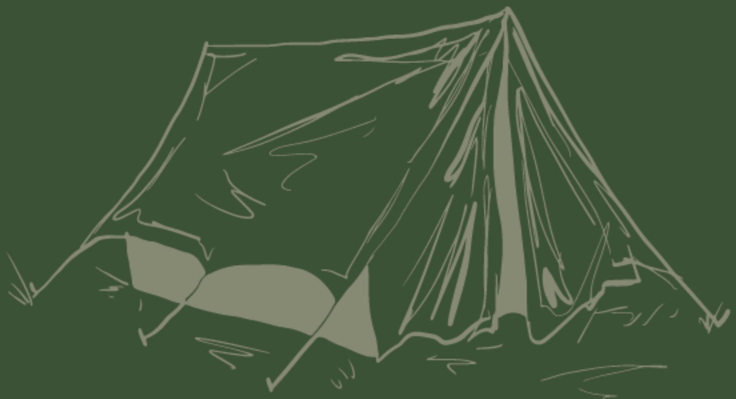


SECURE THE DIB

Summer Camp

AGENDA

- Opening Remarks | 10:00 AM CT
  Sam Stiles

- Session 1 | 10:15 AM CT
  Scout Leader Wisdom:
  CEO's Perspective on CMMC Costs
  Scott Edwards

- Session 2 | 11:30 AM CT
  Safeguard the Camp:
  Protecting CUI in GCCH and Azure Gov
  Sam Stiles & Shawn Hays

- Session 3 | 12:45 PM CT
  Trailblazing CMMC:
  Finding a Path with Guardian MSP & Vigilance MSSP
  Brad Shannon & Jana Abbott

- Session 4 | 2:00 PM CT
  An IT Director's
  Thru-Hike on the CMMC Trail
  Christopher Huys & Daniel Akridge

SECURE THE DIB
Summer Camp

Safeguard the Camp:
PROTECTING CUI IN GCCH & AZURE GOV

Shawn Hays (Microsoft) & Sam Stiles (Summit 7)

Shawn Hays

SR PRODUCT MARKETING MANAGER

Microsoft

Sam Stiles

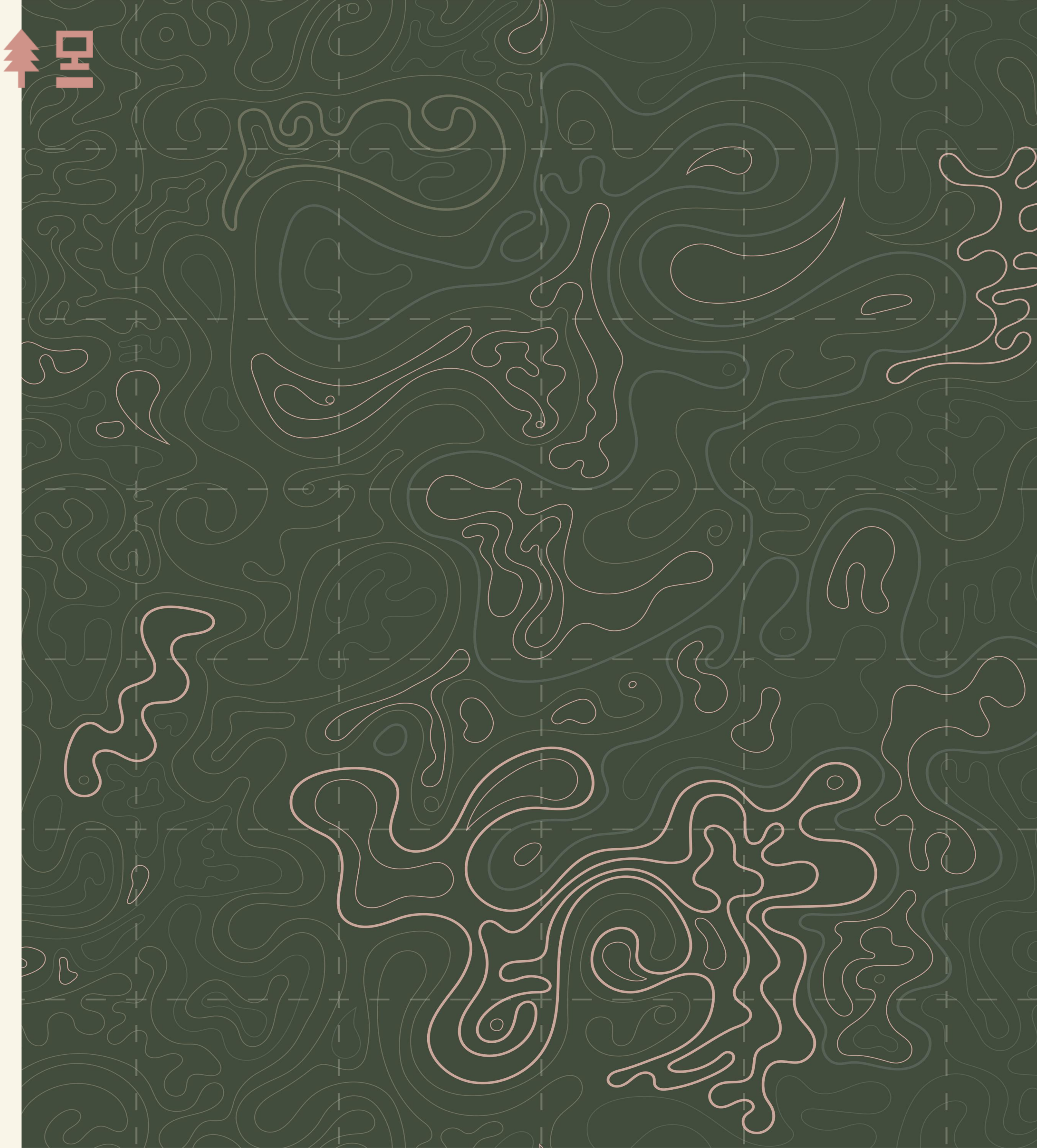
VICE PRESIDENT OF MARKETING

SUMMIT7

AGENDA

The Cooey Camp Adventure List

1. Preventing CUI Leaks In Your Tent
2. Microsoft 365 Gov Clouds Explained
3. Microsoft's End-to-End Security for CMMC
4. Deep Dive on Protecting CUI with Microsoft Purview and Demo
5. Advancing Your CMMC Solutions

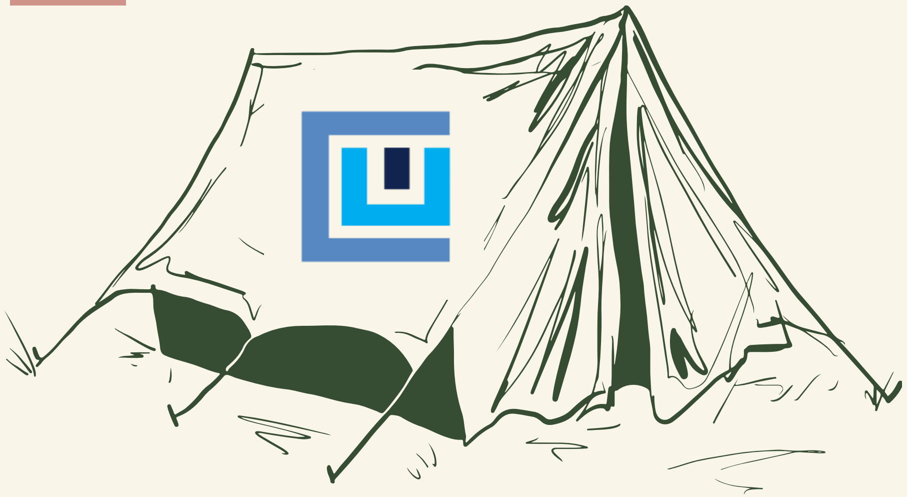


How to Prevent Data Leaks In Your Tent

CUI Spillage!?

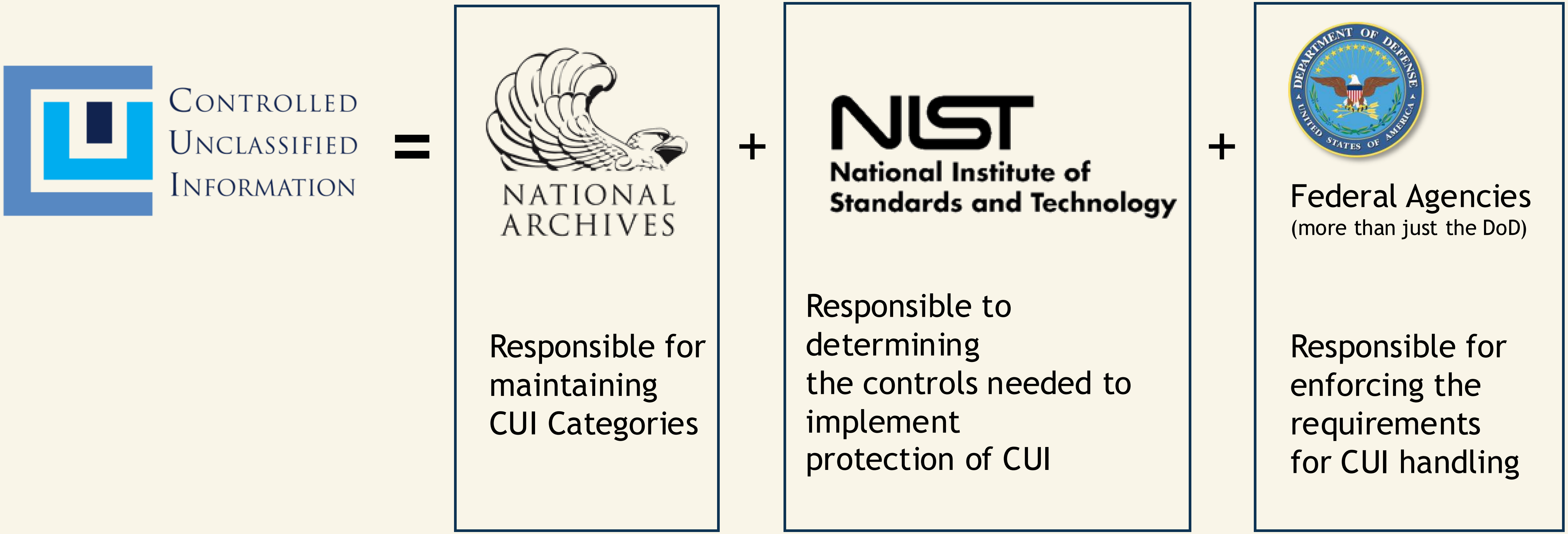
What is CUI?

CONTROLLED UNCLASSIFIED INFORMATION



Controlled Unclassified Information is government *created or owned* information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies.

Who Is In Charge?



CONTROLLED UNCLASSIFIED INFORMATION =

NATIONAL ARCHIVES

Responsible for maintaining CUI Categories

+

NIST

National Institute of Standards and Technology

Responsible to determining the controls needed to implement protection of CUI

+

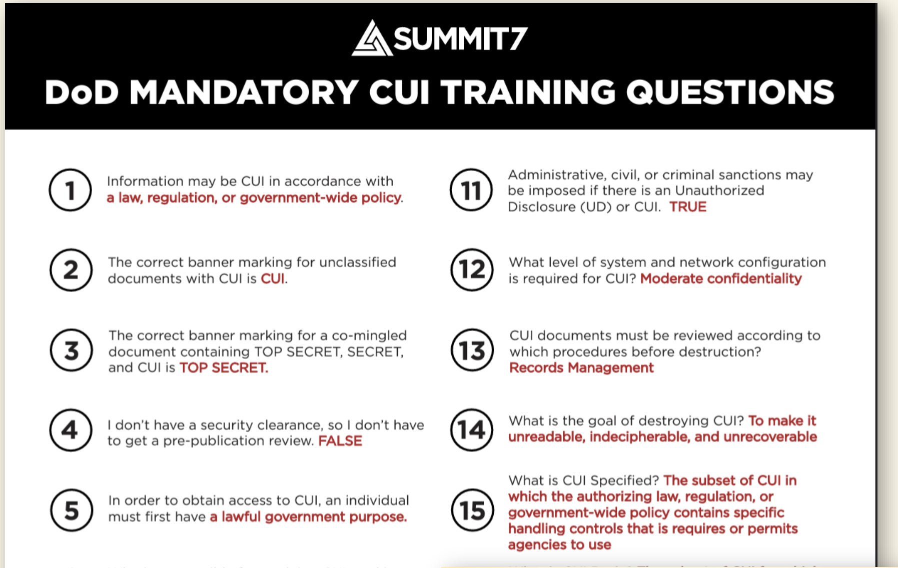
Federal Agencies

(more than just the DoD)

Responsible for enforcing the requirements for CUI handling

Resources

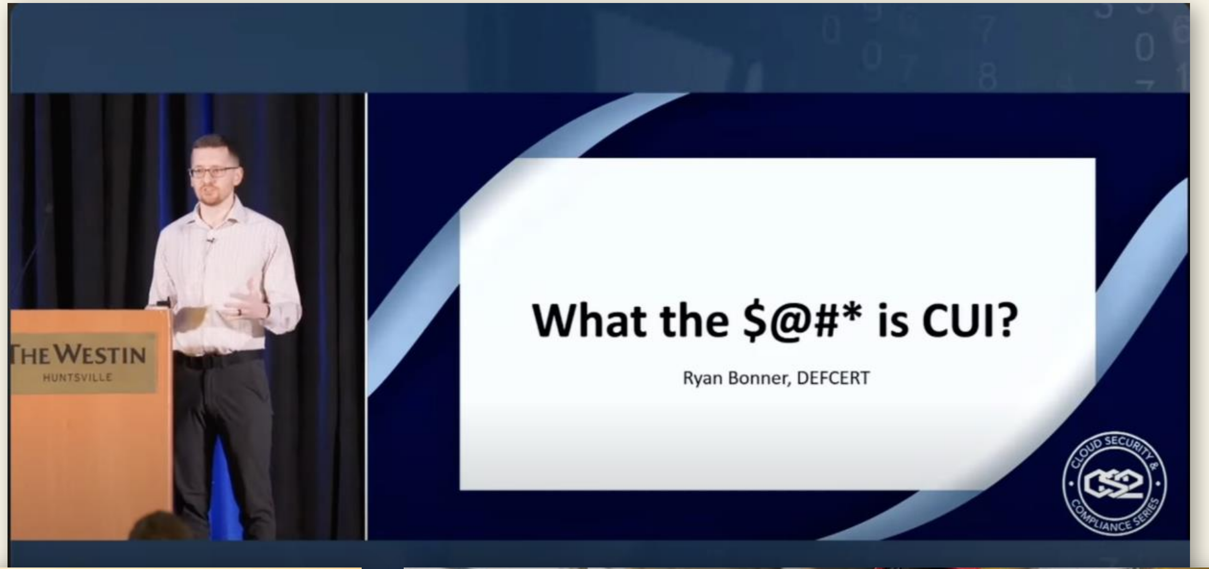
PROTECTING CUI & SENSITIVE DATA IN THE DIB



SUMMIT7

DoD MANDATORY CUI TRAINING QUESTIONS

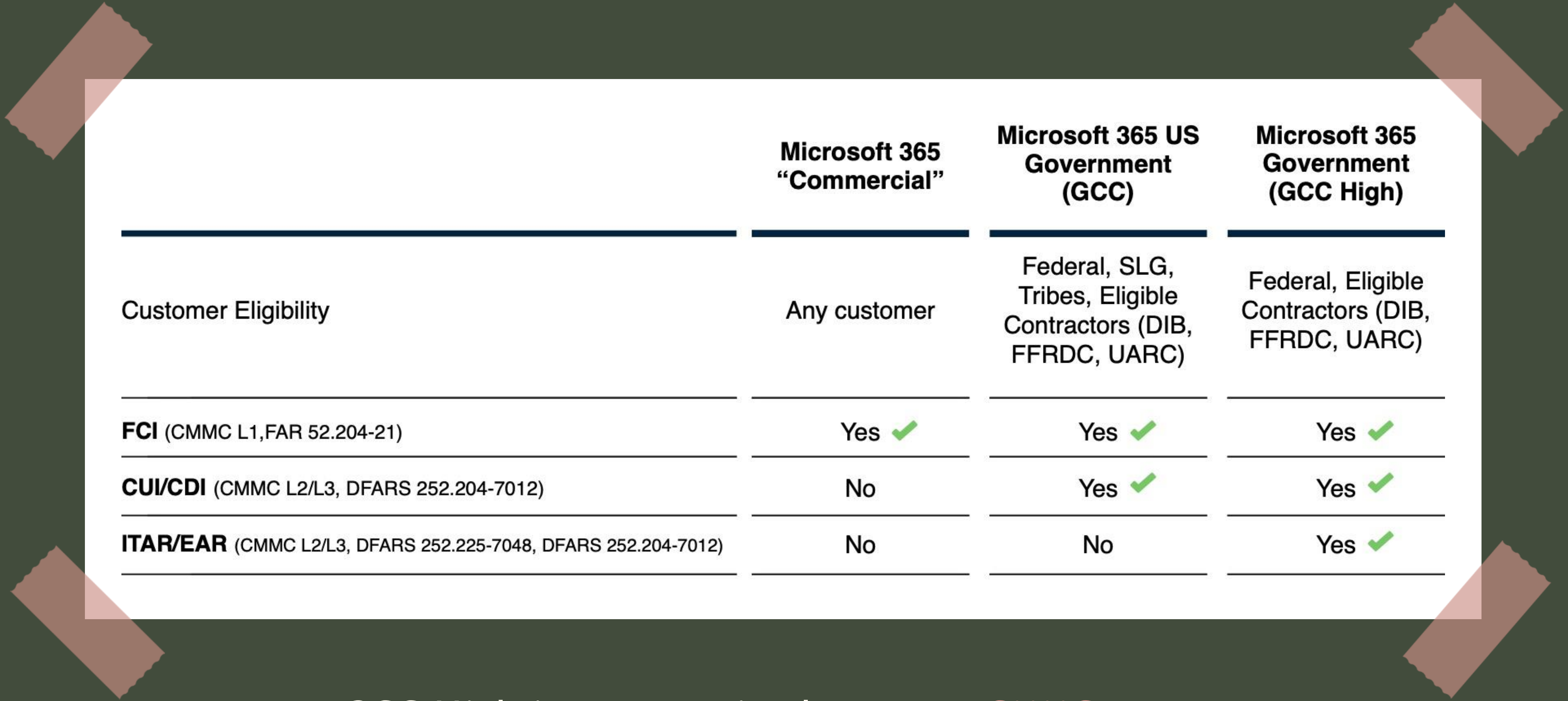
1. Information may be CUI in accordance with a law, regulation, or government-wide policy.
2. The correct banner marking for unclassified documents with CUI is CUI.
3. The correct banner marking for a co-mingled document containing TOP SECRET, SECRET, and CUI is TOP SECRET.
4. I don't have a security clearance, so I don't have to get a pre-publication review. FALSE
5. In order to obtain access to CUI, an individual must first have a lawful government purpose.
6. Who is responsible for applying CUI markings and dissemination instructions? Authorized holder of the information at the time of creation
7. At the time of creation of CUI material, the authorized holder is responsible for determining: CUI category, CUI markings, and dissemination instructions
8. What is the purpose of the ISOO CUI Registry? A government-wide online repository for Federal-level guidance regarding CUI policy and practice
9. It is mandatory to include a banner marking at the top of the page to alert the user that CUI is present. TRUE
10. What is Controlled Unclassified Information (CUI)? Unclassified information requiring safeguarding and dissemination controls, pursuant to and consistent with applicable laws, regulations, and government-wide policies
11. Administrative, civil, or criminal sanctions may be imposed if there is an Unauthorized Disclosure (UD) or CUI. TRUE
12. What level of system and network configuration is required for CUI? Moderate confidentiality
13. CUI documents must be reviewed according to which procedures before destruction? Records Management
14. What is the goal of destroying CUI? To make it unreadable, indecipherable, and unrecoverable
15. What is CUI Specified? The subset of CUI in which the authorizing law, regulation, or government-wide policy contains specific handling controls that is requires or permits agencies to use



What the $@#* is CUI?

