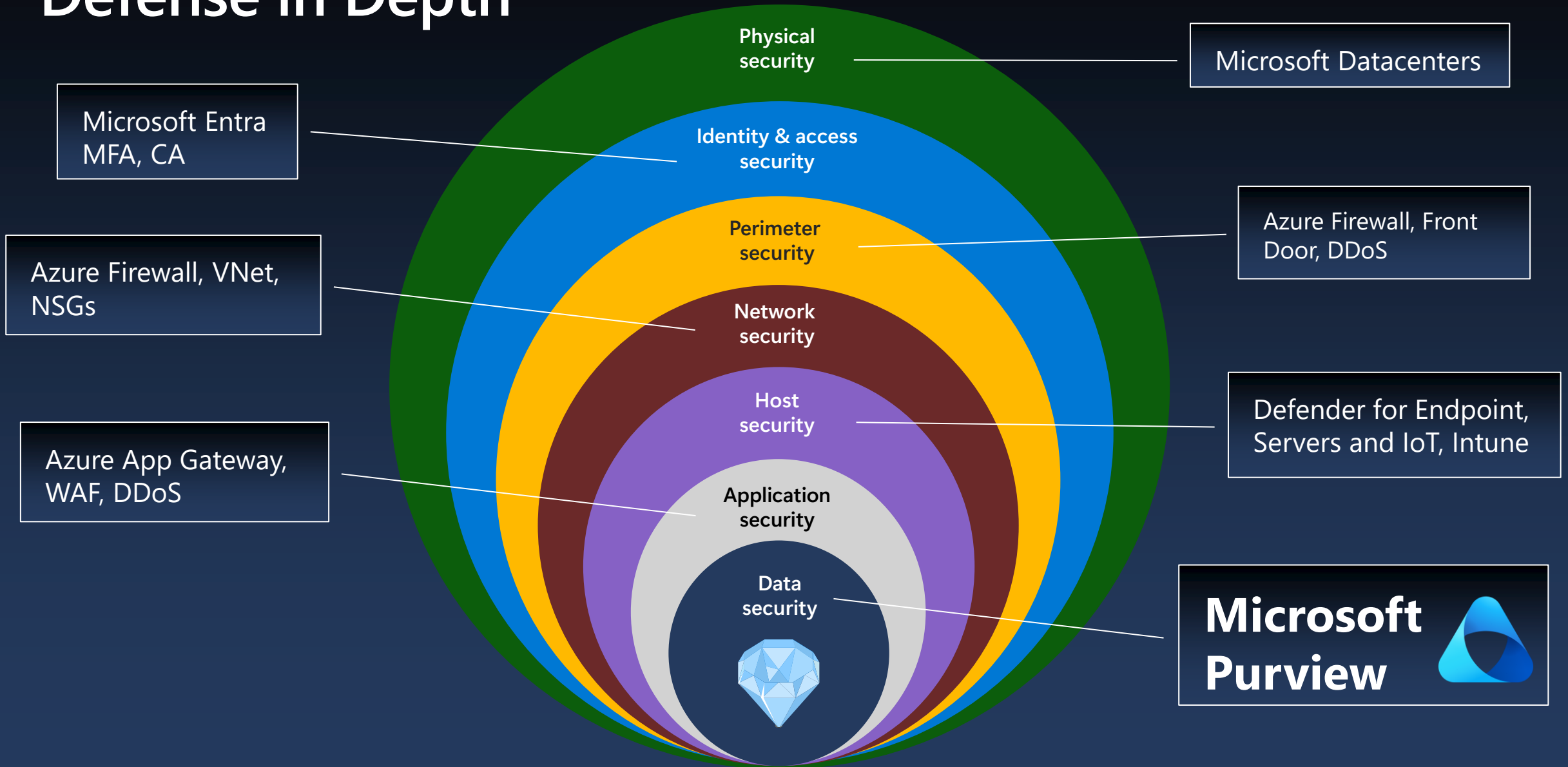


# Data security in Microsoft Purview

Luděk Suk  
Microsoft

# Defense in Depth



# Data security incidents can happen anytime, anywhere

Data at risk of misuse if organization has no visibility into their data estate

## External risks

User falls prey to phishing attack, compromises user credentials



**Data compromise**  
by external threat



## Internal risks

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



**Data theft** by  
malicious insider



User negligently shares sensitive data in generative AI apps



**Data leak** by  
negligent insider



User deletes sensitive information before leaving the organization

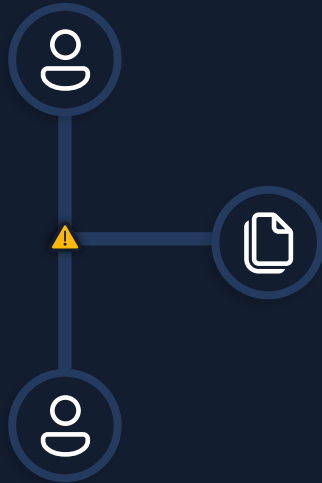


**Data sabotage** by  
disgruntled insider



# To secure their data, organizations need to...

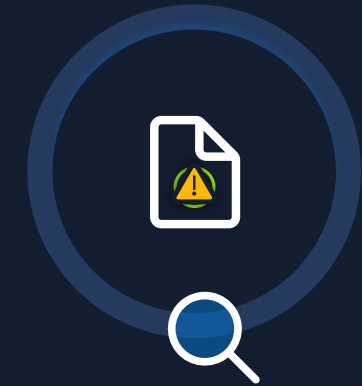
Discover hidden risks  
to data wherever it  
lives or travels



