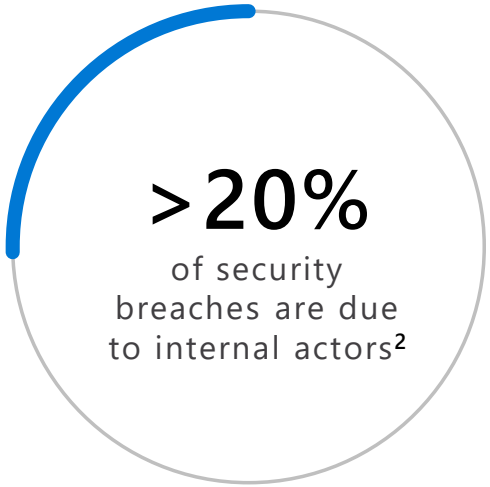
Microsoft

Ein neuer Ansatz zur Erkennung von Insiderrisken und Verhinderung von Datenabfluss

Bernd Vellguth
Technical Specialist
Microsoft
berndv@microsoft.com
+49-89-3176-3893

Insider risks are a universal and growing concern

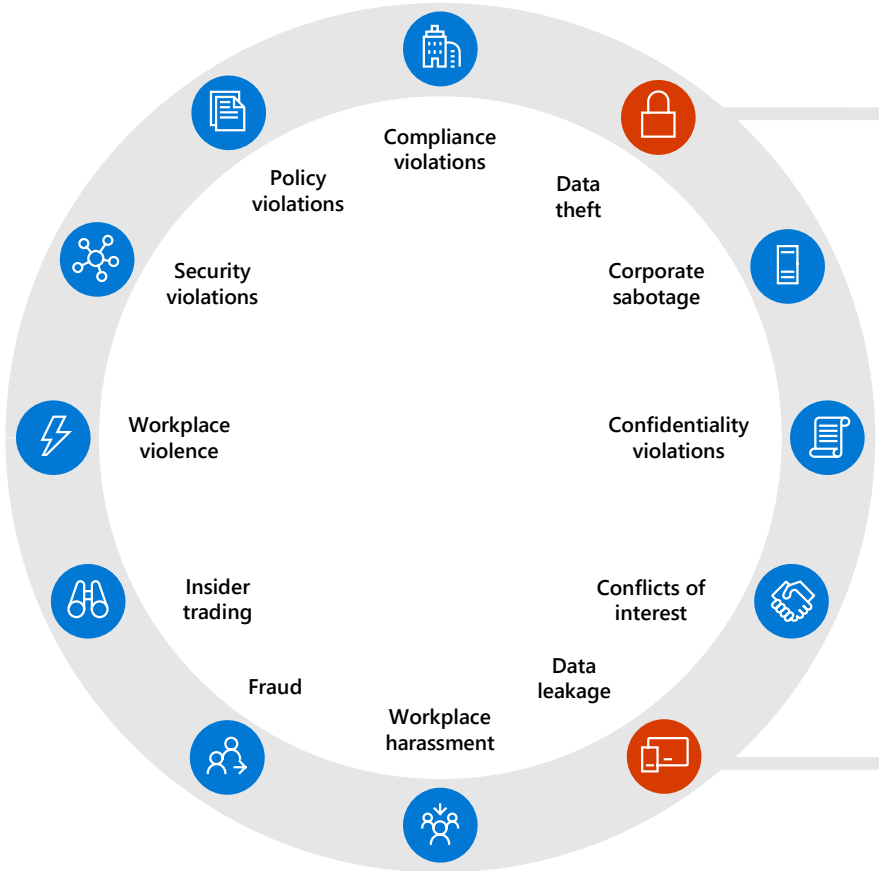


$15.4 million

total average annual cost of activities to resolve insider threats[3]

Sources:
1. Insider Risk Management, Microsoft Market Research, January 2021.
2. Verizon 2021 Data Breach Investigations Report
3. 2022 Cost of Insider Threats: Global Report, The Ponemon Institute