Ryan Bonner, DEFCERT

Microsoft Government Clouds Explained

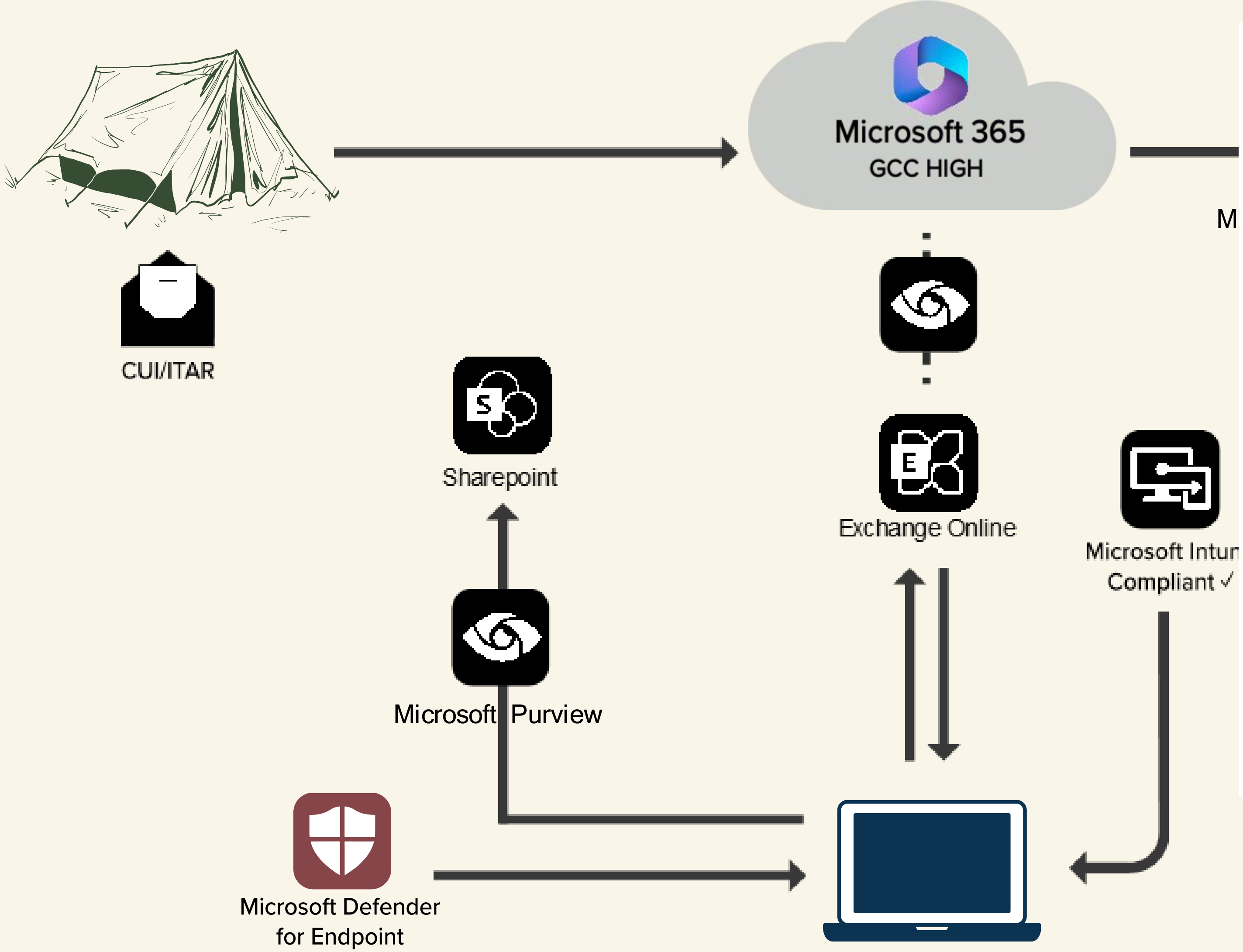


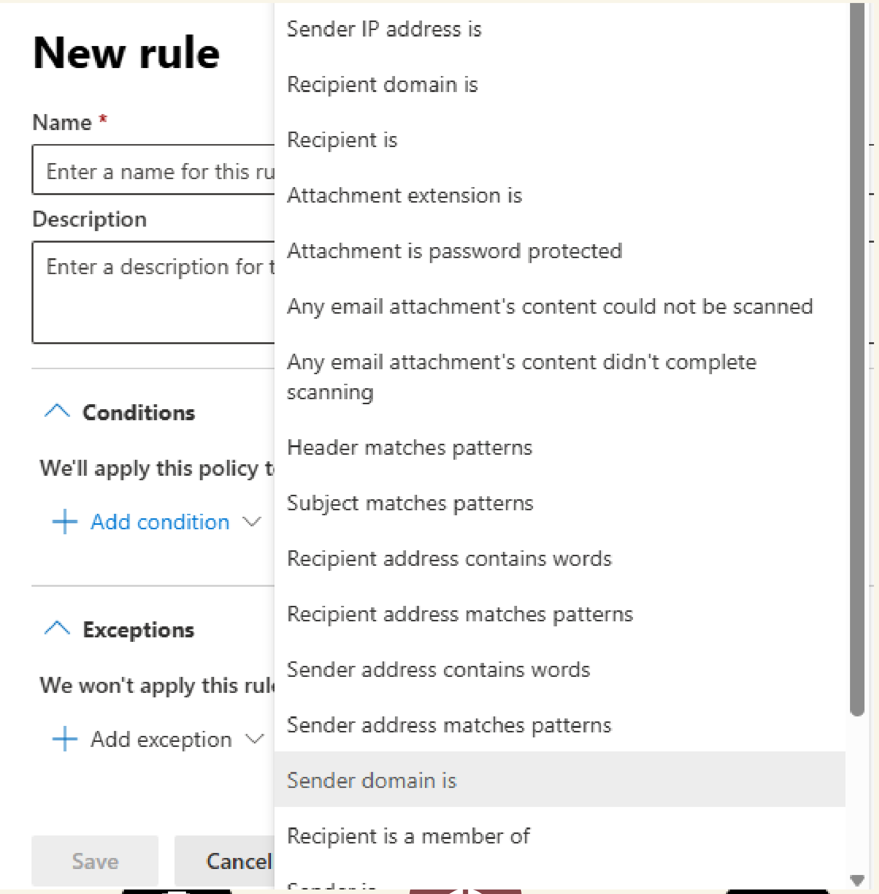
	Microsoft 365 "Commercial"	Microsoft 365 US Government (GCC)	Microsoft 365 Government (GCC High)
Customer Eligibility	Any customer	Federal, SLG, Tribes, Eligible Contractors (DIB, FFRDC, UARC)	Federal, Eligible Contractors (DIB, FFRDC, UARC)
FCI (CMMC L1,FAR 52.204-21)	Yes ✓	Yes ✓	Yes ✓
CUI/CDI (CMMC L2/L3, DFARS 252.204-7012)	No	Yes ✓	Yes ✓
ITAR/EAR (CMMC L2/L3, DFARS 252.225-7048, DFARS 252.204-7012)	No	No	Yes ✓

GCC High is not required to meet CMMC at any Level. However, Microsoft's official recommendation is for organizations planning or required to meet CMMC Level 2 and Level 3 should deploy to Microsoft 365 GCC High.

Su

CUI Flow with M365 GCC High





New rule

Name *

Enter a name for this ru

Description

Enter a description for t

Conditions

We'll apply this policy t

+ Add condition

Exceptions

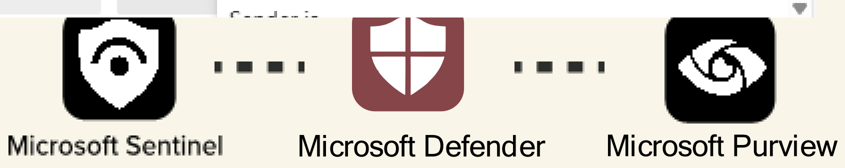
We won't apply this rul

+ Add exception

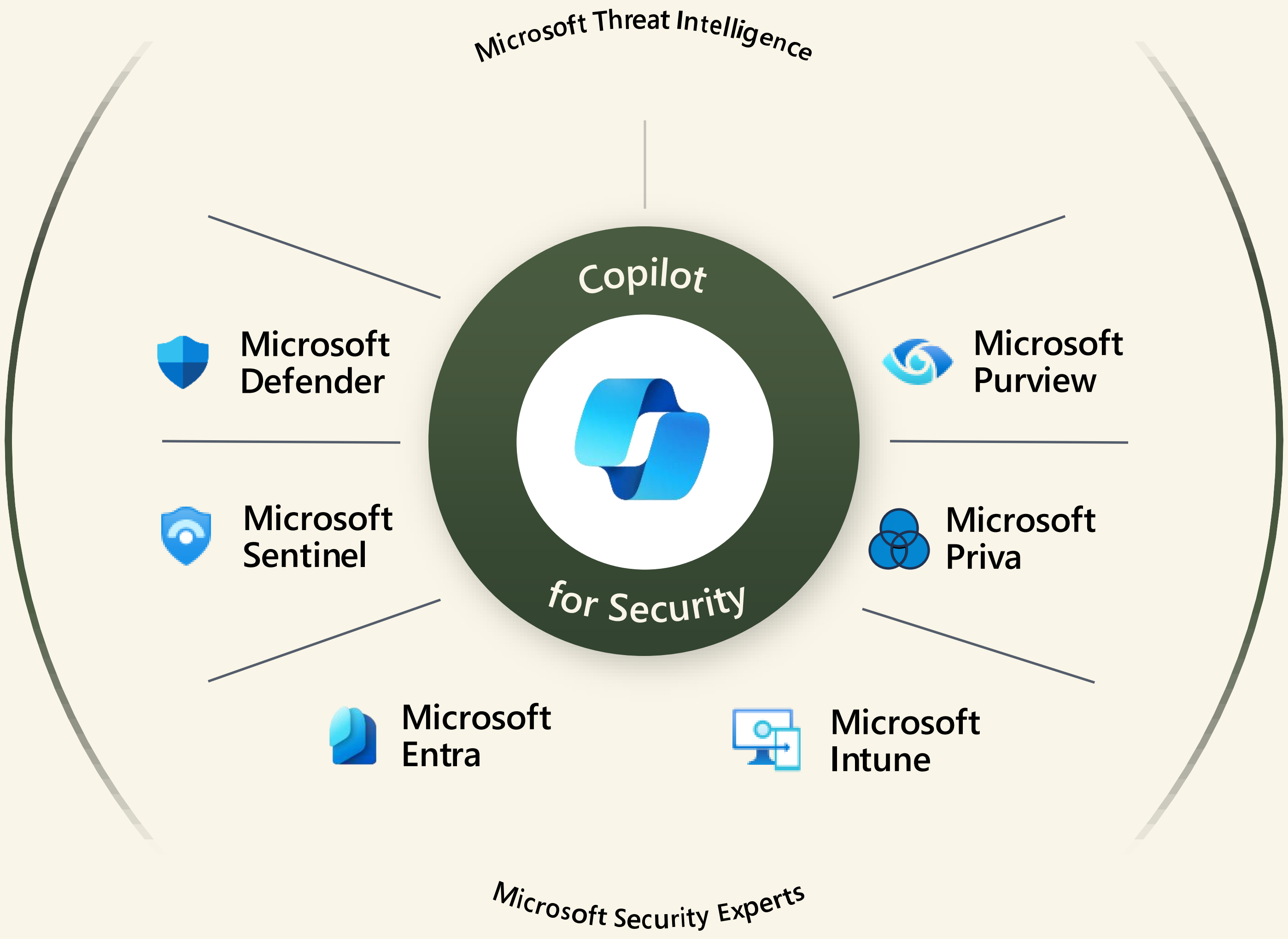
Save

Cancel

- Sender IP address is
- Recipient domain is
- Recipient is
- Attachment extension is
- Attachment is password protected
- Any email attachment's content could not be scanned
- Any email attachment's content didn't complete scanning
- Header matches patterns
- Subject matches patterns
- Recipient address contains words
- Recipient address matches patterns
- Sender address contains words
- Sender address matches patterns
- Sender domain is
- Recipient is a member of



Microsoft’s End-to-End Security for CMMC



Microsoft Threat Intelligence

Copilot for Security

Microsoft Defender

Microsoft Sentinel

Microsoft Entra

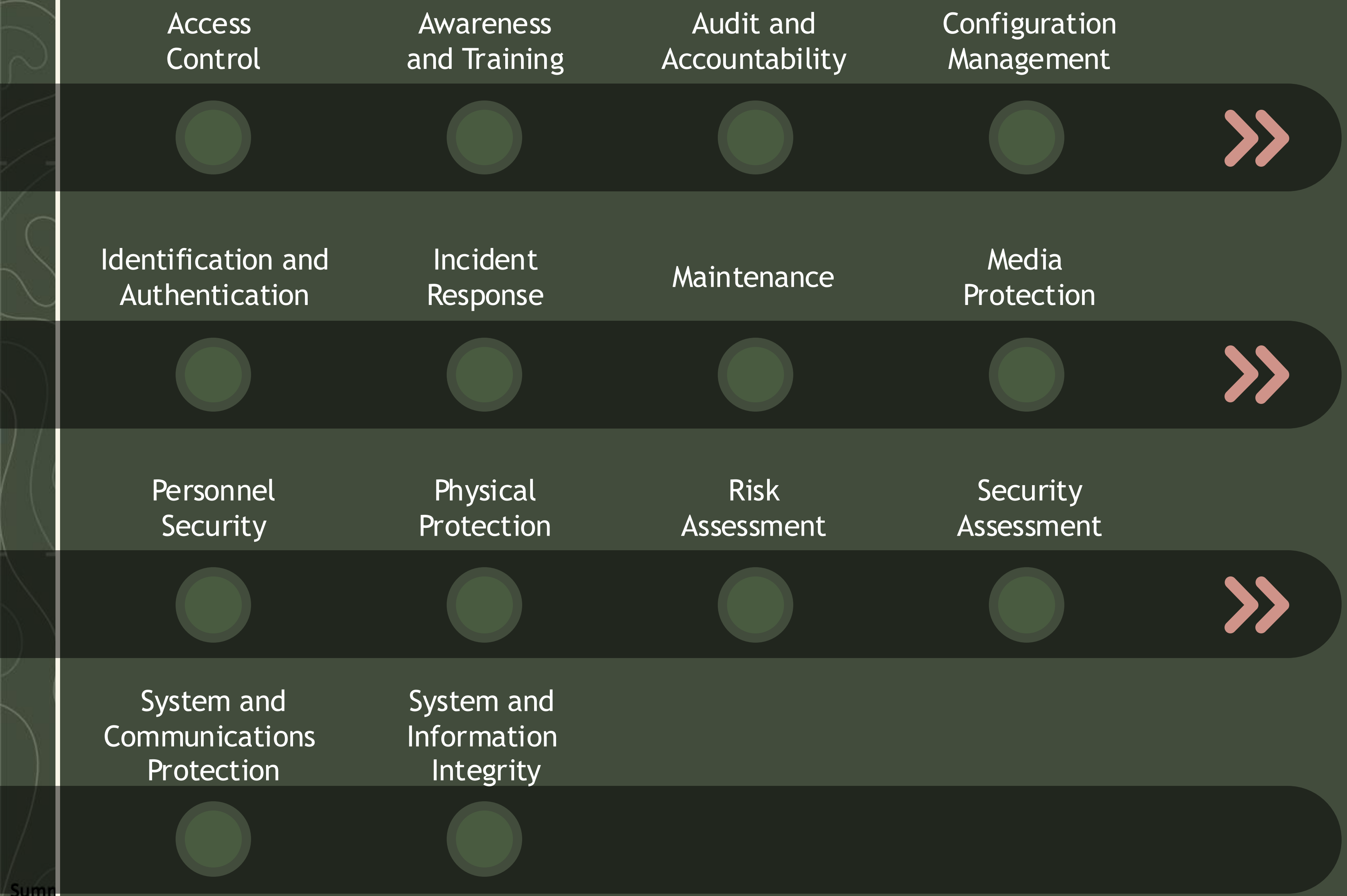
Microsoft Purview

Microsoft Priva

Microsoft Intune

Microsoft Security Experts

NIST 800-171r2 → CMMC Level 2



Access Control

Awareness and Training

Audit and Accountability

Configuration Management

Identification and Authentication

Incident Response

Maintenance

Media Protection

Personnel Security

Physical Protection

Risk Assessment

Security Assessment

System and Communications Protection

System and Information Integrity

Notes

NIST 800-171r3 is the latest release; however, CMMC assessment requirements will be based upon Revision 2 until further notice.