Protect and prevent  
data loss across your  
data estate



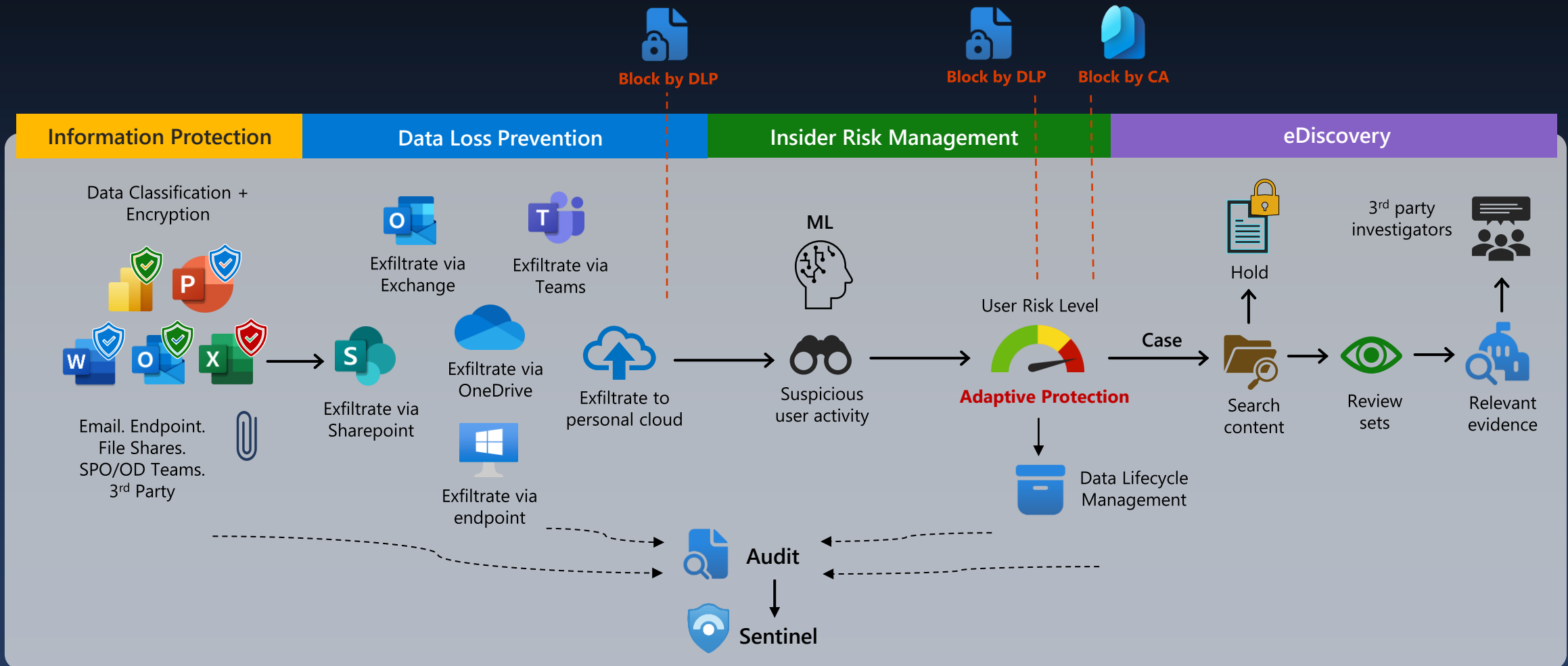
Quickly investigate  
and respond to data  
security incidents