Organizations face a broad range of risks from insiders

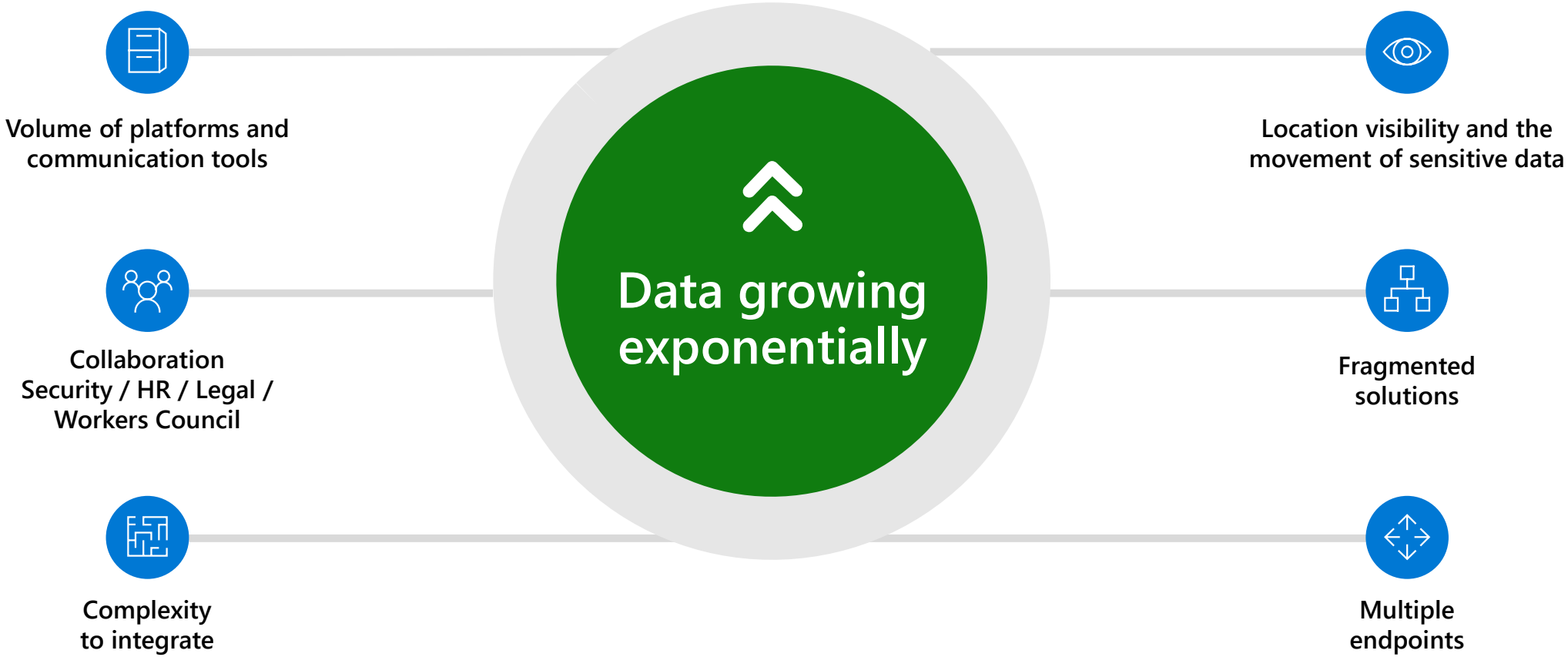


Certain risks are more prevalent, with significant negative impacts.