Sumr

Data Security is critical for strong cybersecurity and CMMC

Data security incidents are widespread	83%	of organizations, including those in the DIB, experience more than one data breach in their lifetime[1]
Insiders account for 20% of data breaches, adding to costs	$15.4M	Total average cost of activities to resolve insider threats over 12-month period[2]
Complexity continues to increase	90%+	of organizations are adopting multiple cloud infrastructures, platforms, and services to run their businesses[3]

Source:
[1,23] Microsoft Data Security Index report

But securing CUI is complex and multi-faceted

⚠ Different types of data, users, and objectives

⚠ New applications + AI future brings new data risk

⚠ NIST 800-171 and threats continue to evolve

And it’s challenging to work with disparate solutions

10+

organizations use an average of 10 solutions to secure their data estate

Exposed infrastructure gaps that are costly and complex to manage

Source: Microsoft Data Security Index report

Fragmented solutions lead to

- Unnecessary data transfers
- Duplicate copies of data
- Inconsistent data classification
- Redundant alerts
- Siloed investigations
- Exposure gaps

»

- Increased CMMC implementation complexity
- Longer deployment times
- Greater management burden
- Higher costs
- Greater risk management with vendors

Microsoft Purview

A comprehensive approach to secure CUI

Microsoft Purview

Integrated solutions to secure & govern your CUI data estate

DATA SECURITY	DATA GOVERNANCE	DATA COMPLIANCE
Secure CUI across its lifecycle, wherever it lives	Responsibly unlock value creation from data	Manage critical risks and regulatory requirements
Data Loss Prevention Insider Risk Management Information Protection	Data Discovery Data Quality Data Curation Data Estate Insights	Compliance Manager eDiscovery and Audit Communication Compliance Data Lifecycle Management Records Management

Unstructured & Structured data

Traditional and AI generated data

Microsoft 365 and Multi-cloud

Shared platform capabilities

Data Map, Data Classification, Data Labels, Audit, Data Connectors

Microsoft Purview

Integrated solutions to secure & govern your entire data estate

DATA SECURITY

Secure CUI across its lifecycle, wherever it lives

Data Loss Prevention
Insider Risk Management
Information Protection

DATA GOVERNANCE

Responsibly unlock value creation from data

Data Discovery
Data Quality
Data Curation
Data Estate Insights

DATA COMPLIANCE

Manage critical risks and regulatory requirements

Compliance Manager
eDiscovery and Audit
Communication Compliance
Data Lifecycle Management
Records Management

Unstructured & Structured data | Traditional and AI generated data | Microsoft 365 and Multi-cloud

Shared platform capabilities

Data Map, Data Classification, Data Labels, Audit, Data Connectors

CUI security incidents can happen anytime, anywhere

NIST 800-171r2: 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

External risks

User falls prey to phishing attack, compromises user credentials

CUI compromise by external threat

Internal risks

User copies file to a USB, then uploads to a personal Dropbox to take to a competitor

CUI theft by malicious insider

User negligently shares CUI in generative AI apps

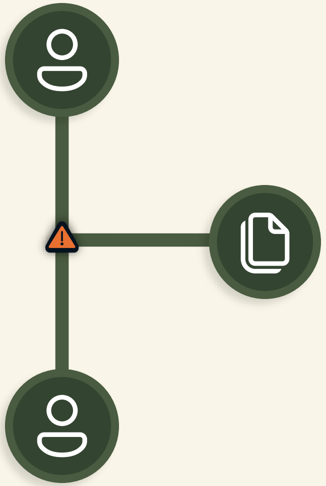
CUI leak by negligent insider

User deletes CUI before leaving the organization

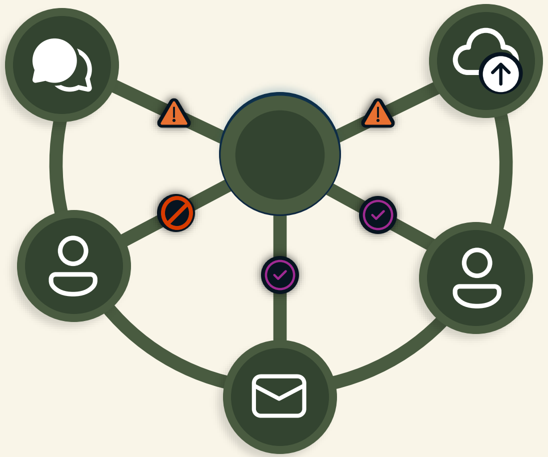
CUI sabotage by disgruntled insider

To secure CUI, organizations need to…

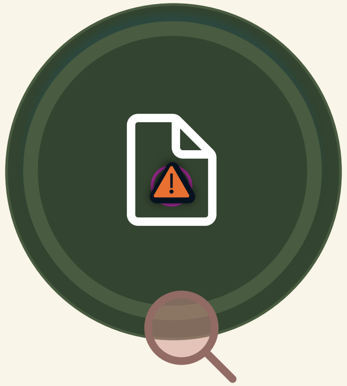
Discover hidden risks to CUI wherever it lives or travels



Protect and prevent data loss across your estate



Quickly investigate and respond to CUI security incidents



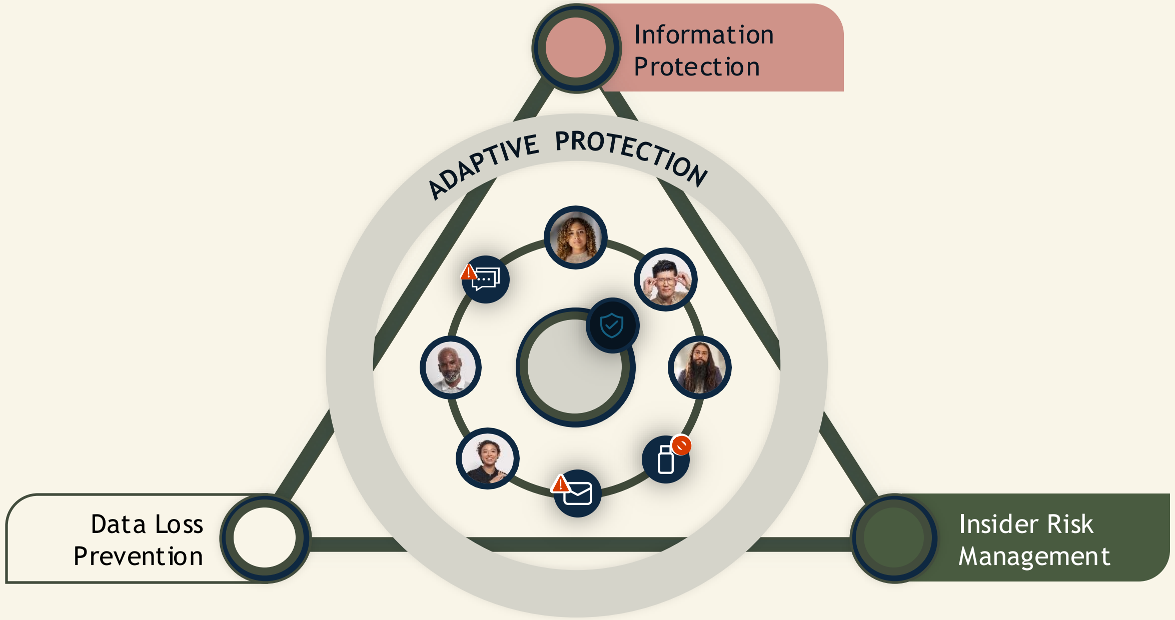
3.1.3 Control the flow of CUI in accordance with approved authorizations.

Fortify CUI security with an integrated approach

Automatically **discover, classify and label sensitive** data, and **prevent its unauthorized use** across apps, services, and devices.

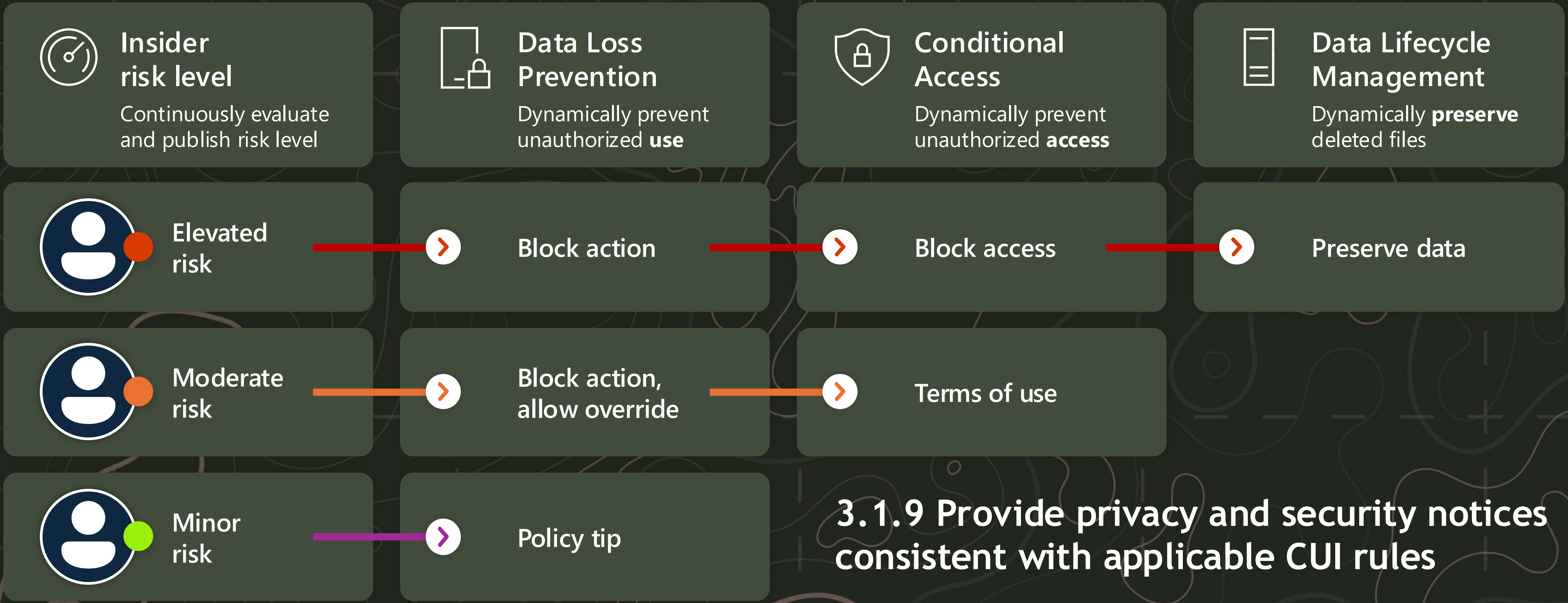
Understand the **user intent and context around the use of sensitive data** to identify the most critical risks

Enable **Adaptive Protection** to assign high-risk users to appropriate DLP, Data Lifecycle Management, and Entra Conditional Access policies



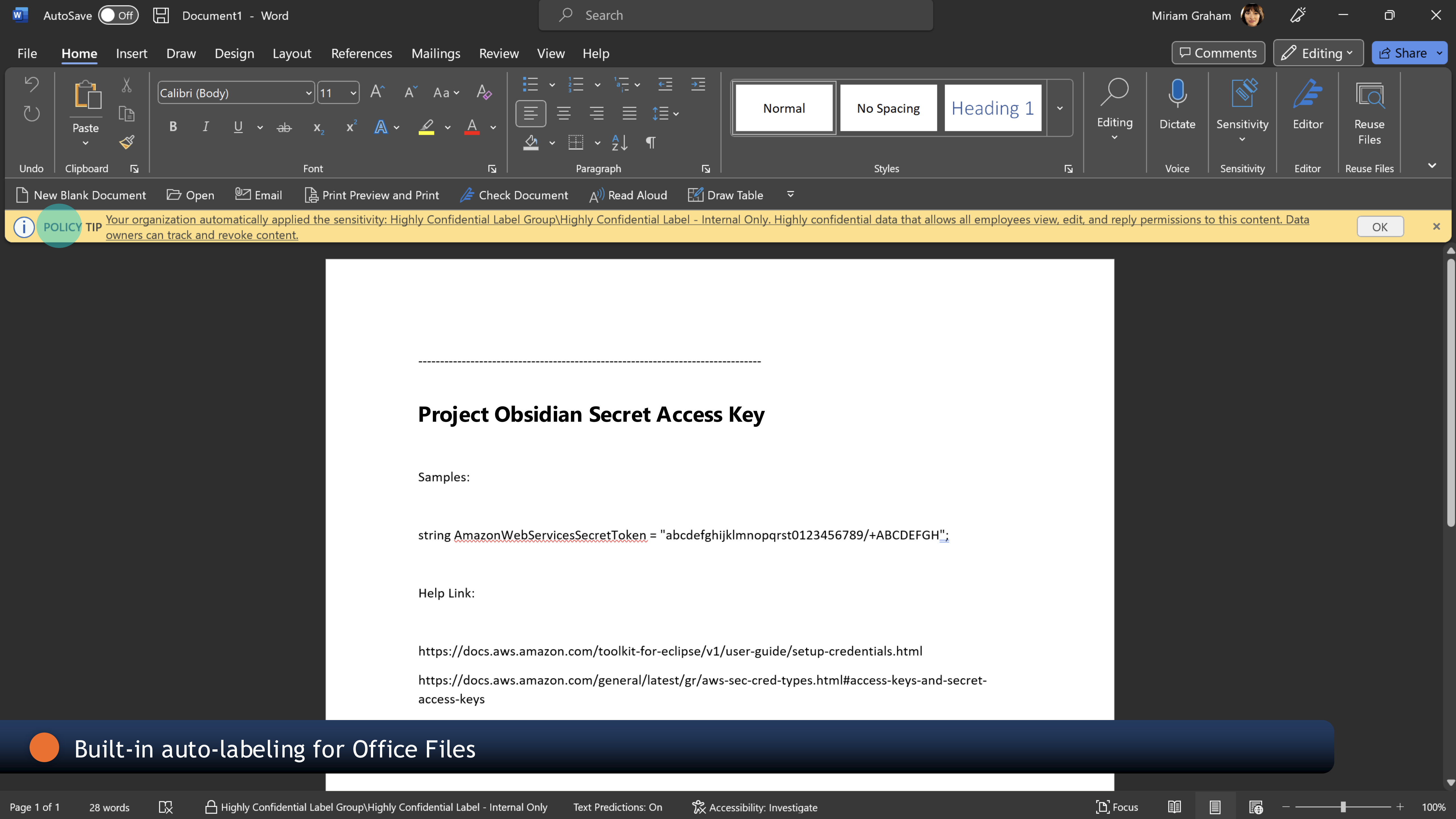
Support for all data – hybrid, Cloud, SaaS, and devices | Partner ecosystem

Adaptive Protection in Microsoft Purview



Insider risk level Continuously evaluate and publish risk level	Data Loss Prevention Dynamically prevent unauthorized **use**	Conditional Access Dynamically prevent unauthorized **access**	Data Lifecycle Management Dynamically **preserve** deleted files
Elevated risk	Block action	Block access	Preserve data
Moderate risk	Block action, allow override	Terms of use	
Minor risk	Policy tip		

3.1.9 Provide privacy and security notices consistent with applicable CUI rules



POLICY TIP Your organization automatically applied the sensitivity: Highly Confidential Label Group\Highly Confidential Label - Internal Only. Highly confidential data that allows all employees view, edit, and reply permissions to this content. Data owners can track and revoke content.

Project Obsidian Secret Access Key

Samples:

string AmazonWebServicesSecretToken = "abcdefghijklmnopqrst0123456789/+ABCDEFGH";

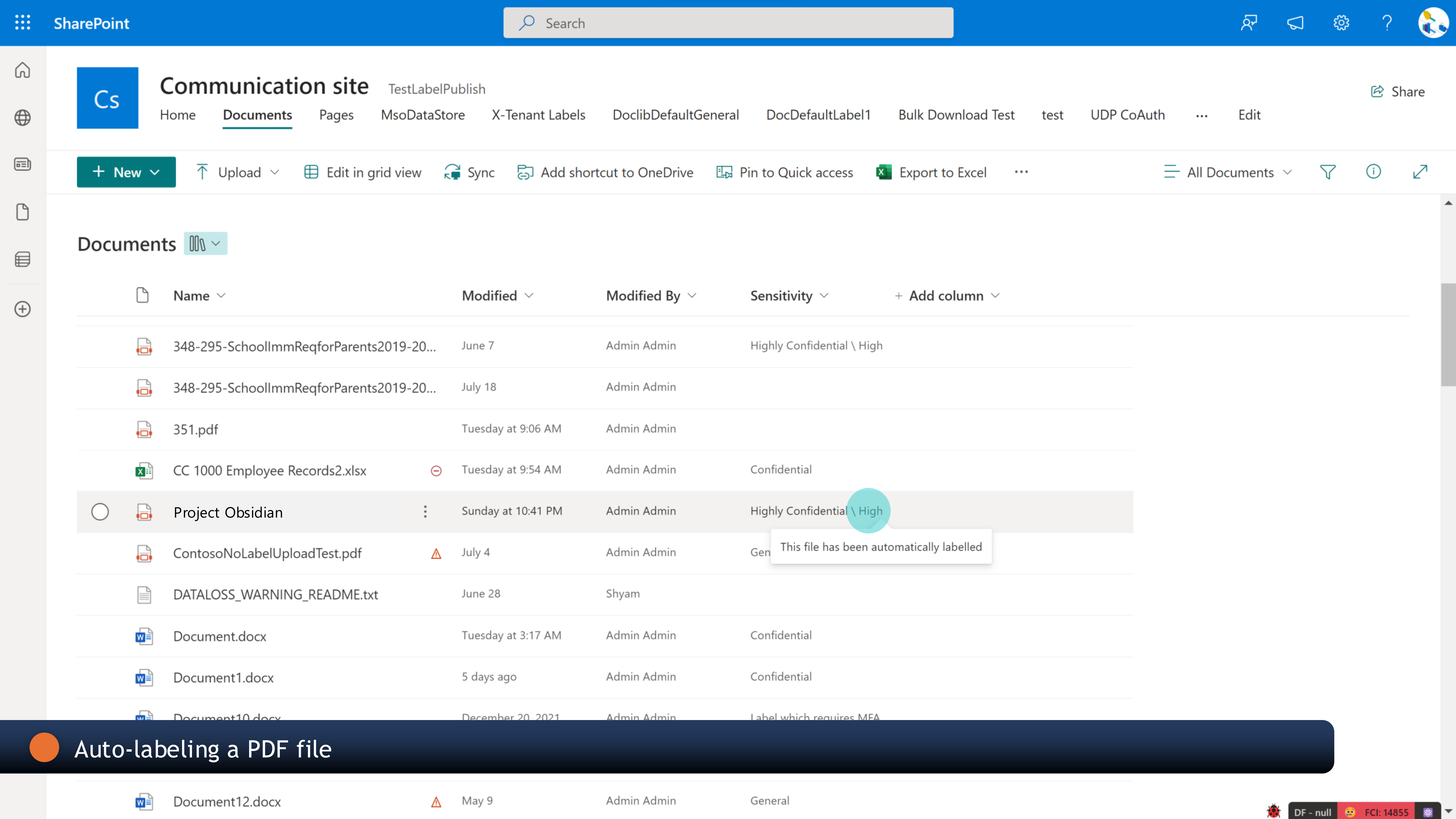
Help Link:

https://docs.aws.amazon.com/toolkit-for-eclipse/v1/user-guide/setup-credentials.html

https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys

Built-in auto-labeling for Office Files

Page 1 of 1
28 words
Highly Confidential Label Group\Highly Confidential Label - Internal Only
Text Predictions: On
Accessibility: Investigate
Focus
100%