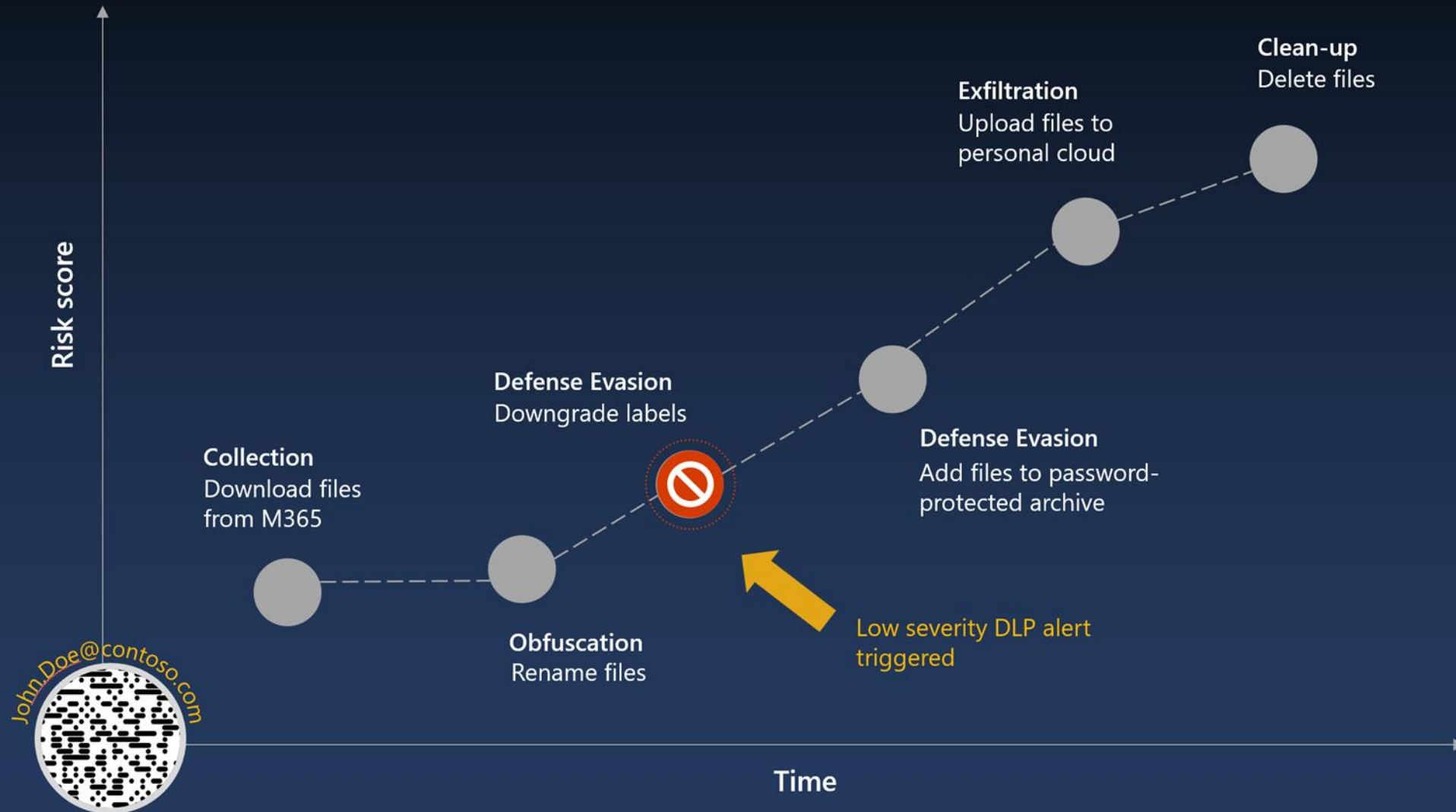
Balance data security and productivity

# Data Exfiltration

## How Purview can help protect, detect and investigate

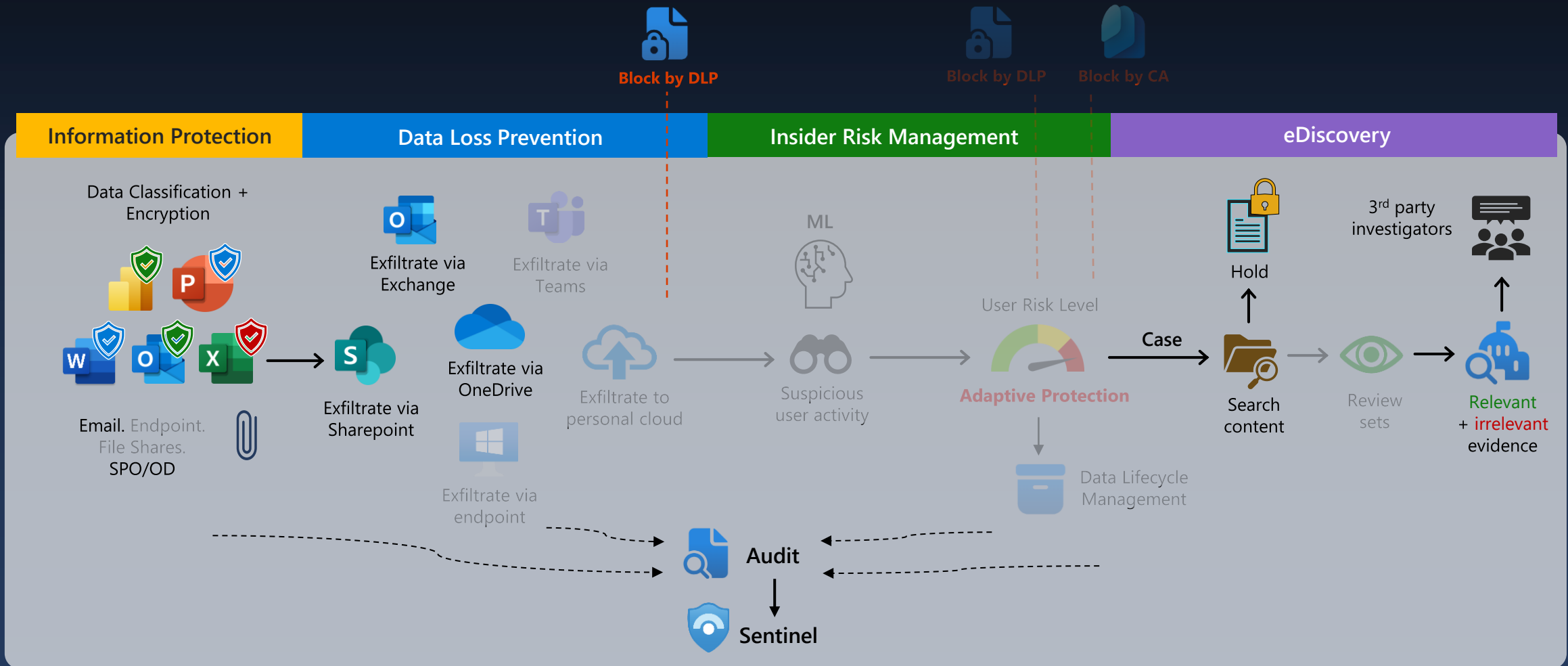


# How threat actors avoid triggering DLP alerts



# Data Exfiltration

## How Purview can help protect, detect and investigate



# Microsoft Purview

Integrated solutions to secure & govern your entire data estate

## DATA SECURITY

Secure data across its lifecycle,  
wherever it lives

Information Protection  
Data Loss Prevention  
Insider Risk Management  
Data Security Posture Management

## 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



# Fortify data 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



Data Loss Prevention

Information Protection

Insider Risk Management

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

# Information Protection



File Home Insert Draw Design Layout References Mailings Review View Help

Comments Editing Share

Undo Paste Font Paragraph Styles Editing Dictate Sensitivity Editor Reuse Files

New Blank Document Open Email Print Preview and Print Check Document Read Aloud Draw Table

