
Learn more about partial indexing.

View samples

Collected items

1.814 items (~129.46 MB) were retrieved from the locations with hits.

Some additions and consolidations occurred during collection. See table below for details.

Item type	Item count	Description
Items with hits	**1.841**	Estimated number of items found by search
Partially indexed items	0	Partially indexed items included in the scope of your collection
Review set duplicates	0	Items that are already in the same review set are not collected.
Search duplicates	0	Duplicate instances of the same items are not collected.

Copy collection | Actions | Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Standard
Premium
User data search
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

eDiscovery (Premium) > Cases > Jellyfish investigation 0013

Overview Data sources Collections Review sets Communications H

New collection Refresh

Name	Review set	Status
Search for Jellyfish specific demo	Jellyfish demo review set	Committ
Search for Jellyfish demo		Estimate

Search for Jellyfish specific demo

Committed

Updated 02/10/2023, 17:56:01

Review search statistics and samples to determine if you want to rerun, edit, review, or export the collection.

Summary Data sources Search statistics Collection options

Collection estimates

Estimated items by location

1.835 items

Estimated items by location

Exchange (1.835)

Estimated locations with hits

20 location(s)

Estimated locations with hits

Exchange (20)

Data volume by location (MB)

129 MB

Data volume by location

Exchange (129 MB)

Condition report

Download your search condition report.

Location type	Part	Condition	Locations with hits	Items	Size (MB)
Exchange	Primary	((size>1))	48	1835	129.07
Exchange	Unindexed	IndexingErrorCode<...	46	2	0.12

Top locations

Download your top locations report.

Copy collection Actions Close

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings
More resources

Saved filter queries | Save | Clear all

Filters | Undo filter query | Redo filter query

AND

Sender | Equals any of | roger kroch, roger kroch ...

Add filter | Add subgroup

269 items

#	Subject/Title	Status	Tag Status	Date (UTC-07:00)	Sender/Author	File class
1	Hey	Ready	No Tag	Sep 20, 2023 7:29:3...	Roger Kroch <Rog...	Email
2	Suppliers	Ready	No Tag	Sep 29, 2023 7:48:5...	Roger Kroch	Email
3	Jellyfish Electrical c...	Ready	No Tag	Sep 20, 2023 6:35:3...	Roger Kroch <Rog...	Email
4	Jellyfish bugs	Ready	No Tag	Sep 20, 2023 6:50:0...	Roger Kroch <Rog...	Email
5	Day After Thanksgi...	Ready	No Tag	Aug 28, 2023 6:09:...	Roger Kroch <Rog...	Email
6	Administrative Prof...	Ready	No Tag	Aug 28, 2023 6:09:...	Roger Kroch <Rog...	Email
7	Collaboration partn...	Ready	No Tag	Sep 28, 2023 4:13:3...	Roger Kroch <Rog...	Email
8	Labor Day	Ready	No Tag	Aug 28, 2023 6:09:...	Roger Kroch <Rog...	Email
9	Columbus Day	Ready	No Tag	Aug 28, 2023 6:09:...	Roger Kroch <Rog...	Email
10	More...	Ready	No Tag	Sep 30, 2023 12:17:...	Roger Kroch <Rog...	Email
11	Labor Day	Ready	No Tag	Aug 28, 2023 6:09:...	Roger Kroch <Rog...	Email
12	Check this	Ready	No Tag	Sep 29, 2023 6:27:2...	Roger Kroch <Rog...	Email
13	Jellyfish project me...	Ready	No Tag	Sep 20, 2023 6:39:0...	Roger Kroch <Rog...	Email

Viewing: Page 1 of 6 | 50 items/page

More...

Source | Plain text | Annotate | Metadata

Show pinned metadata

From: Roger Kroch <RogerKroch@M365x98433645.onmicrosoft.com>
Sent on: Saturday, September 30, 2023 7:17:58 AM
To: ajaganjac@microsoft.com
Subject: More...
Attachments: Architecture design.docx (12.22 KB), Analyst Research.docx (34.19 KB)

Hi Anela,

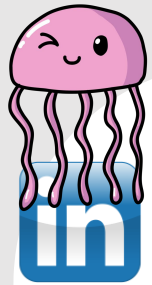
Here we go 😃!

RK

Tag | Group by families (3) | Group by conversations (3)

Microsoft Security

Thank you



Anela Jaganjac
Ellen van Meurs