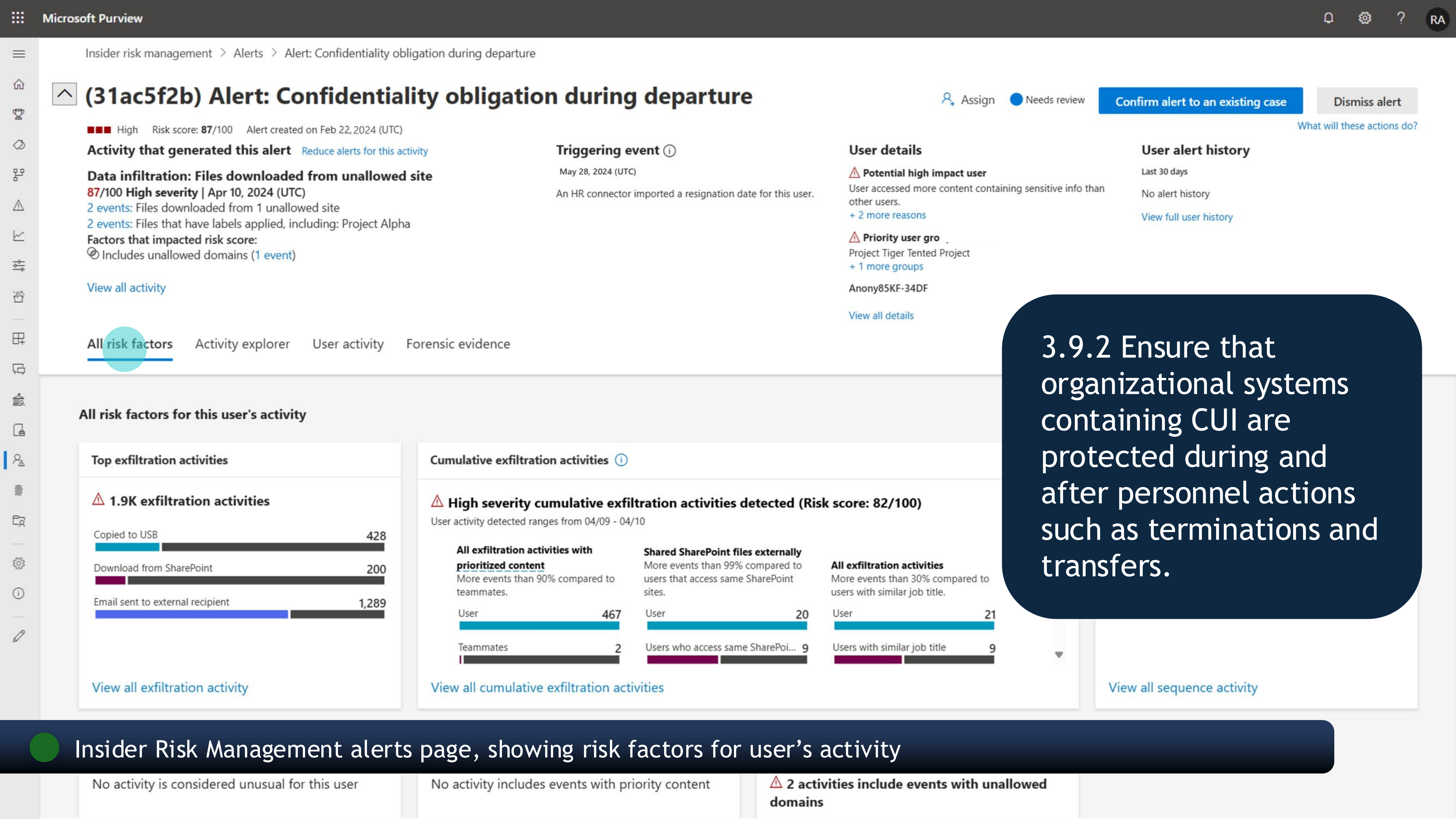


Documents

Name	Modified	Modified By	Sensitivity	Add column
348-295-SchoolImmReqforParents2019-20...	June 7	Admin Admin	Highly Confidential \ High	
348-295-SchoolImmReqforParents2019-20...	July 18	Admin Admin		
351.pdf	Tuesday at 9:06 AM	Admin Admin		
CC 1000 Employee Records2.xlsx	Tuesday at 9:54 AM	Admin Admin	Confidential	
Project Obsidian	Sunday at 10:41 PM	Admin Admin	Highly Confidential \ High	
ContosoNoLabelUploadTest.pdf	July 4	Admin Admin	Gen	
DATALOSS_WARNING_README.txt	June 28	Shyam		
Document.docx	Tuesday at 3:17 AM	Admin Admin	Confidential	
Document1.docx	5 days ago	Admin Admin	Confidential	
Document10.docx	December 20, 2021	Admin Admin	Label which requires MFA	
Document12.docx	May 9	Admin Admin	General	

This file has been automatically labelled

Auto-labeling a PDF file



Microsoft Purview
RA
Insider risk management > Alerts > Alert: Confidentiality obligation during departure

(31ac5f2b) Alert: Confidentiality obligation during departure

Assign
Needs review
Confirm alert to an existing case
Dismiss alert
What will these actions do?

High | Risk score: 87/100 | Alert created on Feb 22, 2024 (UTC)

Activity that generated this alert Reduce alerts for this activity

Data infiltration: Files downloaded from unallowed site
87/100 High severity | Apr 10, 2024 (UTC)
2 events: Files downloaded from 1 unallowed site
2 events: Files that have labels applied, including: Project Alpha
Factors that impacted risk score:
Includes unallowed domains (1 event)

View all activity

Triggering event
May 28, 2024 (UTC)
An HR connector imported a resignation date for this user.

User details
Potential high impact user
User accessed more content containing sensitive info than other users.
+ 2 more reasons
Priority user gro
Project Tiger Tented Project
+ 1 more groups
Anony85KF-34DF
View all details

User alert history
Last 30 days
No alert history
View full user history

All risk factors for this user's activity

Top exfiltration activities
1.9K exfiltration activities

Copied to USB	428
Download from SharePoint	200
Email sent to external recipient	1,289

View all exfiltration activity

Cumulative exfiltration activities
High severity cumulative exfiltration activities detected (Risk score: 82/100)
User activity detected ranges from 04/09 - 04/10

All exfiltration activities with prioritized content
More events than 90% compared to teammates.

User	467
Teammates	2

Shared SharePoint files externally
More events than 99% compared to users that access same SharePoint sites.

User	20
Users who access same SharePoi...	9

All exfiltration activities
More events than 30% compared to users with similar job title.

User	21
Users with similar job title	9

View all cumulative exfiltration activities

View all sequence activity

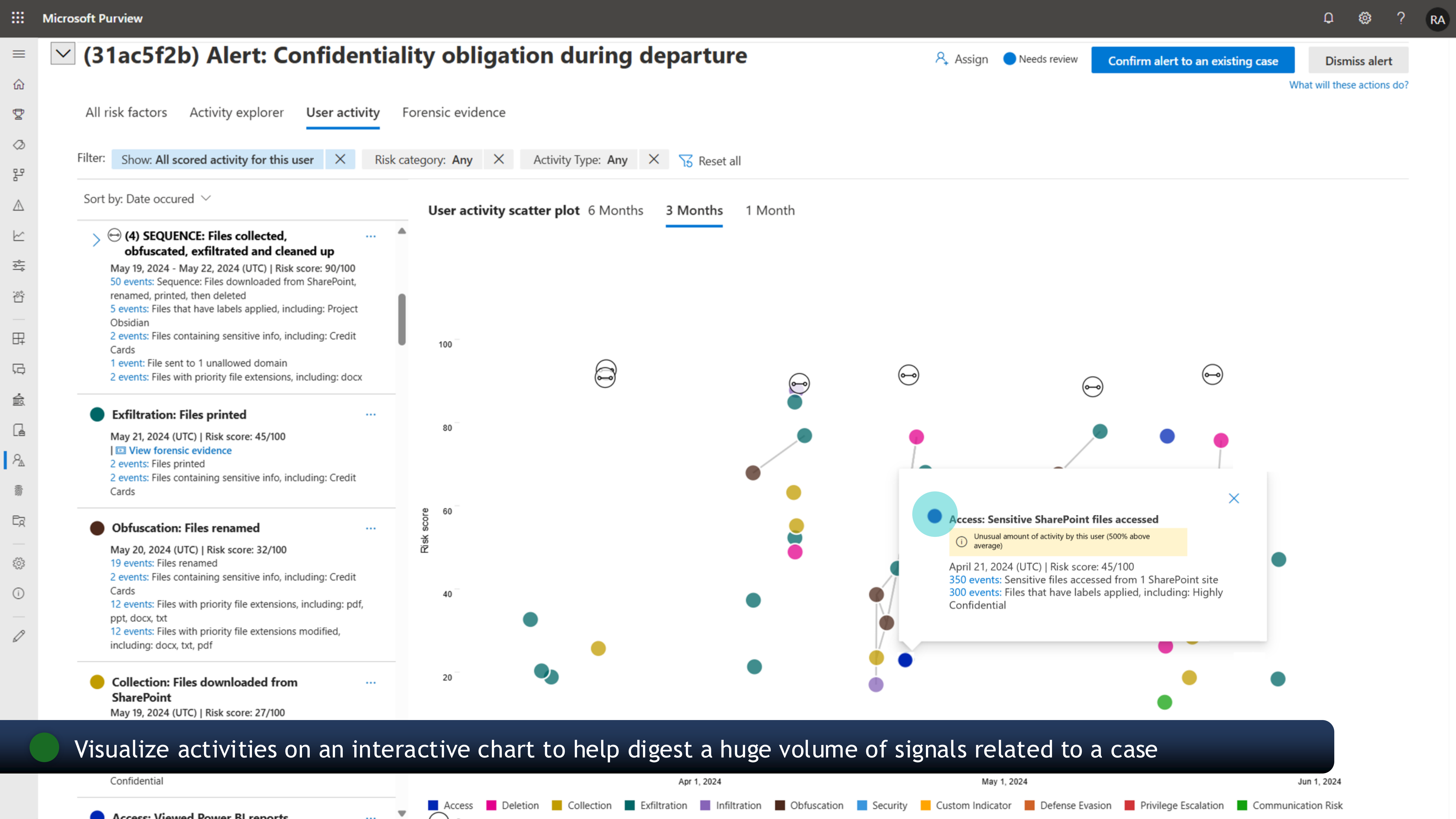
No activity is considered unusual for this user

No activity includes events with priority content

2 activities include events with unallowed domains

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Insider Risk Management alerts page, showing risk factors for user’s activity



(31ac5f2b) Alert: Confidentiality obligation during departure

Filter: Show: All scored activity for this user ✕ Risk category: Any ✕ Activity Type: Any ✕

Sort by: Date occured

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

May 19, 2024 - May 22, 2024 (UTC) | Risk score: 90/100

50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted

5 events: Files that have labels applied, including: Project Obsidian

2 events: Files containing sensitive info, including: Credit Cards

1 event: File sent to 1 unallowed domain

2 events: Files with priority file extensions, including: docx

Exfiltration: Files printed

May 21, 2024 (UTC) | Risk score: 45/100

| View forensic evidence

2 events: Files printed

2 events: Files containing sensitive info, including: Credit Cards

Obfuscation: Files renamed

May 20, 2024 (UTC) | Risk score: 32/100

19 events: Files renamed

2 events: Files containing sensitive info, including: Credit Cards

12 events: Files with priority file extensions, including: pdf, ppt, docx, txt

12 events: Files with priority file extensions modified, including: docx, txt, pdf

Collection: Files downloaded from SharePoint

May 19, 2024 (UTC) | Risk score: 27/100

Confidential

Access: Viewed Power BI reports

Access: Sensitive SharePoint files accessed

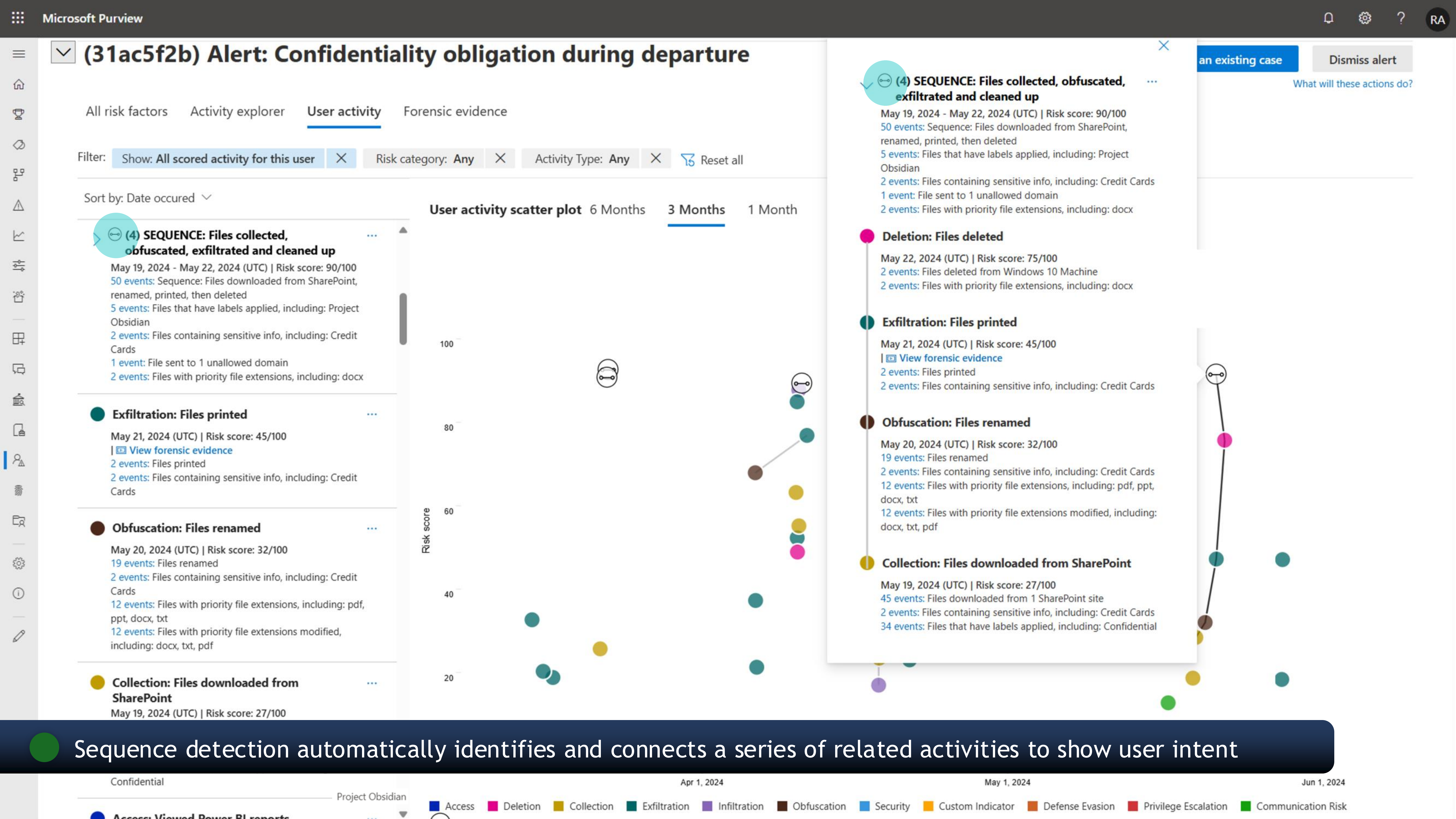
Unusual amount of activity by this user (500% above average)

April 21, 2024 (UTC) | Risk score: 45/100

350 events: Sensitive files accessed from 1 SharePoint site

300 events: Files that have labels applied, including: Highly Confidential

Visualize activities on an interactive chart to help digest a huge volume of signals related to a case



Microsoft Purview

(31ac5f2b) Alert: Confidentiality obligation during departure

an existing case | Dismiss alert

What will these actions do?