**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. OK

---

## Project Obsidian Secret Access Key

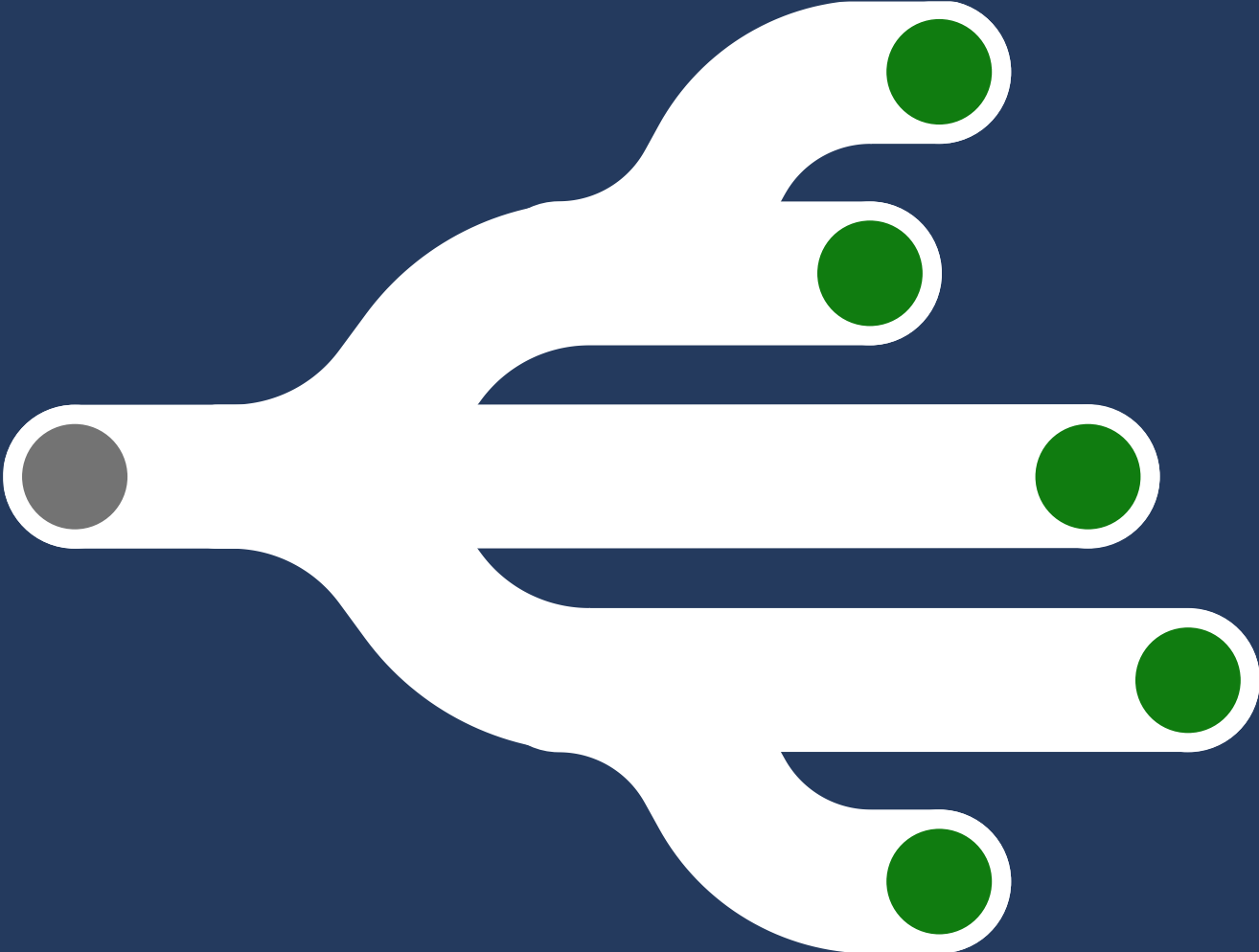
Samples:

```
string AmazonWebServicesSecretToken = "abcdefghijklnopqrst0123456789/+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>
-

# MIP Demo



# Data Loss Prevention



# Bluetooth & devices > Devices

Show notifications to connect using Swift Pair

Connect to supported Bluetooth devices quickly when they're close by and in pairing mode

On 

Browse

Documents > 2210 > 19


Search 19


Organise New folder

| Name   | Date modified    | Type                  | Size  |
|--|------------------|-----------------------|-------|
| <input checked="" type="checkbox"/> KB-L-CER-Word-1640 | 21/10/2022 09:10 | Microsoft Word Doc... | 27 KB |
| <input type="checkbox"/> KB-L-SIR-Word-1               | 21/10/2022 09:12 | Microsoft Word Doc... | 37 KB |
| <input type="checkbox"/> LB-Local-CIR-1                | 21/10/2022 09:27 | Microsoft Word Doc... | 23 KB |

File name: KB-L-CER-Word-1640

## Related support

 Help with Devices




Data Loss Prevention

Your organisation's policy

Transferring KB-L-CER-Word-1640.docx via Bluetooth in this app is not allowed.


Dismiss



Your organization's policy

Copying while Ssn[2305843009213696040].docx is open is not recommended. If you allow it, you'll need to copy again.

Dismiss Allow



Data Loss Prevention

Your organization's policy

Printing while endpointlp.docx is open is not allowed.

Dismiss



Document1 - Word Confidential Alex Wilber AW

File Home Insert Draw Design Layout References Mailings Review View Help

Clipboard Font Paragraph Styles Editing Voice Sensitivity Add-ins Editor Copilot

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:

ChatGPT

New chat

Previous 30 Days

Proj. Obsidian: Digitizing Mesopotamia

Microsoft Purview Data Loss Prevention

Your organization has blocked pasting protected content to unprotected locations.

You tried to paste protected content, which is prohibited by your organization.

OK



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...

Upgrade plan Get GPT-4, DALL-E, and more

Chat | David Kulhánek (Guest) | M x +


https://teams.microsoft.com/v2/

Search (Ctrl+Alt+E) MP

DK David Kulhánek (Guest) Chat Shared +

5:01 PM

Ahoj Davide

 This message was blocked. [What can I do?](#)

Tady je slíbené číslo kreditní karty: VISA 4716 9147 0653 4228

Type a message

Activity Chat Teams Calendar Calls OneDrive Apps

Chat | Martina Petraskova | Micro x +

https://teams.microsoft.com/v2/


Search (Ctrl+Alt+E) DK


MP Martina Petraskova Chat Shared +

Last read

Martina Petraskova 5:01 PM

Ahoj Davide

 This message was blocked due to organization policy. [What's this?](#)



Type a message

Activity Chat Teams



# Insider Risk Management



# (31ac5f2b) Alert: Confidentiality obligation during departure

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 occurred

User activity scatter plot 6 Months 3 Months 1 Month

**(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

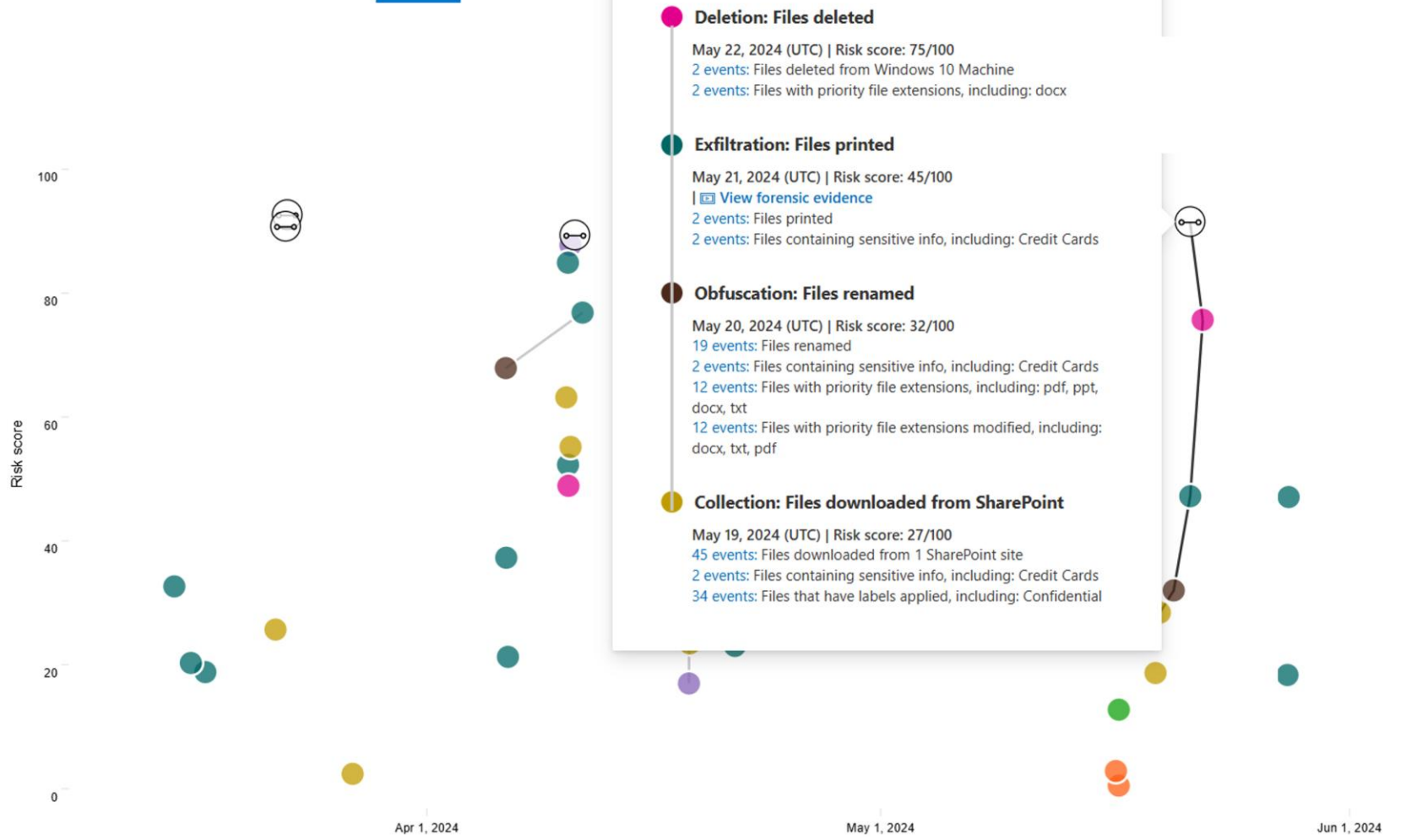
**Collection: Files downloaded from SharePoint**

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

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



## (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

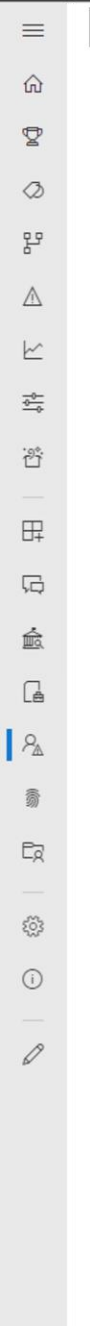
45 events: Files downloaded from 1 SharePoint site

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

34 events: Files that have labels applied, including: Confidential

[an existing case](#) [Dismiss alert](#)

What will these actions do?



# 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

- Home