Data theft by departing employees

Data leakage, both malicious and inadvertent

Insider risks can be difficult to identify and manage



Insider Risk Management

Intelligently detect and mitigate the most critical risks

Privacy

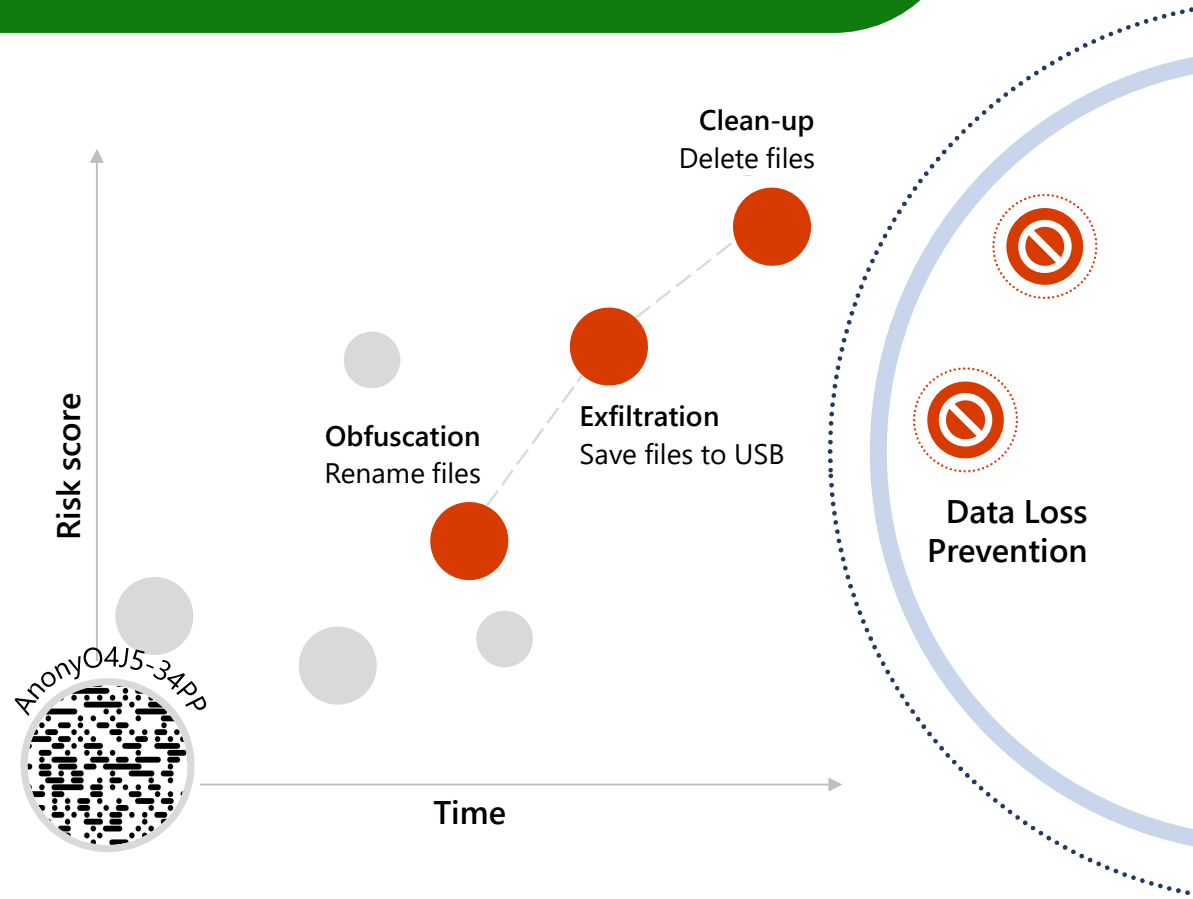
Protect user trust and build a holistic insider risk program with **pseudonymization** and strong privacy controls.

Simplicity

Identify hidden risks with 100+ **built-in machine-learning models** and indicators, requiring **no endpoint agents**.