All risk factors | Activity explorer | **User activity** | Forensic evidence

Filter: Show: **All scored activity for this user** ✕ | Risk category: **Any** ✕ | Activity Type: **Any** ✕ | Reset all

Sort by: Date occured

(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
May 19, 2024 - May 22, 2024 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
5 events: Files that have labels applied, including: Project Obsidian
2 events: Files containing sensitive info, including: Credit Cards
1 event: File sent to 1 unallowed domain
2 events: Files with priority file extensions, including: docx

Exfiltration: Files printed
May 21, 2024 (UTC) | Risk score: 45/100
| View forensic evidence
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards

Obfuscation: Files renamed
May 20, 2024 (UTC) | Risk score: 32/100
19 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
12 events: Files with priority file extensions, including: pdf, ppt, docx, txt
12 events: Files with priority file extensions modified, including: docx, txt, pdf

Collection: Files downloaded from SharePoint
May 19, 2024 (UTC) | Risk score: 27/100

Confidential

Project Obsidian

Access: Viewed Power BI reports

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

■ Access ■ Deletion ■ Collection ■ Exfiltration ■ Infiltration ■ Obfuscation ■ Security ■ Custom Indicator ■ Defense Evasion ■ Privilege Escalation ■ Communication Risk

(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
May 19, 2024 - May 22, 2024 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
5 events: Files that have labels applied, including: Project Obsidian
2 events: Files containing sensitive info, including: Credit Cards
1 event: File sent to 1 unallowed domain
2 events: Files with priority file extensions, including: docx

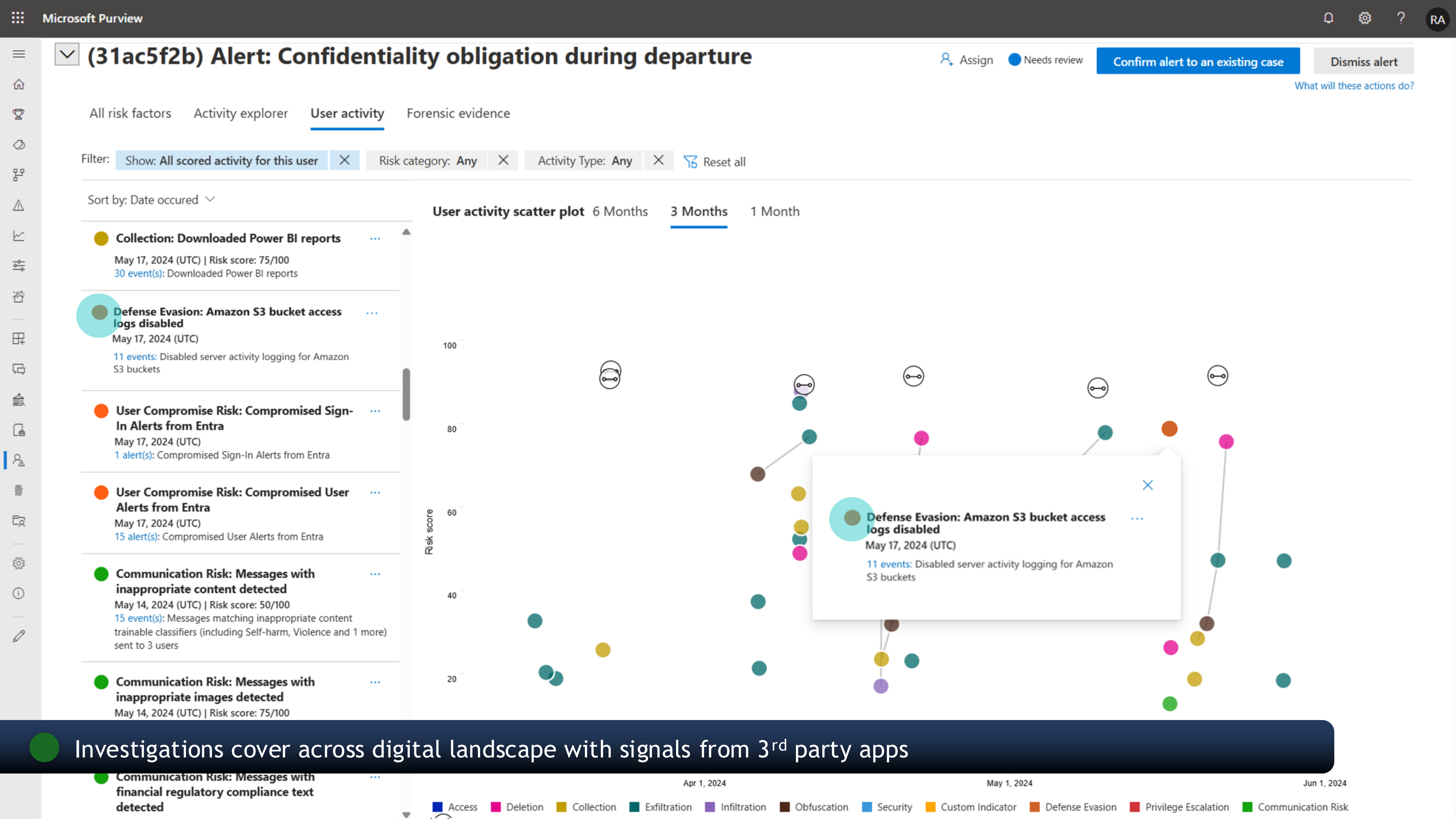
Deletion: Files deleted
May 22, 2024 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine
2 events: Files with priority file extensions, including: docx

Exfiltration: Files printed
May 21, 2024 (UTC) | Risk score: 45/100
| View forensic evidence
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards

Obfuscation: Files renamed
May 20, 2024 (UTC) | Risk score: 32/100
19 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
12 events: Files with priority file extensions, including: pdf, ppt, docx, txt
12 events: Files with priority file extensions modified, including: docx, txt, pdf

Collection: Files downloaded from SharePoint
May 19, 2024 (UTC) | Risk score: 27/100
45 events: Files downloaded from 1 SharePoint site
2 events: Files containing sensitive info, including: Credit Cards
34 events: Files that have labels applied, including: Confidential

Sequence detection automatically identifies and connects a series of related activities to show user intent



(31ac5f2b) Alert: Confidentiality obligation during departure

Filter: Show: All scored activity for this user | Risk category: Any | Activity Type: Any

Sort by: Date occured

Collection: Downloaded Power BI reports
May 17, 2024 (UTC) | Risk score: 75/100
30 event(s): Downloaded Power BI reports

Defense Evasion: Amazon S3 bucket access logs disabled
May 17, 2024 (UTC)
11 events: Disabled server activity logging for Amazon S3 buckets

User Compromise Risk: Compromised Sign-In Alerts from Entra
May 17, 2024 (UTC)
1 alert(s): Compromised Sign-In Alerts from Entra

User Compromise Risk: Compromised User Alerts from Entra
May 17, 2024 (UTC)
15 alert(s): Compromised User Alerts from Entra

Communication Risk: Messages with inappropriate content detected
May 14, 2024 (UTC) | Risk score: 50/100
15 event(s): Messages matching inappropriate content trainable classifiers (including Self-harm, Violence and 1 more) sent to 3 users

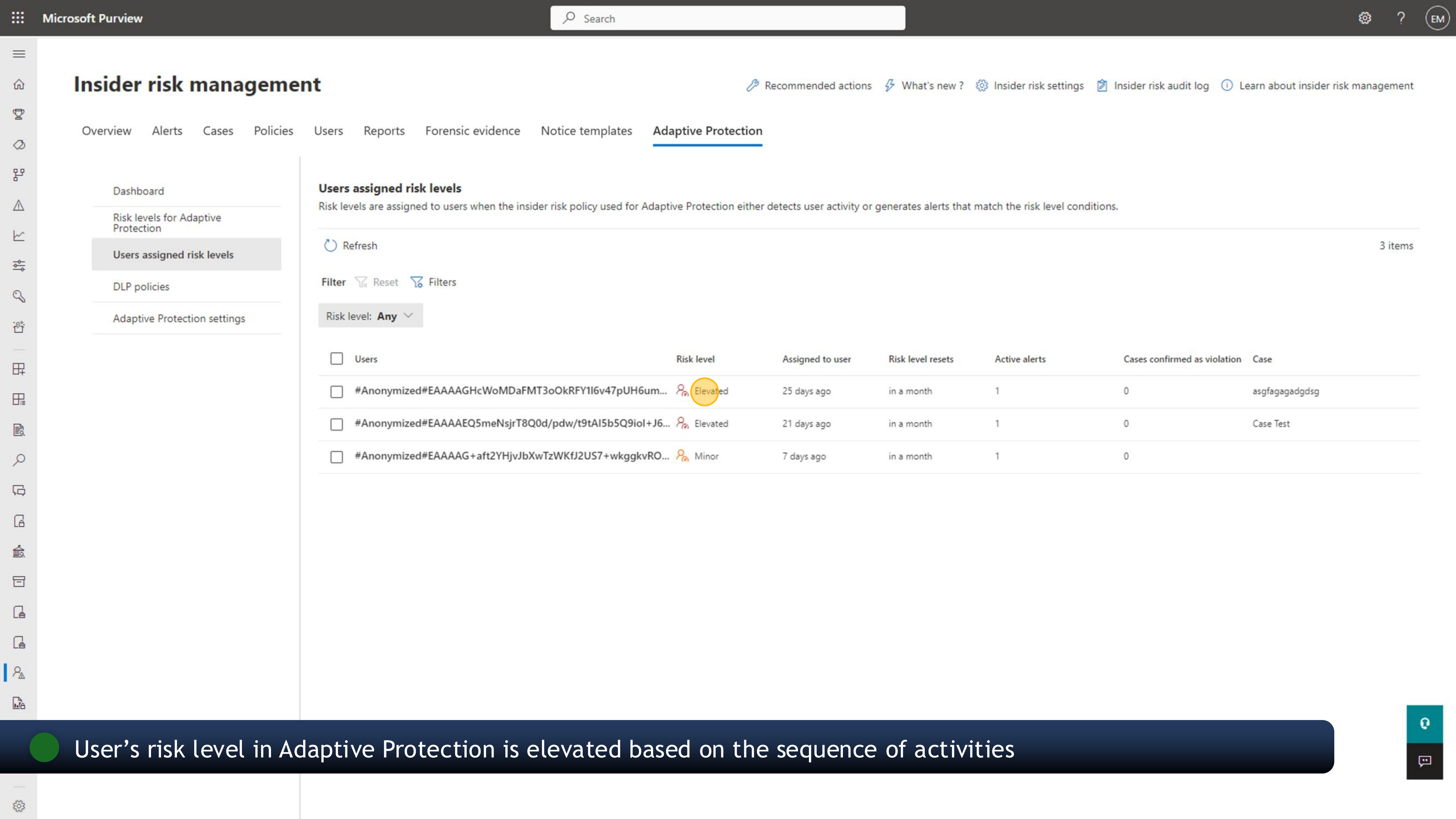
Communication Risk: Messages with inappropriate images detected
May 14, 2024 (UTC) | Risk score: 75/100

Communication Risk: Messages with financial regulatory compliance text detected

User activity scatter plot

Defense Evasion: Amazon S3 bucket access logs disabled
May 17, 2024 (UTC)
11 events: Disabled server activity logging for Amazon S3 buckets

Investigations cover across digital landscape with signals from 3rd party apps



Insider risk management

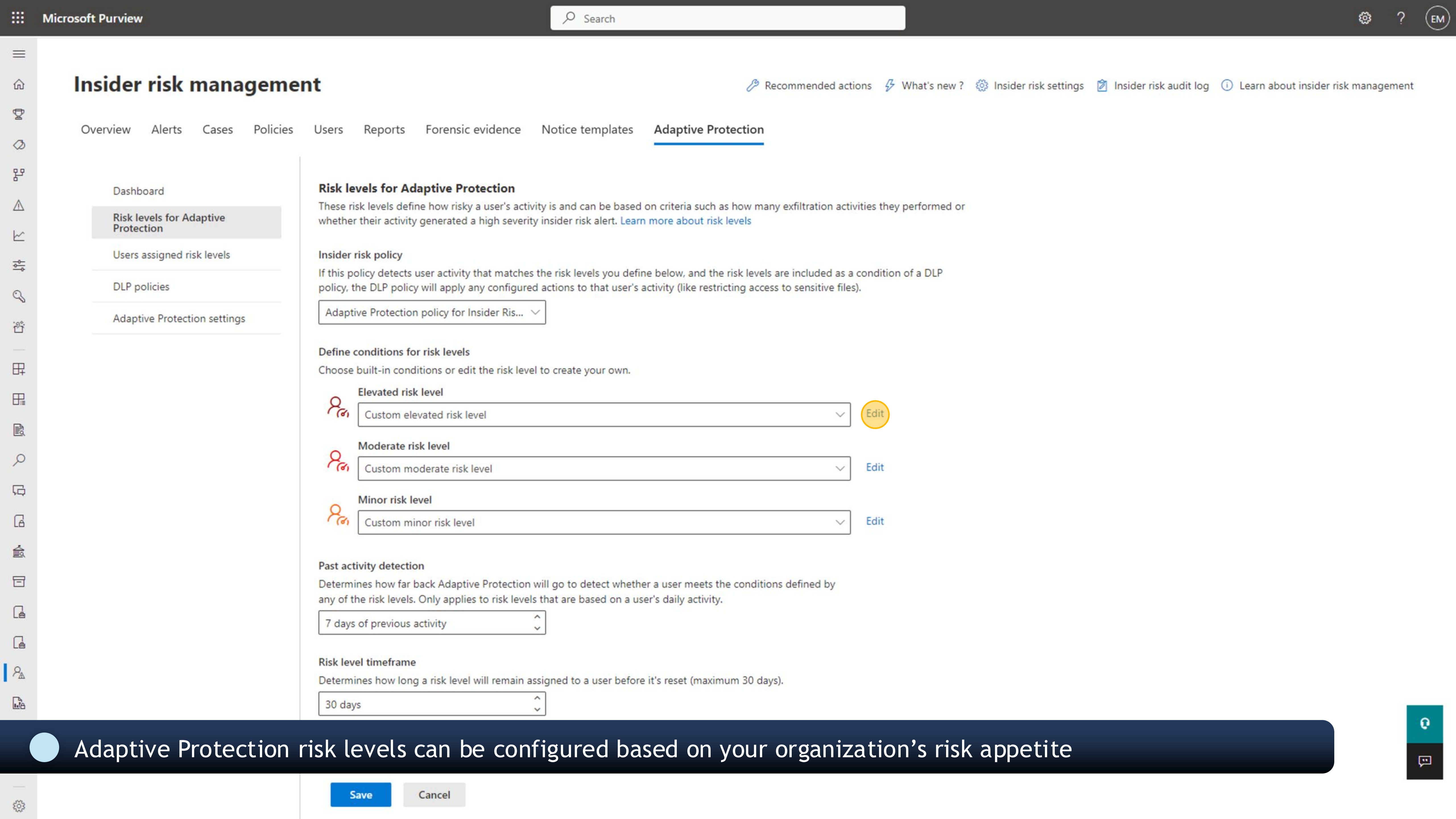
Users assigned risk levels

Risk levels are assigned to users when the insider risk policy used for Adaptive Protection either detects user activity or generates alerts that match the risk level conditions.

Risk level: **Any**

□	Users	Risk level	Assigned to user	Risk level resets	Active alerts	Cases confirmed as violation	Case
□	#Anonymized#EAAAAGHcWoMDaFMT3oOkRFY1l6v47pUH6um...	Elevated	25 days ago	in a month	1	0	asgfagagadgdsg
□	#Anonymized#EAAAAEQ5meNsjrT8Q0d/pdw/t9tAI5b5Q9iol+J6...	Elevated	21 days ago	in a month	1	0	Case Test
□	#Anonymized#EAAAAG+aft2YHjvJbXwTzWKfJ2US7+wkggkvRO...	Minor	7 days ago	in a month	1	0	

User’s risk level in Adaptive Protection is elevated based on the sequence of activities



Microsoft Purview

Search

Insider risk management

Recommended actions | What's new ? | Insider risk settings | Insider risk audit log | Learn about insider risk management

Overview | Alerts | Cases | Policies | Users | Reports | Forensic evidence | Notice templates | **Adaptive Protection**

- Dashboard
- **Risk levels for Adaptive Protection**
- Users assigned risk levels
- DLP policies
- Adaptive Protection settings

Risk levels for Adaptive Protection

These risk levels define how risky a user's activity is and can be based on criteria such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. Learn more about risk levels

Insider risk policy

If this policy detects user activity that matches the risk levels you define below, and the risk levels are included as a condition of a DLP policy, the DLP policy will apply any configured actions to that user's activity (like restricting access to sensitive files).

Adaptive Protection policy for Insider Ris...

Define conditions for risk levels

Choose built-in conditions or edit the risk level to create your own.

Elevated risk level: Custom elevated risk level — Edit

Moderate risk level: Custom moderate risk level — Edit

Minor risk level: Custom minor risk level — Edit

Past activity detection

Determines how far back Adaptive Protection will go to detect whether a user meets the conditions defined by any of the risk levels. Only applies to risk levels that are based on a user's daily activity.

7 days of previous activity

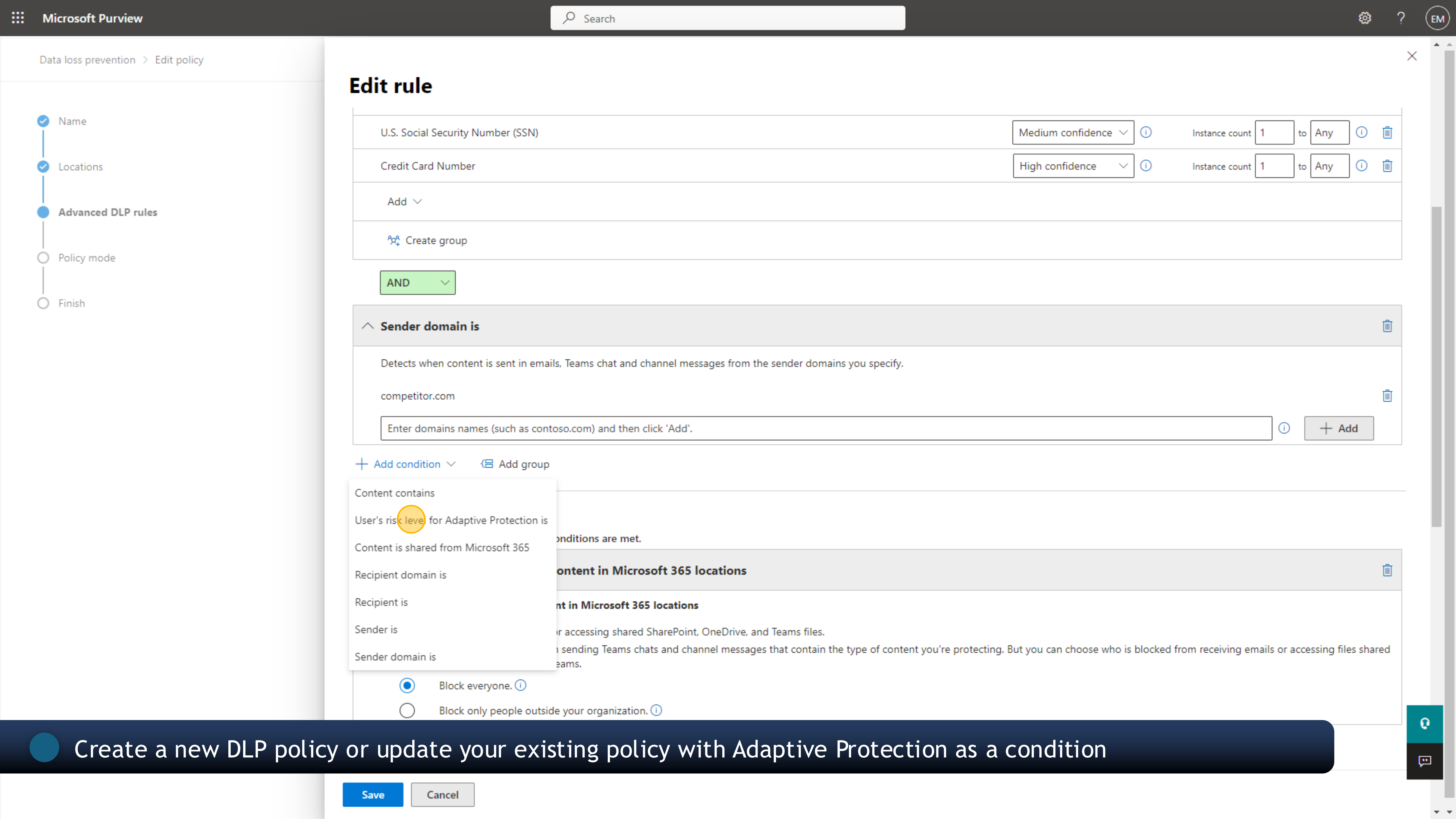
Risk level timeframe

Determines how long a risk level will remain assigned to a user before it's reset (maximum 30 days).

30 days

Save | Cancel

Adaptive Protection risk levels can be configured based on your organization’s risk appetite



Microsoft Purview

Search

Data loss prevention > Edit policy

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

Edit rule

U.S. Social Security Number (SSN)	Medium confidence	Instance count	1	to	Any
Credit Card Number	High confidence	Instance count	1	to	Any

Add

Create group

AND

Sender domain is

Detects when content is sent in emails, Teams chat and channel messages from the sender domains you specify.

competitor.com

Enter domains names (such as contoso.com) and then click 'Add'.