- Solutions
- Learn
- Settings
- Insider Risk Management
- Information Protection
- Data Loss Prevention
- eDiscovery
- AI Hub (preview)

- Insider Risk Management
- Overview
- Recommendations
- Alerts
- Cases
- Policies
- Users
- Reports
- Forensic Evidence
- Notice templates
- Audit log
- Adaptive Protection**

- Related solutions
- Communication Compliance
  - Information Barriers
  - Data Loss Prevention

# Adaptive Protection

**i** Orgs that are currently using the Microsoft 365 E5 Insider Risk Management add-on will need to upgrade soon to continue using Adaptive Protection. Starting June 2024, Adaptive Protection will start rolling out from public preview to general availability. When roll-out is complete in July 2024, org's using the add-on will have 180 days to upgrade to either Microsoft 365 E5 or Microsoft 365 E5 Compliance. After the 180-day grace period, Adaptive Protection will be turned off for org's that haven't upgraded. [Learn more about accessing adaptive protection](#)

- Dashboard
- Insider risk levels
- Users assigned insider risk levels
- Conditional Access
- Data Loss Prevention

## Adaptive Protection settings

### Adaptive Protection settings

When turned on, Adaptive Protection detects users who match your defined insider risk levels. If those risk levels are included as a condition of a Data Loss Prevention policy or a Conditional Access policy, the Data Loss Prevention policy or the Conditional Access policy will apply the configured actions to that user's activity.

[Learn more about Adaptive Protection](#)

To maintain referential integrity, pseudonymization of usernames (if turned on) isn't preserved for users from Adaptive Protection who have alerts or activity appear outside Insider Risk Management. Actual usernames will appear in related Data Loss Prevention alerts and activity explorer.

If Adaptive Protection is turned off after having been on and active, insider risk levels will stop being assigned to users and shared with DLP and Conditional Access. After turning off, it might take up to 6 hours to stop assigning risk levels to user activity and reset them all.

#### Adaptive Protection

On



Save

# eDiscovery Premium



- Home
- Solutions
  - eDiscovery
    - Overview (preview)
    - Cases (preview)
    - Content Search (preview)
    - Classic eDiscovery
- Related solutions
  - Audit
- Information Protection
- Insider Risk Management
- Data Loss Prevention
- AI Hub (preview)

Cases > Marketing Department Case > Review sets > Tier 1 review set

# Tier 1 review set

Process manager

Saved filter queries

Filters Undo filter query Redo filter query

AND

Select a filter

+ Add filter Add subgroup

1 of 1014 selected

| #  | Subject/Title          | Status | Tag Status | Date (UTC+02:00)        | Sender  |
|----|------------------------|--------|------------|-------------------------|---------|
| 1  | Test Watermark 2       | Ready  | No Tag     | Mar 15, 2024 11:55...   | Petr N  |
| 2  | You've joined the R... | Ready  | No Tag     | Dec 6, 2023 1:29:14...  | Jiri Ur |
| 3  | Osobni udaje - Con...  | Ready  | No Tag     | Oct 10, 2023 2:04:4...  | Lucie 1 |
| 4  | You've joined the L... | Ready  | No Tag     | Apr 29, 2024 1:33:2...  | Legal   |
| 5  | test 2                 | Ready  | No Tag     | Mar 28, 2024 8:38:...   | katerir |
| 6  |                        | Ready  | No Tag     | Apr 3, 2024 3:11:38...  | pavel   |
| 7  | Call (Missed)/Threa... | Ready  | No Tag     | Jul 2, 2024 3:20:47 ... | +1484   |
| 8  |                        | Ready  | No Tag     | Mar 15, 2024 6:55:...   | pavel   |
| 9  | Your digest email      | Ready  | No Tag     | Mar 4, 2024 8:04:1...   | Micros  |