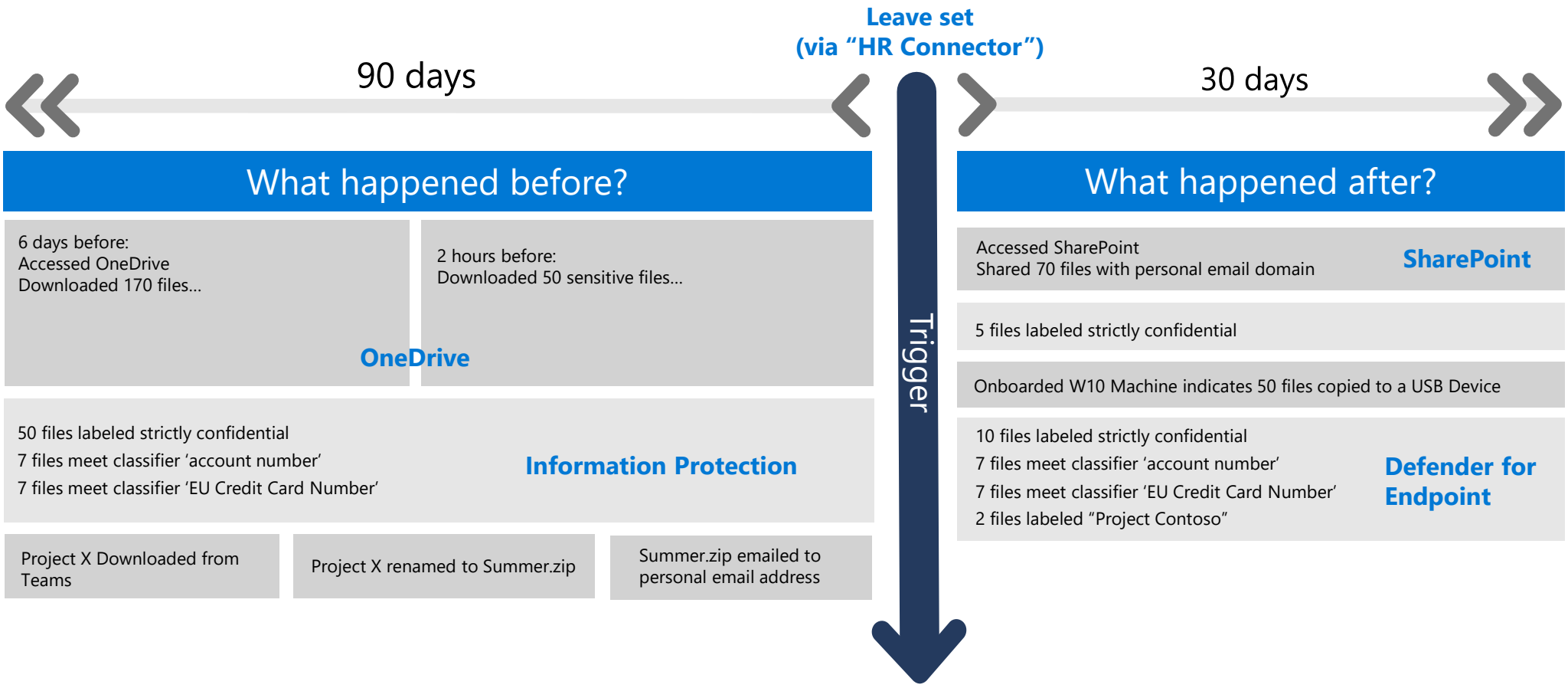
Acceleration

Expedite mitigation with enriched investigations and **Adaptive Protection** that enforce DLP controls dynamically.



Scenario: how Insider Risk Management works

An employee resigns ➔ HR enters resignation date in HR tool…



Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies

Solutions
Catalog
Content search
Communication compliance
Data loss prevention
eDiscovery
Information protection
Information Barriers
Insider risk management
Privacy management