+ Add

+ Add condition   Add group

- Content contains
- User's risk level for Adaptive Protection is
- Content is shared from Microsoft 365
- Recipient domain is
- Recipient is
- Sender is
- Sender domain is

...onditions are met.

...ontent in Microsoft 365 locations

...nt in Microsoft 365 locations

...r accessing shared SharePoint, OneDrive, and Teams files.

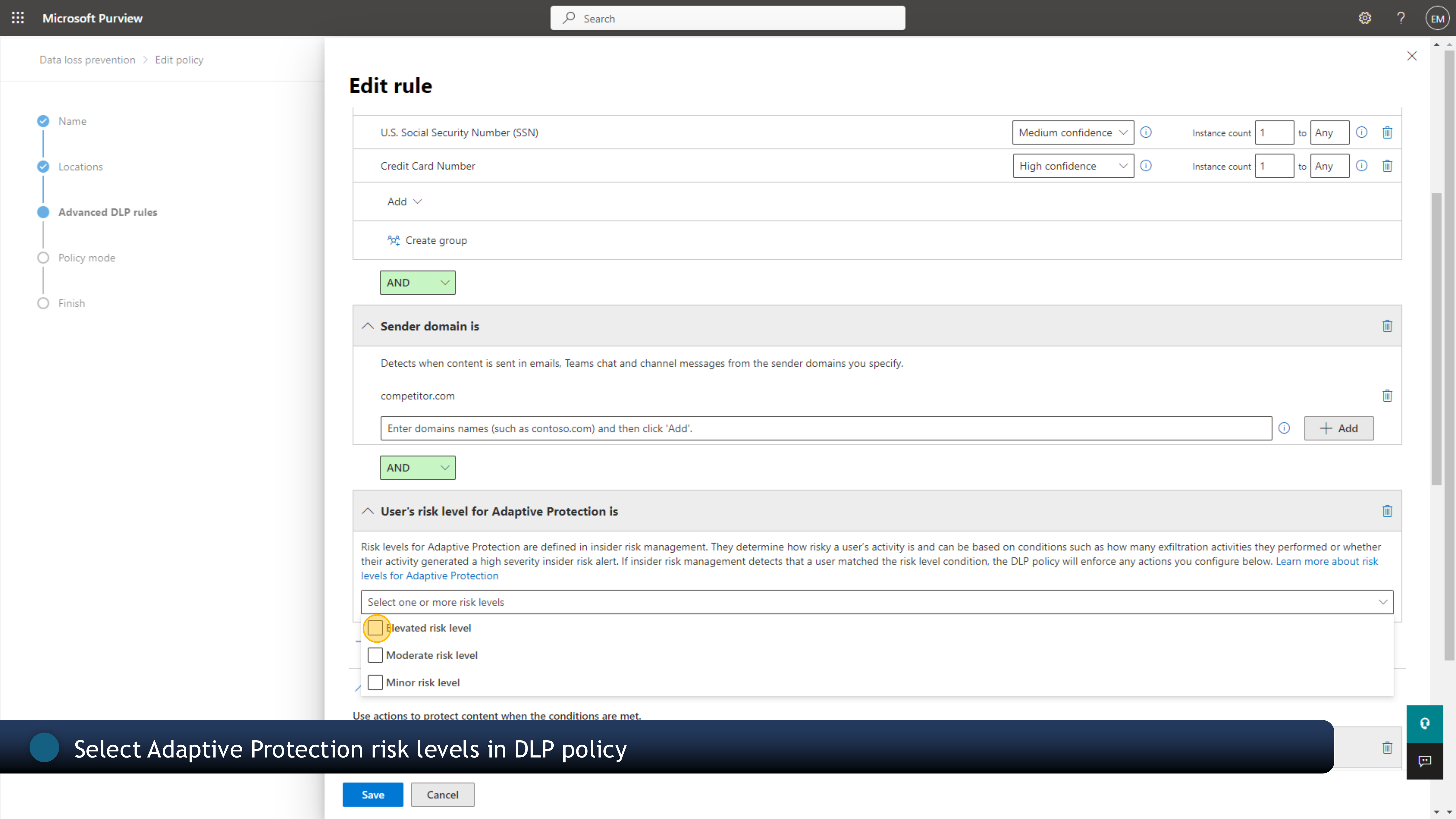
...sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared ...eams.

● Block everyone.

○ Block only people outside your organization.

Save   Cancel

Create a new DLP policy or update your existing policy with Adaptive Protection as a condition



Data loss prevention > Edit policy

- ✓ Name
- ✓ Locations
- ● Advanced DLP rules
- ○ Policy mode
- ○ Finish

Edit rule

U.S. Social Security Number (SSN)	Medium confidence	Instance count 1 to Any	
Credit Card Number	High confidence	Instance count 1 to Any	

Sender domain is

Detects when content is sent in emails, Teams chat and channel messages from the sender domains you specify.

competitor.com

Enter domains names (such as contoso.com) and then click 'Add'.

User's risk level for Adaptive Protection is

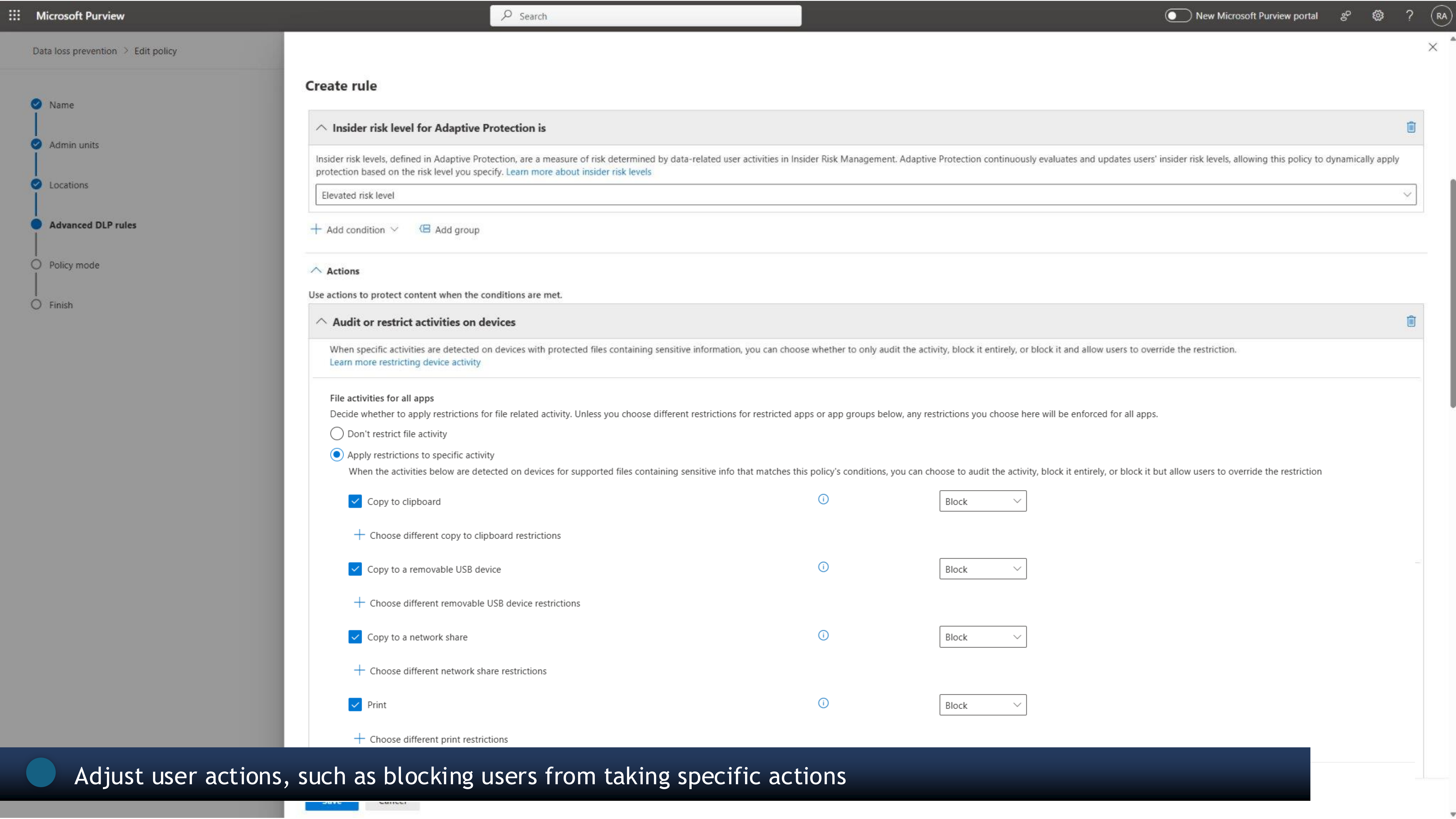
Risk levels for Adaptive Protection are defined in insider risk management. They determine how risky a user's activity is and can be based on conditions such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. If insider risk management 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

Select one or more risk levels

- □ Elevated risk level
- □ Moderate risk level
- □ Minor risk level

Use actions to protect content when the conditions are met.

Select Adaptive Protection risk levels in DLP policy



Create rule

Insider risk level for Adaptive Protection is

Insider risk levels, defined in Adaptive Protection, are a measure of risk determined by data-related user activities in Insider Risk Management. Adaptive Protection continuously evaluates and updates users' insider risk levels, allowing this policy to dynamically apply protection based on the risk level you specify. Learn more about insider risk levels

Elevated risk level

Actions

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

When specific activities are detected on devices with protected files containing sensitive information, you can choose whether to only audit the activity, block it entirely, or block it and allow users to override the restriction.
Learn more restricting device activity

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.

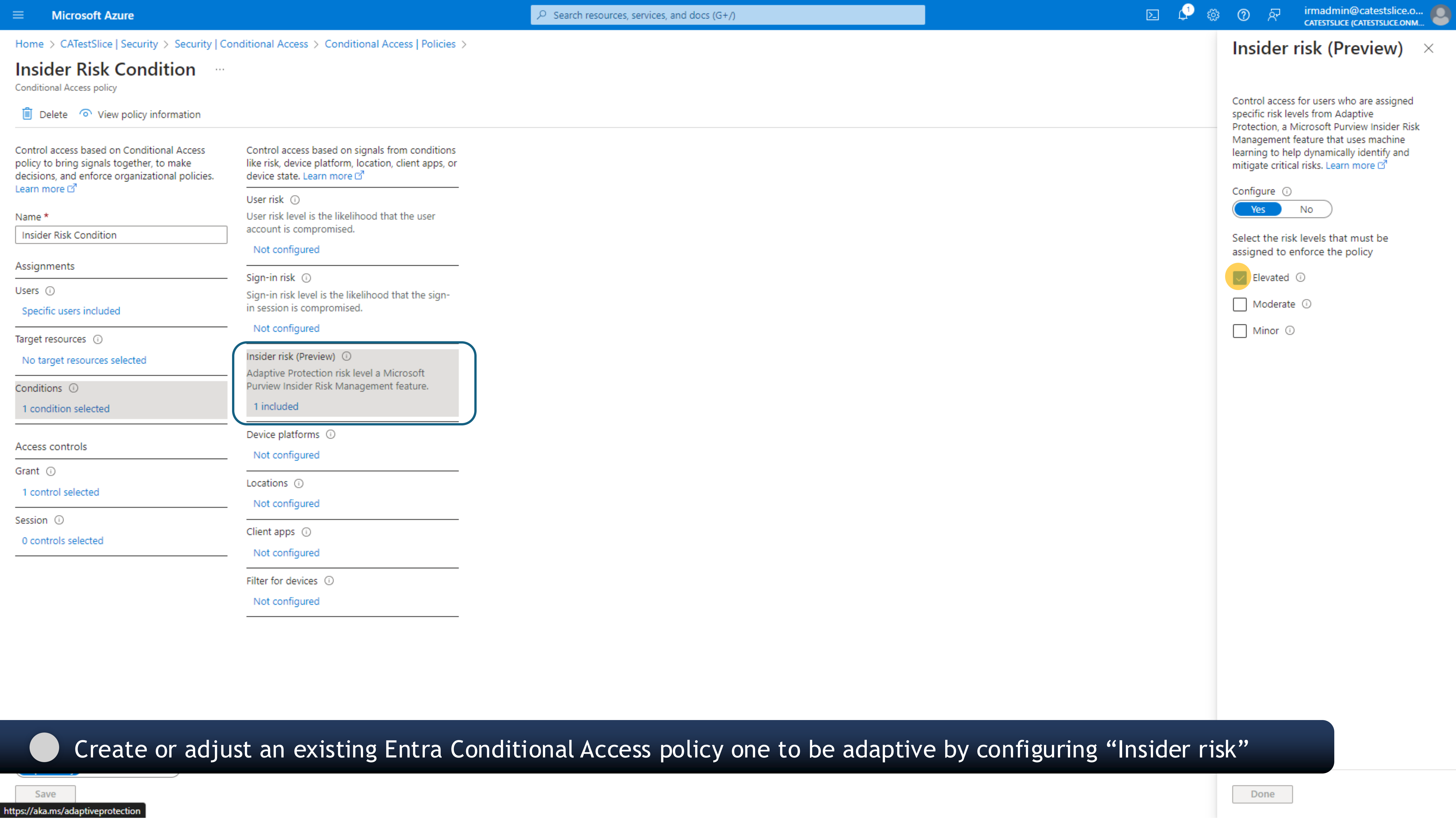
○ Don't restrict file activity

● 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

- ☑ Copy to clipboard — Block
  - + Choose different copy to clipboard restrictions
- ☑ Copy to a removable USB device — Block
  - + Choose different removable USB device restrictions
- ☑ Copy to a network share — Block
  - + Choose different network share restrictions
- ☑ Print — Block
  - + Choose different print restrictions

Adjust user actions, such as blocking users from taking specific actions


Microsoft Azure
Search resources, services, and docs (G+/)
irmadmin@catestslice.o...
CATESTSLICE (CATESTSLICE.ONM...

Home > CATestSlice | Security > Security | Conditional Access > Conditional Access | Policies >

Insider Risk Condition

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Insider Risk Condition

Assignments

Users

Specific users included

Target resources

No target resources selected

Conditions

1 condition selected

Access controls

Grant

1 control selected

Session

0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk

User risk level is the likelihood that the user account is compromised.

Not configured

Sign-in risk

Sign-in risk level is the likelihood that the sign-in session is compromised.

Not configured

Insider risk (Preview)

Adaptive Protection risk level a Microsoft Purview Insider Risk Management feature.

1 included

Device platforms

Not configured

Locations

Not configured

Client apps

Not configured

Filter for devices

Not configured

Insider risk (Preview)

Control access for users who are assigned specific risk levels from Adaptive Protection, a Microsoft Purview Insider Risk Management feature that uses machine learning to help dynamically identify and mitigate critical risks. Learn more

Configure

[✓ Yes] No

Select the risk levels that must be assigned to enforce the policy

☑ Elevated

□ Moderate

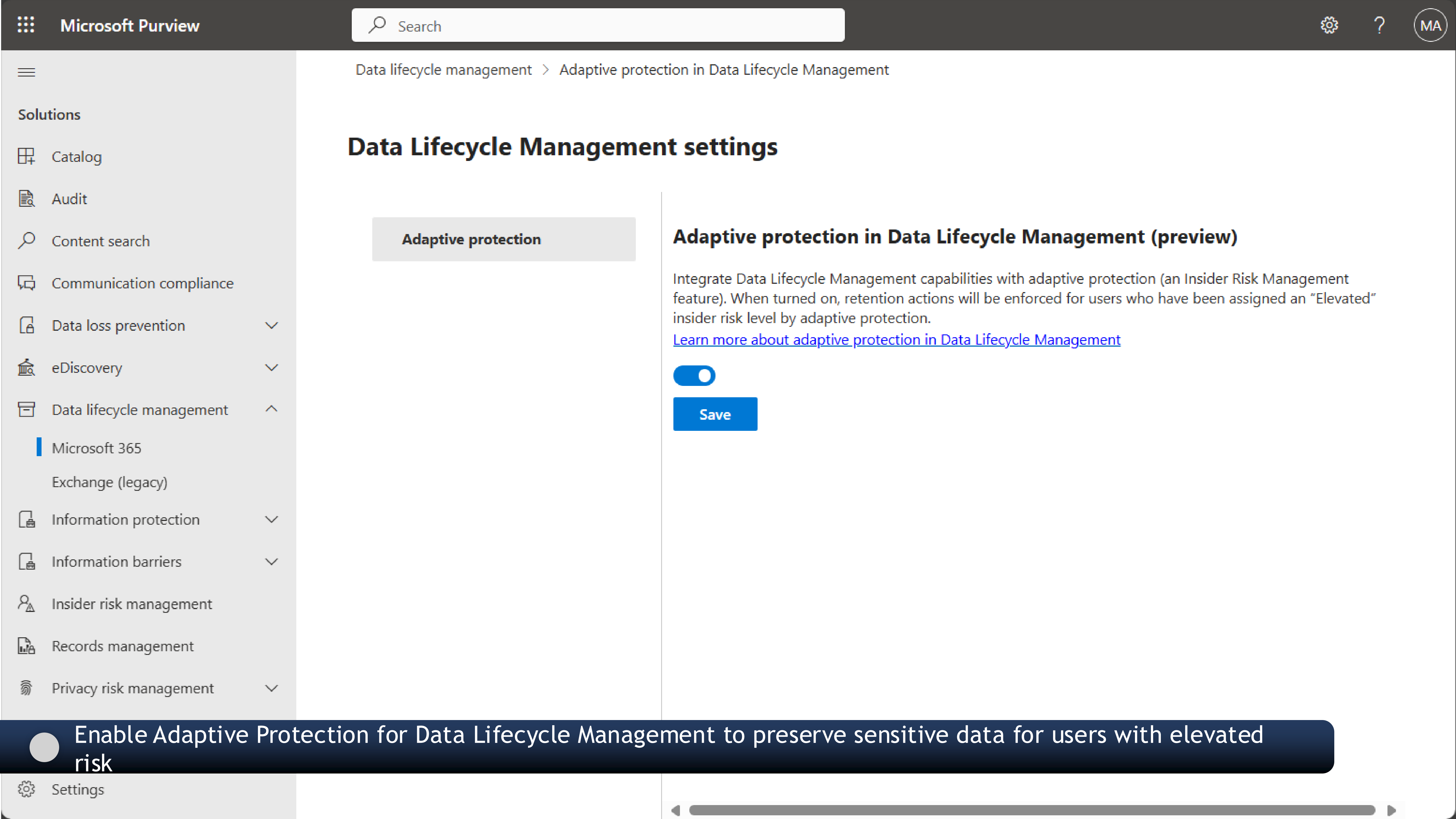
□ Minor

Save

Done

https://aka.ms/adaptiveprotection

Create or adjust an existing Entra Conditional Access policy one to be adaptive by configuring “Insider risk”