| 10 | Your digest email      | Ready  | No Tag     | Mar 18, 2024 8:47:...   | Micros  |
| 11 | Test                   | Ready  | No Tag     | Mar 28, 2024 10:43:...  | Pavel I |
| 12 | Martina Petraskova...  | Ready  | No Tag     | Nov 6, 2023 11:28:...   | Martin  |

Osobni udaje - Confidential.xlsx

Source Plain text Annotate Metadata

Show pinned metadata

File Home Insert Share Page Layout Formulas Data Search

B2 750610/9644

|   | A               | B           | C         | D | E | F | G | H | I |
|---|-----------------|-------------|-----------|---|---|---|---|---|---|
| 1 | Jmeno           | Rodne cislo | Telefon   |   |   |   |   |   |   |
| 2 | Pavel Beran     | 750610/9644 | 603283799 |   |   |   |   |   |   |
| 3 | Lenka Bechynska | 935322/2076 | 772038263 |   |   |   |   |   |   |
| 4 | Richard Vosyka  | 990423/2140 | 777921820 |   |   |   |   |   |   |

Workbook Statistics Count: 3 Give Feedback to Microsoft 100%

Tag Summarize



# Microsoft Purview and Copilot for Security

Working together to protect your data at machine speed



Identify and prioritize data security risks, understanding intent and context



Accelerate and simplify investigations for compliance admins

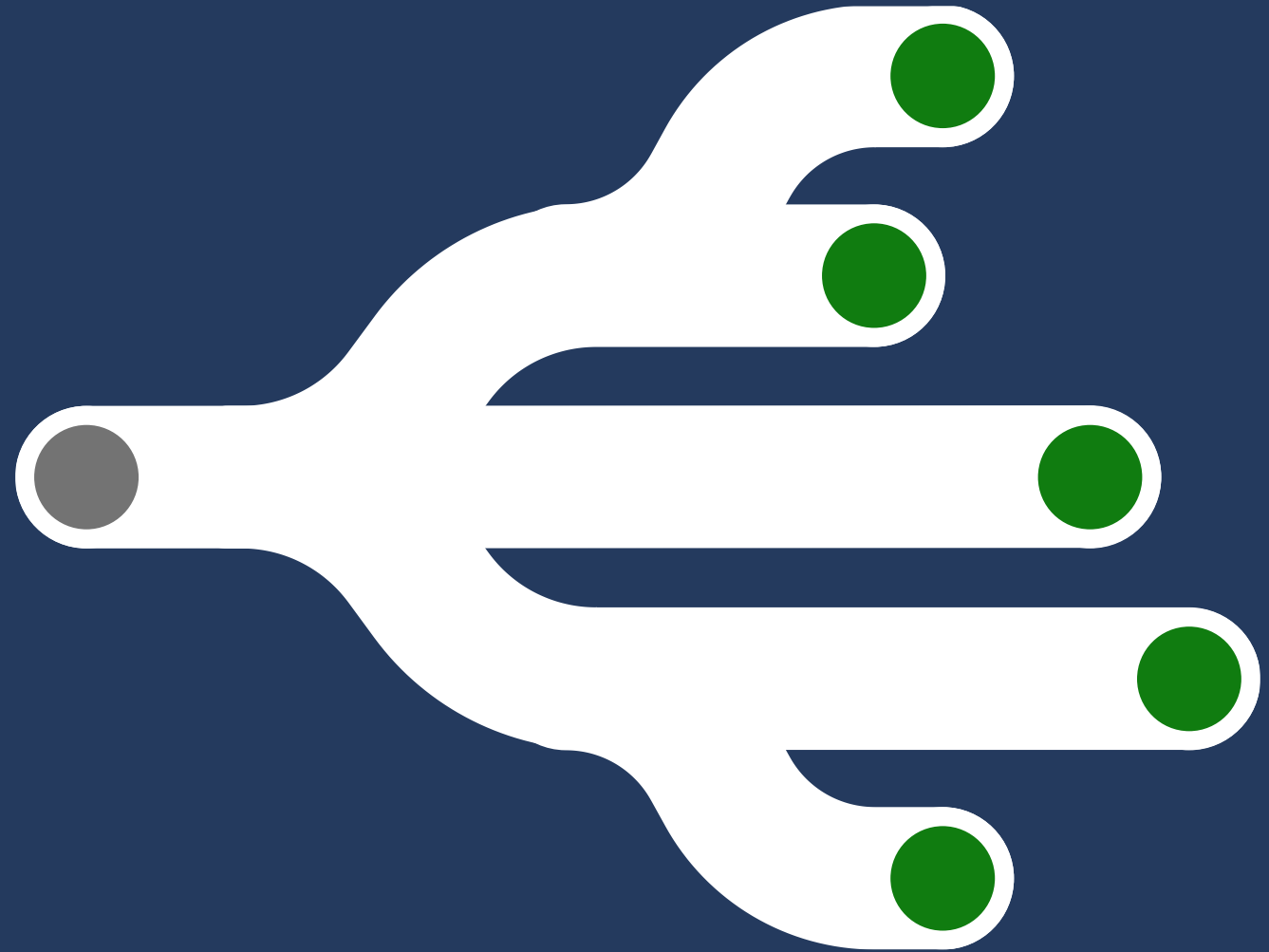


Elevate SOC analysts with intelligence assistance and data insights

## Benefits of AI for security

- > **Efficiency:** Prioritization and automation
- > **Speed:** Ability to faster understand unique cyberthreats
- > **Scale:** Ability to process large volumes of data

# Copilot for Purview Demo





# Alerts

Export Refresh

Filter Reset Filters

Time range: 1/23/2023-2/15/2023 User: Any Alert status: Any Alert severity: Any

- Alert name
- DLP policy match for document 'sales-strategy2023.doc' in SharePoint
- DLP policy match for document 'resume\_345.doc' in SharePoint
- DLP policy match for document 'resume\_345.doc' in SharePoint
- DLP policy match for document 'resume\_345.doc' in SharePoint
- DLP policy match for document 'resume\_345.doc' in SharePoint
- DLP policy match for document 'Q2-Customer Data.xlsx'
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint
- DLP policy match for document 'employee agreement-2.doc' in SharePoint

## Alert: DLP policy match for document 'Q2-Customer Data.xlsx'

Details Events User activity summary

### Alert summary by Security Copilot

The low severity DLP (Data Loss Prevention) alert with ID dl583893090588d-2349d-423085-0909328fbk2948 was generated on 1 Feb 2023 9:03 AM. The alert is currently in "Active" status and is associated with the user jordan.minke@contoso.com. The file involved in this alert is Q2-CustomerData.xlsx, located at <https://contoso.sharepoint.com/sites/Project1>.

The policy responsible for this alert is named "U.S. Financial Data Default Policy" with Policy ID efb767b0-4b45-4948-94b9-b63fb3a773ae. The rule that triggered the alert is "Check Financial Leak" with Rule ID 4bebf68-ab11-4f05-a11a-9cde77323a97.

The file was found to contain Credit Card information which is blocked from sharing under the purview of above policy. Additionally, Jordan Minke is marked as Medium risk level in Insider Risk Management.

AI generated. Verify for accuracy.

Alert ID: 583893090588d-2349d--423085-0909328fbk2948

Alert status: Active

Alert severity: Low

Time detected: 1 Feb 2023 9:03 AM

# (7bbc3040) Data theft by departing users

High severity Risk score: 90/100 Alert created on Sept 30, 2023

Assign Needs review Summarize Dismiss alert Confirm alert

## Activity that generated this alert

**Data infiltration: Files downloaded from unallowed site**  
87/100 High severity | Sept 28, 2023 (UTC)  