Data lifecycle management > Adaptive protection in Data Lifecycle Management

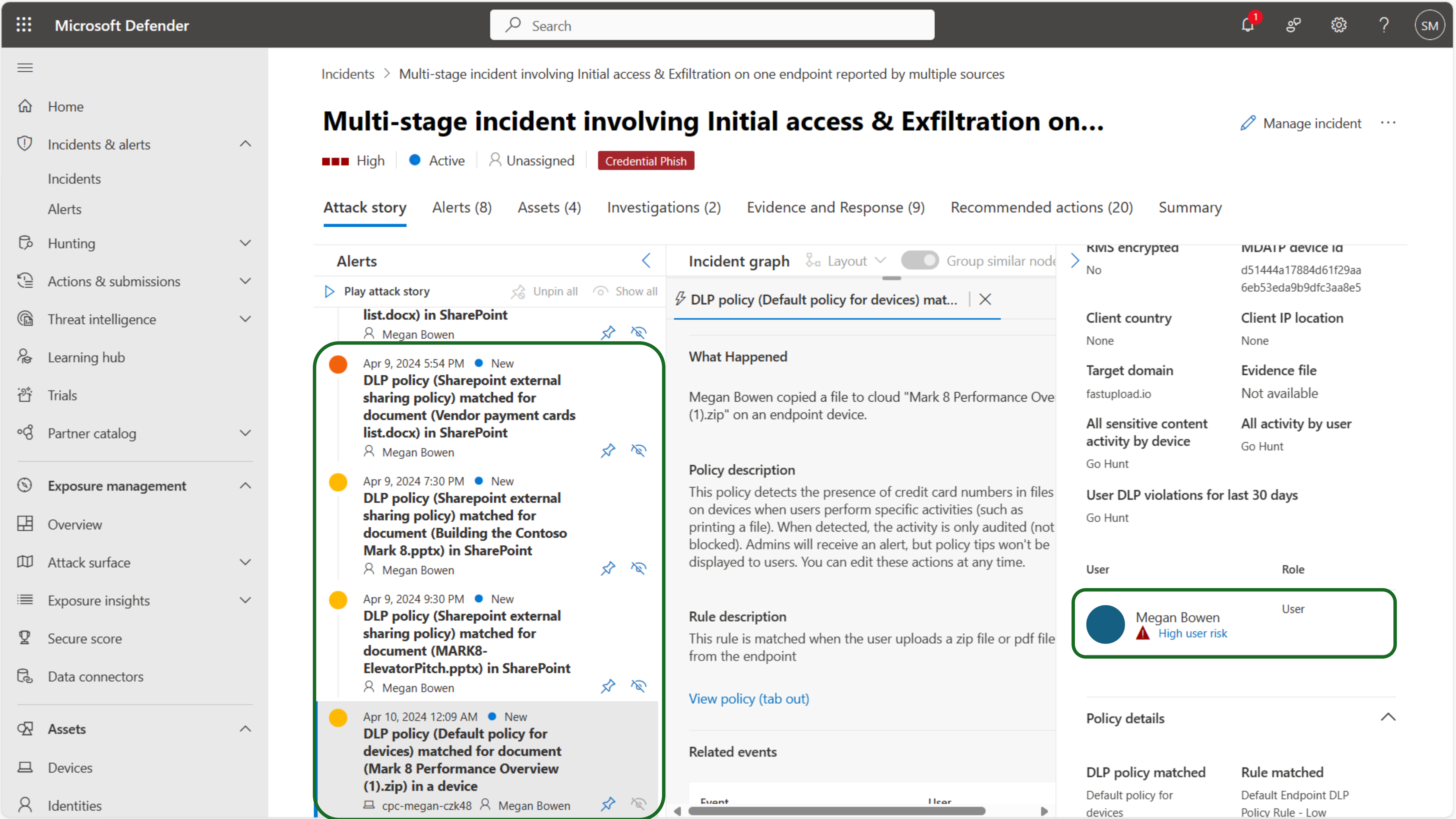
Data Lifecycle Management settings

Adaptive protection in Data Lifecycle Management (preview)

Integrate Data Lifecycle Management capabilities with adaptive protection (an Insider Risk Management feature). When turned on, retention actions will be enforced for users who have been assigned an "Elevated" insider risk level by adaptive protection.

Learn more about adaptive protection in Data Lifecycle Management

Enable Adaptive Protection for Data Lifecycle Management to preserve sensitive data for users with elevated risk



Incidents > Multi-stage incident involving Initial access & Exfiltration on one endpoint reported by multiple sources

Multi-stage incident involving Initial access & Exfiltration on...

Manage incident ···

High | Active | Unassigned | Credential Phish

Attack story | Alerts (8) | Assets (4) | Investigations (2) | Evidence and Response (9) | Recommended actions (20) | Summary

Alerts

Play attack story | Unpin all | Show all

list.docx) in SharePoint
Megan Bowen

Apr 9, 2024 5:54 PM ● New
DLP policy (Sharepoint external sharing policy) matched for document (Vendor payment cards list.docx) in SharePoint
Megan Bowen

Apr 9, 2024 7:30 PM ● New
DLP policy (Sharepoint external sharing policy) matched for document (Building the Contoso Mark 8.pptx) in SharePoint
Megan Bowen

Apr 9, 2024 9:30 PM ● New
DLP policy (Sharepoint external sharing policy) matched for document (MARK8-ElevatorPitch.pptx) in SharePoint
Megan Bowen

Apr 10, 2024 12:09 AM ● New
DLP policy (Default policy for devices) matched for document (Mark 8 Performance Overview (1).zip) in a device
cpc-megan-czk48 Megan Bowen

Incident graph Layout | Group similar node

DLP policy (Default policy for devices) mat... ✕

What Happened

Megan Bowen copied a file to cloud "Mark 8 Performance Ove (1).zip" on an endpoint device.

Policy description

This policy detects the presence of credit card numbers in files on devices when users perform specific activities (such as printing a file). When detected, the activity is only audited (not blocked). Admins will receive an alert, but policy tips won't be displayed to users. You can edit these actions at any time.

Rule description

This rule is matched when the user uploads a zip file or pdf file from the endpoint

View policy (tab out)

Related events

Event	User

RMS encrypted No	**MDATP device id** d51444a17884d61f29aa6eb53eda9b9dfc3aa8e5
Client country None	**Client IP location** None
Target domain fastupload.io	**Evidence file** Not available
All sensitive content activity by device Go Hunt	**All activity by user** Go Hunt
User DLP violations for last 30 days Go Hunt	

User	Role
Megan Bowen High user risk	User

Policy details

DLP policy matched Default policy for devices	**Rule matched** Default Endpoint DLP Policy Rule - Low

Generative AI is reshaping the world but there are associated data security risks..

User creates document without proper access controls making it easy for other users to reference it in Copilot

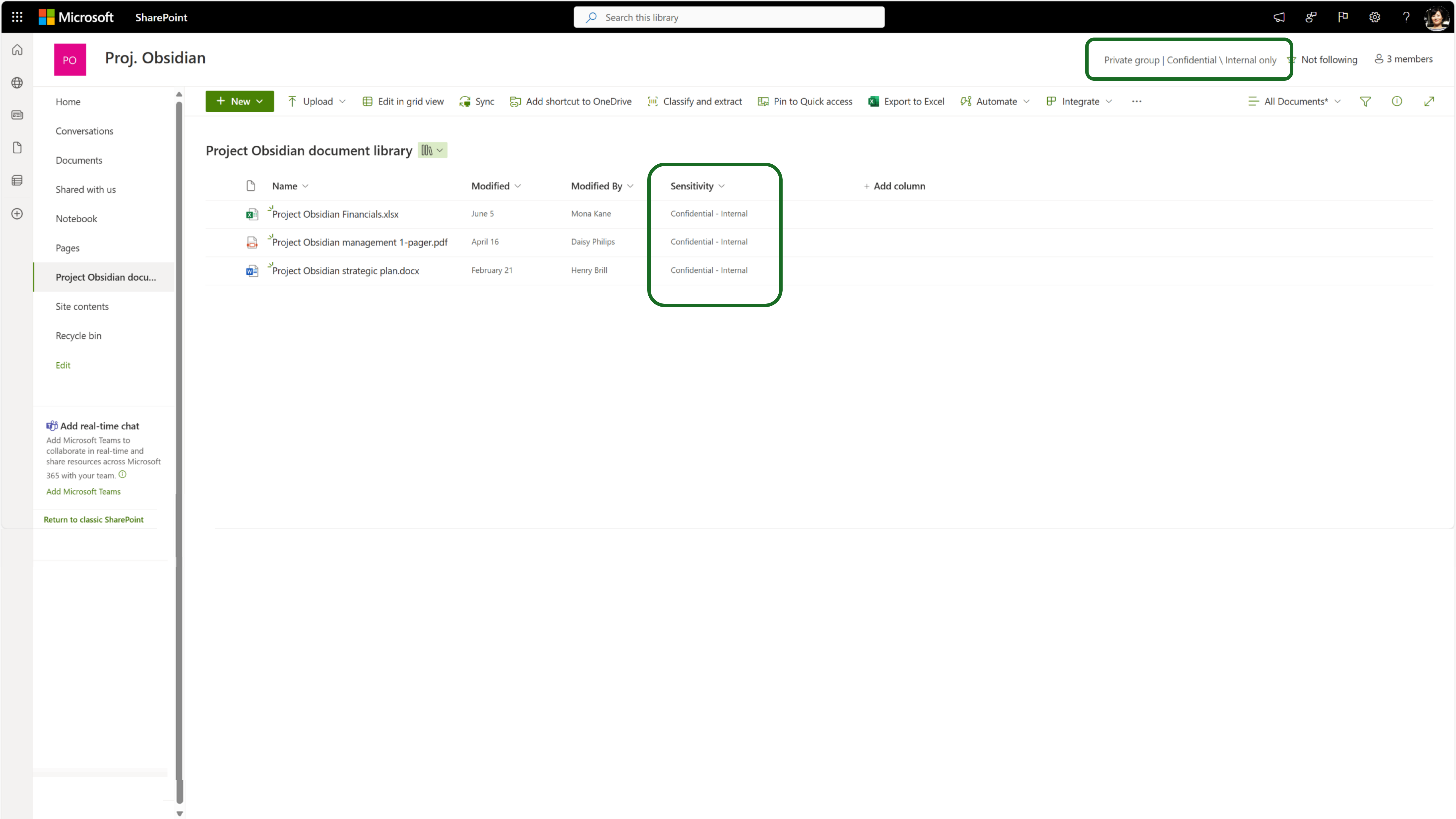
Data overexposure by negligent insider

User asks generative AI to find information on a secret project and leaks it to the press for personal gain

Data leak by disgruntled insider

User negligently shares sensitive data in consumer generative AI apps

Data leak by negligent insider

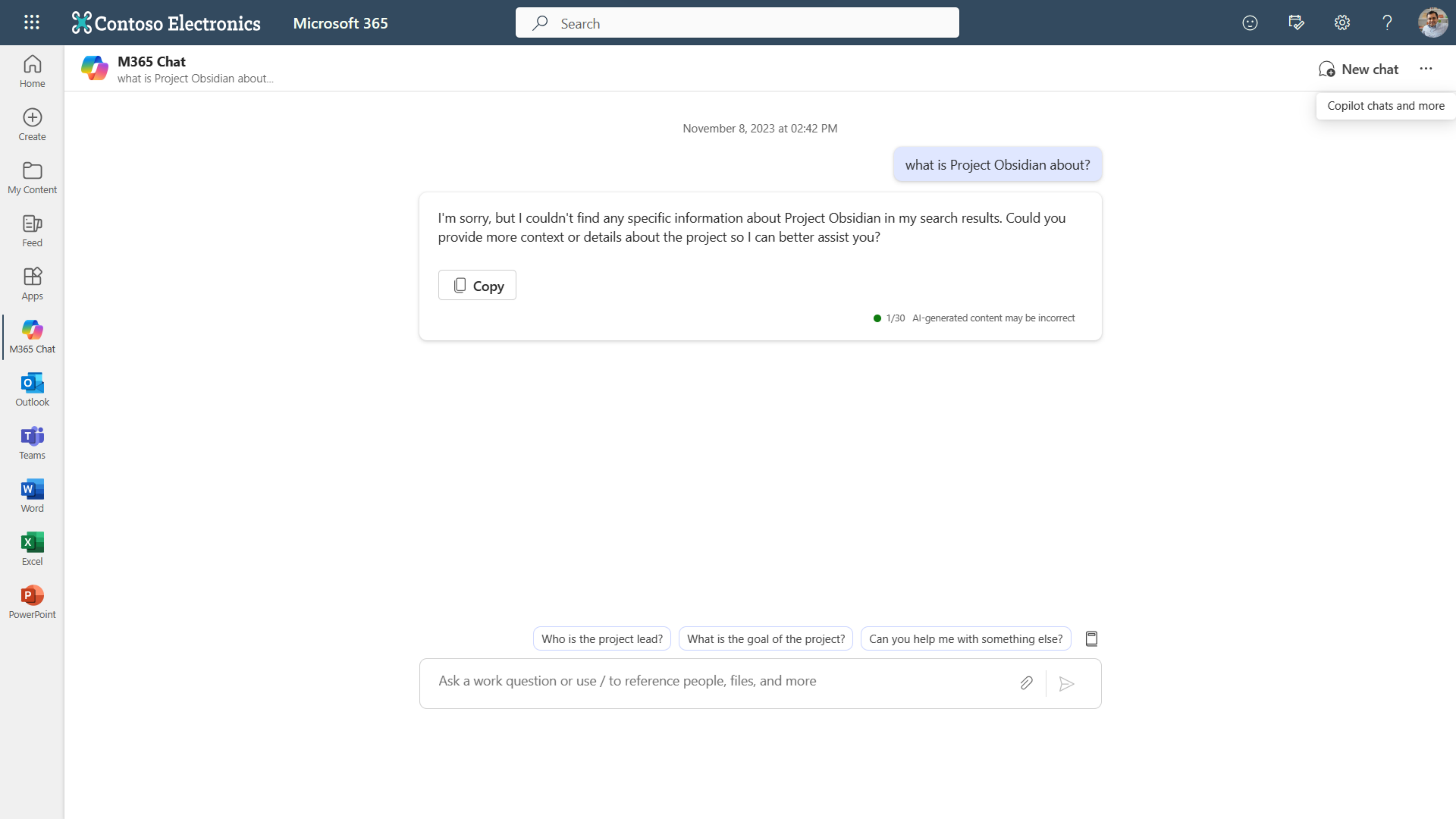


Proj. Obsidian

Add Microsoft Teams to collaborate in real-time and share resources across Microsoft 365 with your team.

Project Obsidian document library

Name	Modified	Modified By	Sensitivity
Project Obsidian Financials.xlsx	June 5	Mona Kane	Confidential - Internal
Project Obsidian management 1-pager.pdf	April 16	Daisy Philips	Confidential - Internal
Project Obsidian strategic plan.docx	February 21	Henry Brill	Confidential - Internal

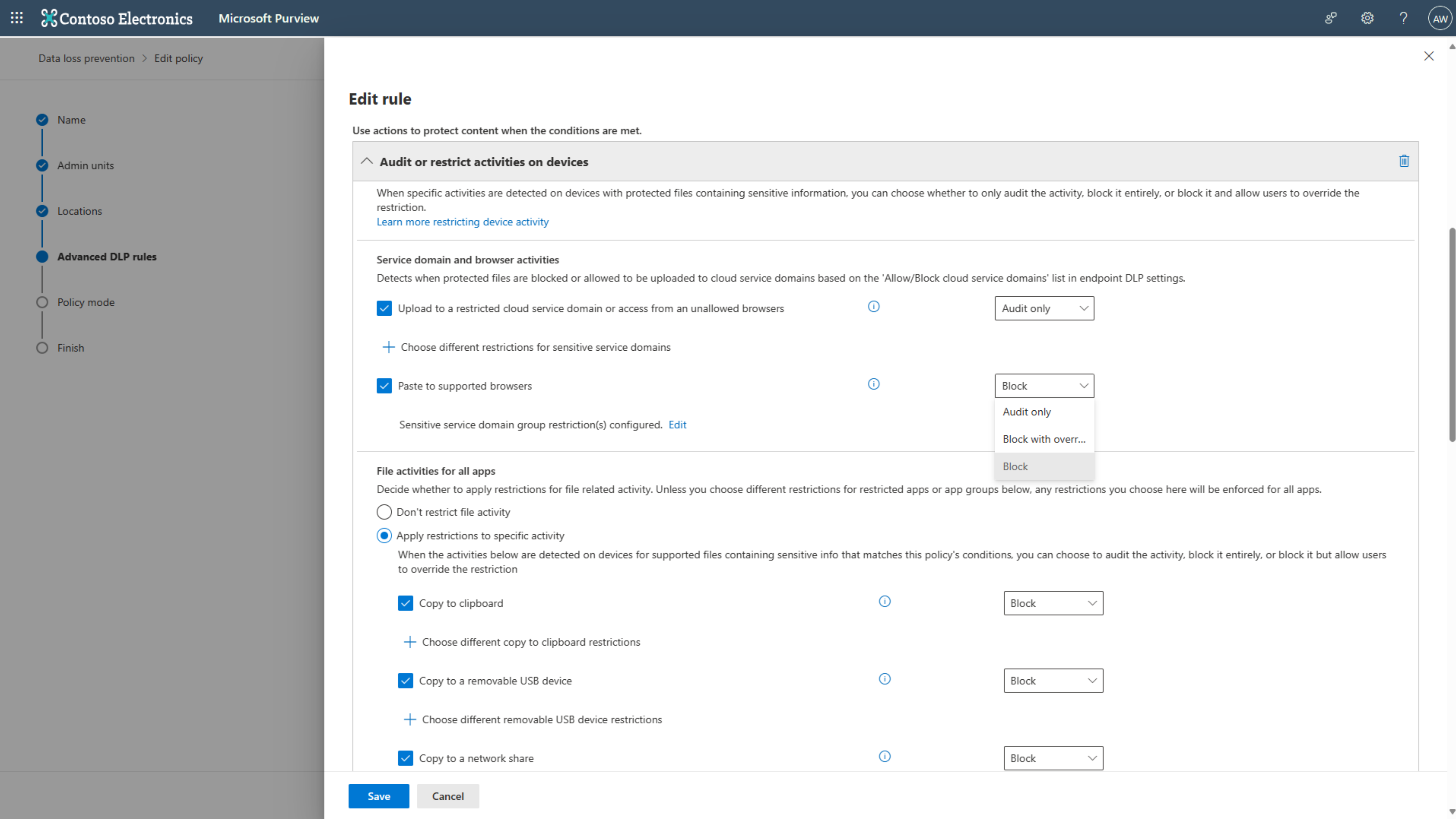


November 8, 2023 at 02:42 PM

what is Project Obsidian about?