12 events: Files downloaded from 1 unallowed site  
8 events: Files that have labels applied, including: Project Alpha  
Factors that impacted risk score  
Includes unallowed domains (1 event)

Reduce alerts for this activity

## Triggering event

Sept 25, 2023 (UTC)  
An HR connector imported a resignation date for this user.

## User details

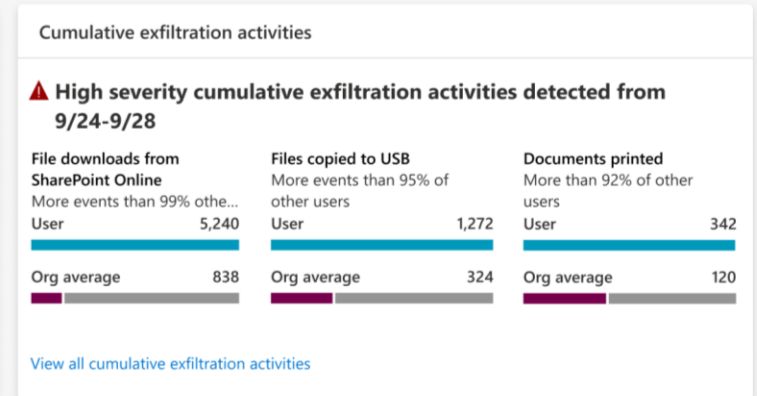
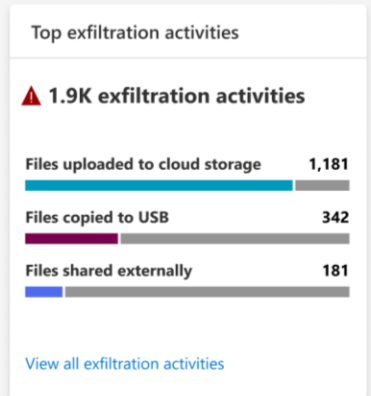
jdoh@ediscodf.onmicrosoft.com  
[View all details](#)

## User alert history

Last 30 days  
Data theft for departing employees 3 alerts  
Sensitive data leaks 1 alert  
Security violations 2 alerts

Summary Activity explorer User activity Forensic evidence

## Risk factors



### Sequences of activity

No sequences detected

### Unusual activity for this user

▲ 3 patterns of unusual activities

### Priority content

No priority content detected

### Unallowed domains

▲ 4 unallowed domains

### Security Copilot

#### Alert summary

The alert with alert Id: 7bbc3040 is a high severity Insider Risk Management alert involving Jane Doe that was detected on September 30, 2023. The policy "Data theft by departing users" was triggered when the user submitted their resignation on September 28, 2023. The user was involved in 2 events where files containing sensitivity labels were downloaded from an unallowed site that led to this alert being generated. The alert is currently in "Needs review" state.

AI generated. Verify for accuracy.

Cases > Contoso vs. Robinson > Searches > Fabrikam production

### Fabrikam production Complete

Version: Review 1 (Current) (Today, 2:00 PM)

Query: ((i.e. OR ie OR "internet explorer" OR "o'hare") AND ("background image" OR redraw OR... [Show query](#))

Query Statistics Sample results Full item results **Review results**

|                                     | Analytics | Actions                          | Tag files | 1 of 102 selected    |
|-------------------------------------|-----------|----------------------------------|-----------|----------------------|
| <input type="checkbox"/>            | >         | Subject                          | Status    | Date                 |
| <input type="checkbox"/>            | >         | Re: pricing                      | Ready     | 28 Mar 2023 8:01 PM  |
| <input type="checkbox"/>            | >         | I have tried to rectify this ... | Ready     | 28 Mar 2023 8:01 PM  |
| <input checked="" type="checkbox"/> | >         | Megan Bowen please rev...        | Ready     | 28 Mar 2023 12:05 AM |
| <input type="checkbox"/>            | >         | loan offer letter_2238417...     | Ready     | 28 Mar 2023 12:56 PM |
| <input type="checkbox"/>            | >         | Re: FW: 2002 Plan Lay            | Ready     | 3 Oct 2023 2:48 AM   |
| <input type="checkbox"/>            | >         | 84669-IC-FINDPHOTOS.png          | Ready     | 5 Jun 2023 7:45 PM   |
| <input type="checkbox"/>            | >         | Site Assets                      | Ready     | 29 Mar 2023 1:40 PM  |
| <input type="checkbox"/>            | >         | Proposal for Seattle Expansio... | Ready     | 21 Sep 2023 6:25 PM  |
| <input type="checkbox"/>            | >         | 494942.jpg                       | Ready     | 29 Jun 2023 5:25 AM  |
| <input type="checkbox"/>            | >         | Corporate Charge questions       | Ready     | 30 Sep 2016 9:07 AM  |
| <input type="checkbox"/>            | >         | The Leadership Team met last...  | Ready     | 26 Apr 2023 7:12 AM  |
| <input type="checkbox"/>            | >         | X1050 Launch Team.xlsx           | Ready     | 28 Mar 2023 8:01 AM  |

#### Megan Bowen please review the contract

Native view Plain view Metadata

- Megan Bowen** <Mbowen@Mm365x809305.onMicrosoft.c...> 9/14/2021 1:48 PM  
Please review the contract with Adatum. We need to approve the RFP by 4:00. Thanks!
- Nestor Wilke** <NestorW@Mm365x809305.onMicrosoft.com> 9/14/2021 1:48 PM  
@Isaiah Langer That approval is being pushed by 48 hours. We don't have the text matrix set up yet.
- Isaiah Langer** <IsaiahL@Mm365x809305.onMicrosoft.com> 9/14/2021 1:48 PM  
@MeganBowen FYI
- Megan Bowen** <Mbowen@Mm365x809305.onMicrosoft.com> 9/14/2021 1:48 PM  
Let me get the document name for you
- Megan Bowen** <Mbowen@Mm365x809305.onMicrosoft.com> 9/14/2021 1:48 PM  
PricingGuidelinesforX1050.doc

#### Security Copilot

**Message summary**

The conversation discusses the contract with Adatum, approval delay, and a helpful document.

**Key takeaways:**

1. The approval for the RFP with Adatum has been delayed by 48 hours due to the text matrix not being set up yet.
2. Megan Bowen has requested that the contract with Adatum be reviewed and approved by 4:00.
3. Megan Bowen has shared a document called "Pricing Guidelines for X1050" that may be helpful for everyone.

AI generated. Verify for accuracy.

What are the key topics and related timelines?  
Who are the key people mentioned here?  
Are there any related data items mentioned here?  
Ask a question about this message...

# Microsoft Security Partners portal

## Product and solution presentations

- [Secure data in the Age of AI with Microsoft Purview overview](#) 🔒
- [Data security customer pitch deck](#) 🔒
- [Microsoft Purview Data Governance product deck](#) 🔒
- [Microsoft Purview Data Lifecycle Management overview deck](#) 🔒
- [Microsoft Purview Records Management overview deck](#) 🔒
- [Microsoft Purview Information Protection overview deck](#) 🔒
- [Microsoft Purview Data Loss Prevention overview deck](#) 🔒

<https://securitypartners.transform.microsoft.com>

# M365 E5 Compliance promo offer for M365 Copilot

## Promotion summary

We're offering 50 percent off E5 Compliance PUPM for every seat of Microsoft 365 Copilot purchased. This offer can be applied retroactively to customers who have already purchased M365 Copilot but don't have E5 Compliance.

## Duration

February 1, 2025 to February 1, 2026

## Geography

Worldwide

## Promo type

New commerce, Volume Licensing (VL), Enterprise Agreement (EA), Cloud Solution Provider (CSP)

## Products

This offer applies to E5 Compliance. The customer must also have M365 Copilot, as well as the standard prerequisites required for attaching E5 Compliance.

## Discount percent and discount description

50 percent off each seat of E5 Compliance for each seat of M365 Copilot sold

## Customer eligibility

All commercial customers

See the latest [Operations Promo Guide Excel](#) file for the latest list of promotion IDs and product SKU IDs for all new commerce promotions. The new commerce promotion details tab in the Excel file allows partners to filter by promotion type.

## End customer value prop

The promo aims to ensure that each M365 Copilot is safely secured with our Hero Data Security product.

## Partner value prop

Partners can not only increase the size of M365 Copilot deals but can also go back to previously closed M365 Copilot deals and solicit the new discount opportunity.

## How it works

The promo has both modern partner-led and customer SKUs which are available in Partner Center.

## Next steps/Learn more

- [See the FAQ](#) for more information.
- If you have additional questions about this promotion, refer to the [Global Readiness Promo Guide](#).





# Microsoft Partner Security Day

Praha, 11. 2. 2025