I'm sorry, but I couldn't find any specific information about Project Obsidian in my search results. Could you provide more context or details about the project so I can better assist you?

● 1/30 AI-generated content may be incorrect



Data loss prevention > Edit policy

- 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 specific activities are detected on devices with protected files containing sensitive information, you can choose whether to only audit the activity, block it entirely, or block it and 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.

☑ Upload to a restricted cloud service domain or access from an unallowed browsers — Audit only

+ Choose different restrictions for sensitive service domains

☑ Paste to supported browsers — Block

Sensitive service domain group restriction(s) configured. Edit

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

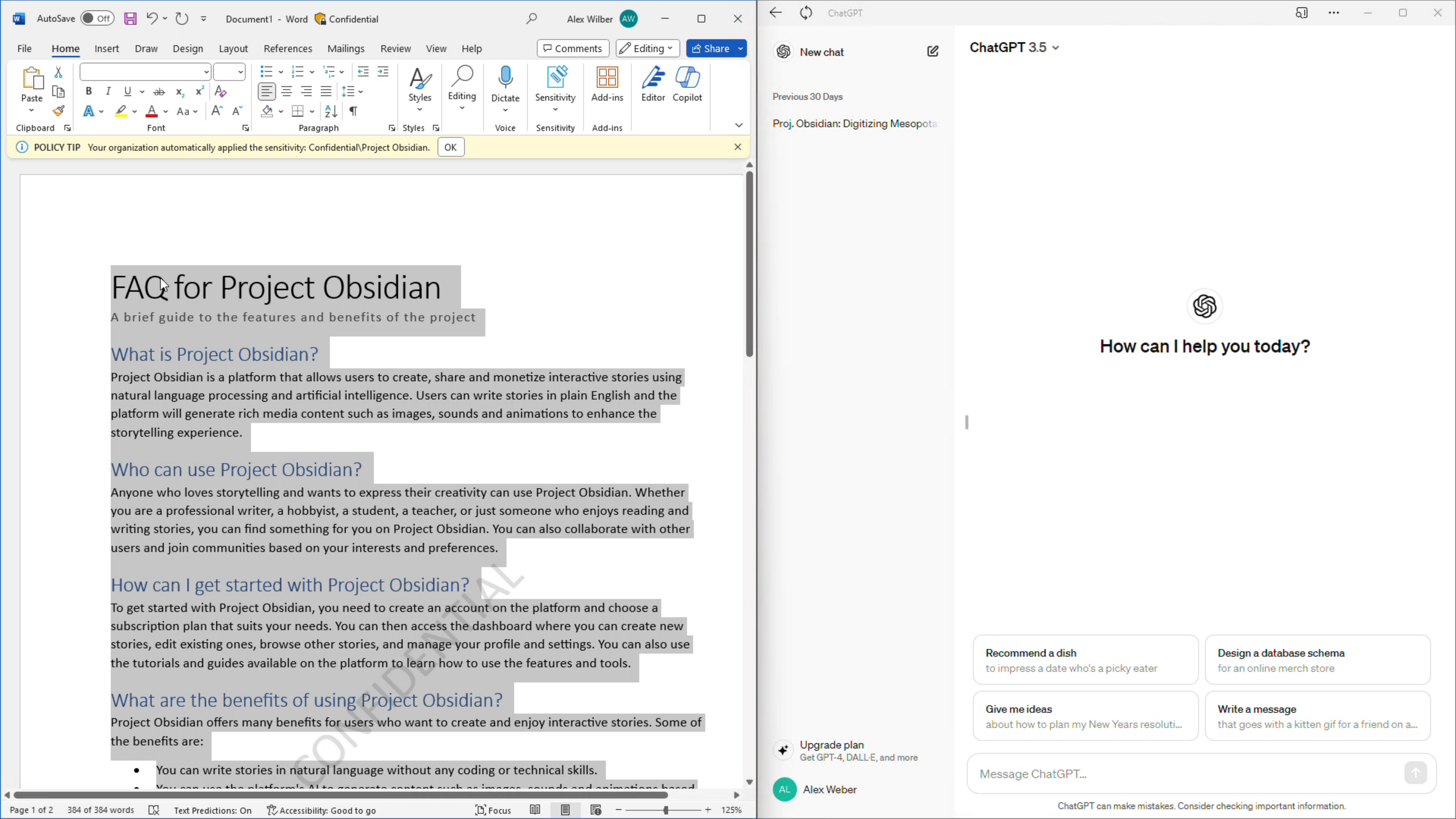
☑ Copy to clipboard — Block

+ Choose different copy to clipboard restrictions

☑ Copy to a removable USB device — Block

+ Choose different removable USB device restrictions

☑ Copy to a network share — Block



POLICY TIP Your organization automatically applied the sensitivity: Confidential\Project Obsidian. OK

FAQ for Project Obsidian

A brief guide to the features and benefits of the project

What is Project Obsidian?

Project Obsidian is a platform that allows users to create, share and monetize interactive stories using natural language processing and artificial intelligence. Users can write stories in plain English and the platform will generate rich media content such as images, sounds and animations to enhance the storytelling experience.

Who can use Project Obsidian?

Anyone who loves storytelling and wants to express their creativity can use Project Obsidian. Whether you are a professional writer, a hobbyist, a student, a teacher, or just someone who enjoys reading and writing stories, you can find something for you on Project Obsidian. You can also collaborate with other users and join communities based on your interests and preferences.

How can I get started with Project Obsidian?

To get started with Project Obsidian, you need to create an account on the platform and choose a subscription plan that suits your needs. You can then access the dashboard where you can create new stories, edit existing ones, browse other stories, and manage your profile and settings. You can also use the tutorials and guides available on the platform to learn how to use the features and tools.

What are the benefits of using Project Obsidian?

Project Obsidian offers many benefits for users who want to create and enjoy interactive stories. Some of the benefits are:

- You can write stories in natural language without any coding or technical skills.
- You can use the platform's AI to generate content such as images, sounds and animations based

How can I help you today?

Recommend a dish
to impress a date who's a picky eater

Design a database schema
for an online merch store

Give me ideas
about how to plan my New Years resoluti...

Write a message
that goes with a kitten gif for a friend on a...

ChatGPT can make mistakes. Consider checking important information.

Microsoft Purview data security | for all your data

3.13.16 Protect the confidentiality of CUI at rest

Built-in

Manual labelling built into Microsoft Fabric workloads

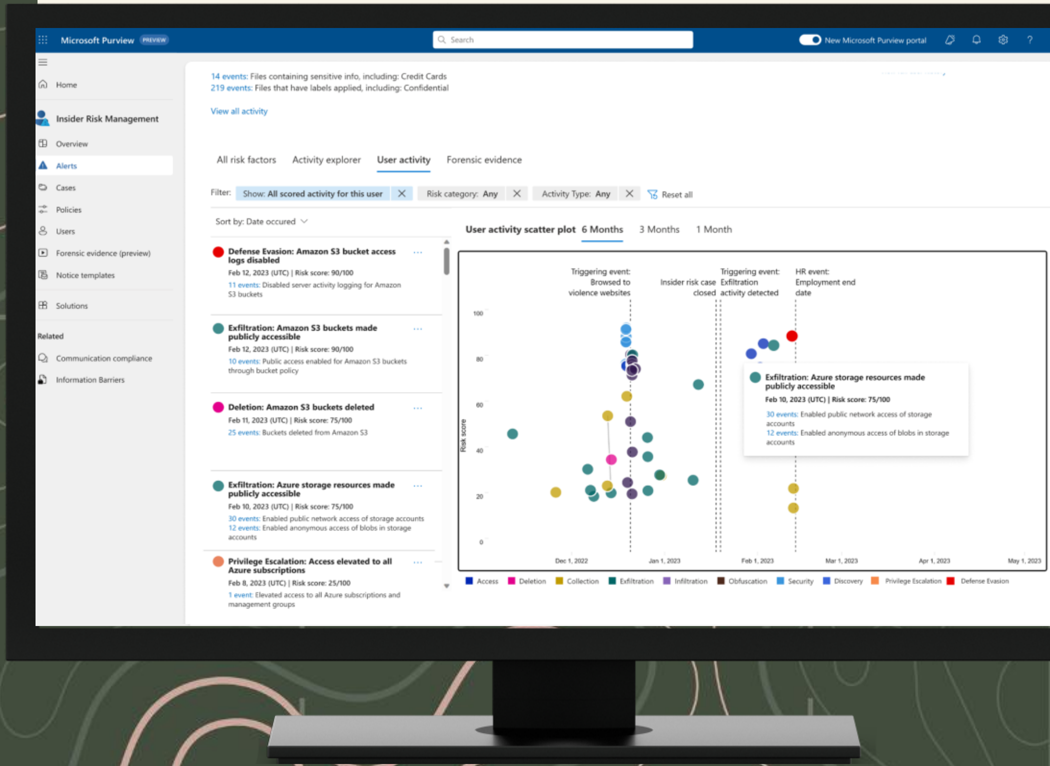
Consistent enforcements

Extend label-based protections to Fabric, Azure SQL, Azure Data Lake Storage, and Amazon S3 buckets

Data risk detections

Signals from clouds and apps now ingested into Purview Insider Risk Management

PREVIEW



14 events: Files containing sensitive info, including: Credit Cards
219 events: Files that have labels applied, including: Confidential

View all activity

Filter: Show: All scored activity for this user | Risk category: Any | Activity Type: Any

Sort by: Date occured

Defense Evasion: Amazon S3 bucket access logs disabled
Feb 12, 2023 (UTC) | Risk score: 90/100
11 events: Disabled server activity logging for Amazon S3 buckets

Exfiltration: Amazon S3 buckets made publicly accessible
Feb 12, 2023 (UTC) | Risk score: 90/100
10 events: Public access enabled for Amazon S3 buckets through bucket policy

Deletion: Amazon S3 buckets deleted
Feb 11, 2023 (UTC) | Risk score: 75/100
25 events: Buckets deleted from Amazon S3

Exfiltration: Azure storage resources made publicly accessible
Feb 10, 2023 (UTC) | Risk score: 75/100
30 events: Enabled public network access of storage accounts
12 events: Enabled anonymous access of blobs in storage accounts

Privilege Escalation: Access elevated to all Azure subscriptions
Feb 8, 2023 (UTC) | Risk score: 25/100
1 event: Elevated access to all Azure subscriptions and management groups

Exfiltration: Azure storage resources made publicly accessible
Feb 10, 2023 (UTC) | Risk score: 75/100
30 events: Enabled public network access of storage accounts
12 events: Enabled anonymous access of blobs in storage accounts

Why choose Microsoft Purview for CUI security

Simplifying the complex with end-to-end protection, saving you time and money.

Comprehensive visibility

Gain insights correlated across data and user context – across structured and unstructured CUI data sources, including Microsoft Azure, AWS, cloud applications as well as generative AI apps.

Seamless integration

Secure CUI end to end using solutions built on a single platform that integrate with each other unlocking new data security value across your estate.

AI-powered security

Get ahead of potential data security incidents with AI-powered data classifiers, risk detection, and adaptive protection.

Getting started with CMMC Level 2

CMMC L2 – Microsoft Purview

Gather insights and deploy policies

Discover CUI in your estate

Leverage out-of-the-box and custom Sensitive Information Types (SITs), trainable classifiers, and more.

Understand critical insider risks

Turn on insider risk analytics and create a recommended CUI leak policy. *Turn on Adaptive Protection.*

Understand critical CUI exfiltration risks

Turn on DLP analytics and create a recommended DLP policy in Microsoft 365 GCC High.

Integrate seamlessly on a unified platform with Microsoft Entra, Microsoft Intune, Microsoft Defender, and more

Actionable insights for security and compliance teams without impact on end users

Advance your CMMC Level 2 journey

CMMC L2 – Microsoft Purview

Gather intelligence and tailor policies

Label and protect CUI

Define label taxonomy and label content by enabling default labels, configuring manual labeling, and scaling with auto-labeling.

Investigate critical risks

Review and investigate high-severity insider risk alerts and finetune policies.

Prevent CUI and sensitive data loss

Fine-tune DLP policies and add Adaptive Protection as a condition in your DLP policy. Run DLP policy in block or block with override mode.

Resources

Data Security Interactive Guides

- Microsoft Purview Information Protection
- Microsoft Purview Data Loss Prevention
- Microsoft Purview Insider Risk management
- Microsoft Copilot for Security in Insider Risk Management

What Licensing Do I Need?

M365E5

M365F3
+ F5 Security / Compliance

OR

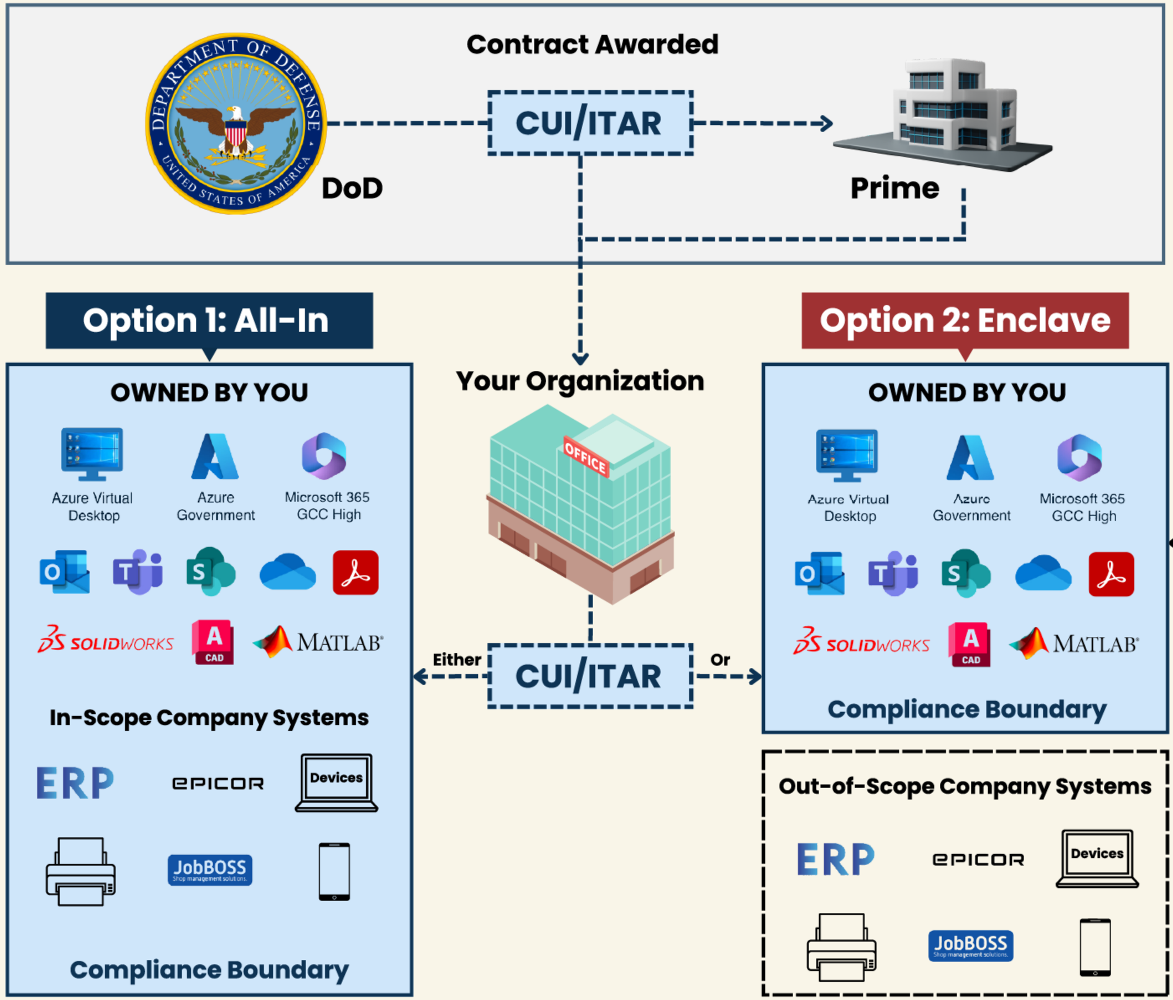
okta onelogin MaaS360 cisco Meraki Cisco webex RingCentral exabeam TITUS Symantec

PingIdentity SailPoint airwatch by vmware McAfee TREND MICRO 3CX Grasshopper proofpoint. VARONIS virtru

RSA mobileiron CROWDSTRIKE GoToMeeting by LogMeIn ShoreTel zoom mimecast netskope bitglass RAPID7

Su

CMMC Solutions



Contract Awarded

DoD

CUI/ITAR

Prime

Your Organization

Either

CUI/ITAR

Or

Option 1: All-In

OWNED BY YOU

Azure Virtual Desktop

Azure Government

Microsoft 365 GCC High

SOLIDWORKS

CAD

MATLAB

In-Scope Company Systems

ERP

EPICOR

Devices

JobBOSS

Compliance Boundary

Option 2: Enclave

OWNED BY YOU

Azure Virtual Desktop

Azure Government

Microsoft 365 GCC High

SOLIDWORKS

CAD

MATLAB

Compliance Boundary

Out-of-Scope Company Systems

ERP

EPICOR

Devices

JobBOSS

SUPPORTED BY US

U.S. Citizens Only

24 x 7 Support

Audit Support

Security Operations

SSP & POAM Management

SUMMIT7

GUARDIAN+ VIGILANCE

NIST ✓

SP 800-171

THE CYBER AB

CMMC CERTIFICATION ✓

DEPARTMENT OF STATE · UNITED STATES OF AMERICA

INTERNATIONAL TRAFFIC IN ARMS

ITAR

REGULATIONS COMPLIANT ✓

Su

Why Summit 7

MICROSOFT LICENSING

CMMC COMPLIANCE

MANAGED SERVICES

SOC SERVICES

CLEARED SERVICES

11
Passed DoD Client Assessments (3) JSVA's

215+
Employees, All US Persons

500+
CMMC/NIST Implementations

900+
Clients- we only support Defense contractors

2024 Microsoft Global Security Partner of the Year Finalist

- Microsoft's #1 AOSG/GCC High Partner
- Summit 7 is the only Azure Expert MSP Microsoft Partner focused on the Microsoft Government Cloud
- 11 Microsoft Advanced Specializations
- Vigilance Service validated into the Microsoft MXDR Partner Program
- Microsoft Partner of the Year for Security in 2020 & Compliance in 2020 and 2022

Contact

☎ 256.585.6868

✉ cmmc@summit7.us

🌐 summit7.us

SECURE THE DIB

Summer Camp