Settings
More resources
Customize navigation

Case 449: Potential IP theft

Active Low 25 risk score

Resolve case Case actions

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

Filter: Show: All user activity

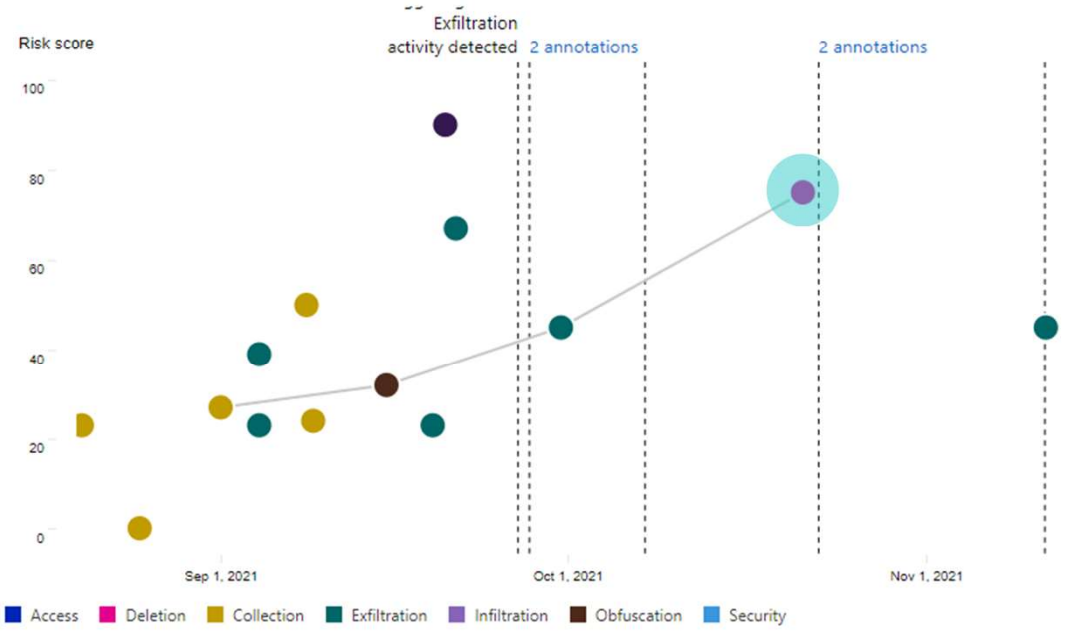
Sort by: Date occured

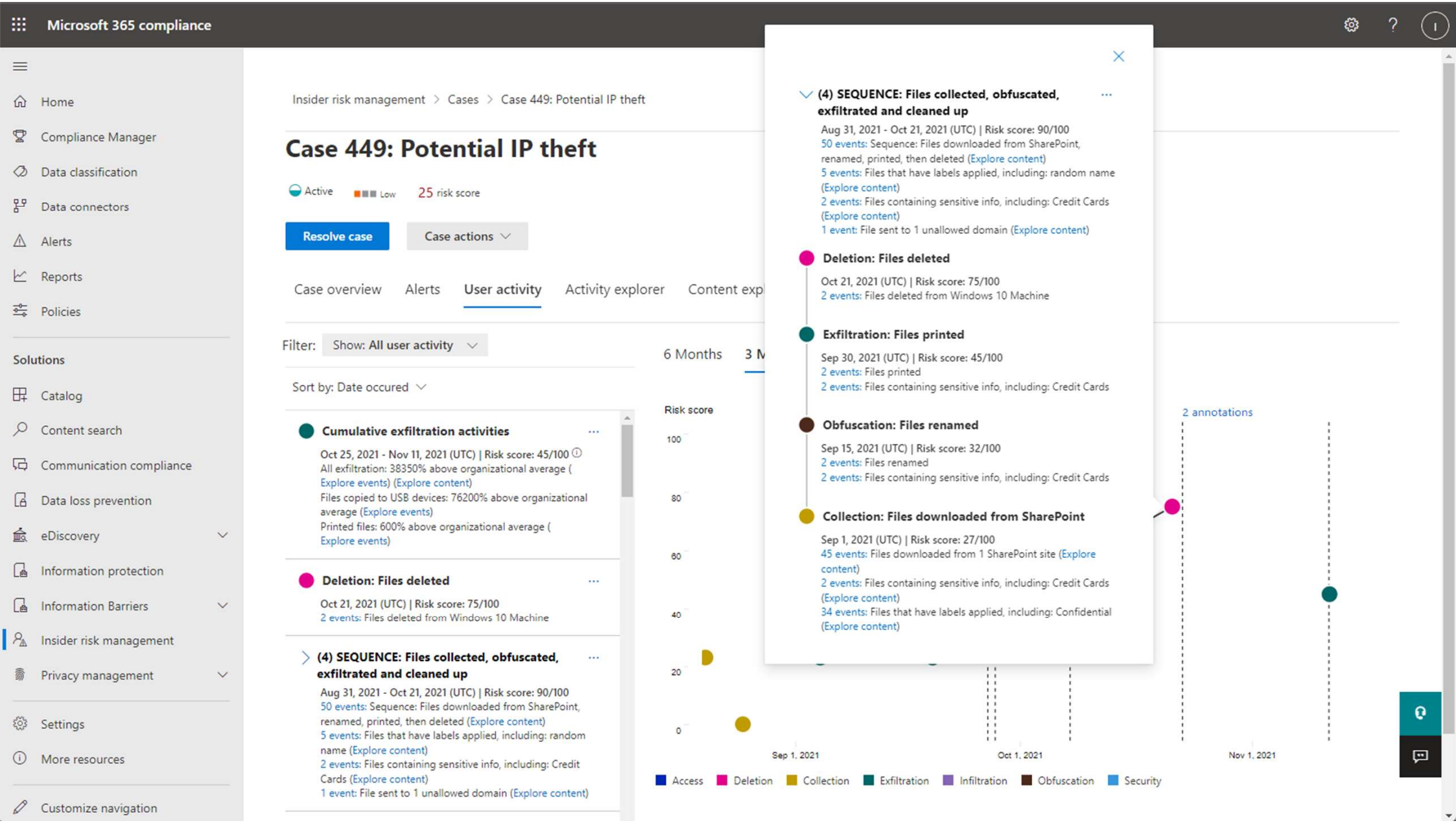
Cumulative exfiltration activities
Oct 25, 2021 - Nov 11, 2021 (UTC) | Risk score: 45/100
All exfiltration: 38350% above organizational average (Explore events) (Explore content)
Files copied to USB devices: 76200% above organizational average (Explore events)
Printed files: 600% above organizational average (Explore events)

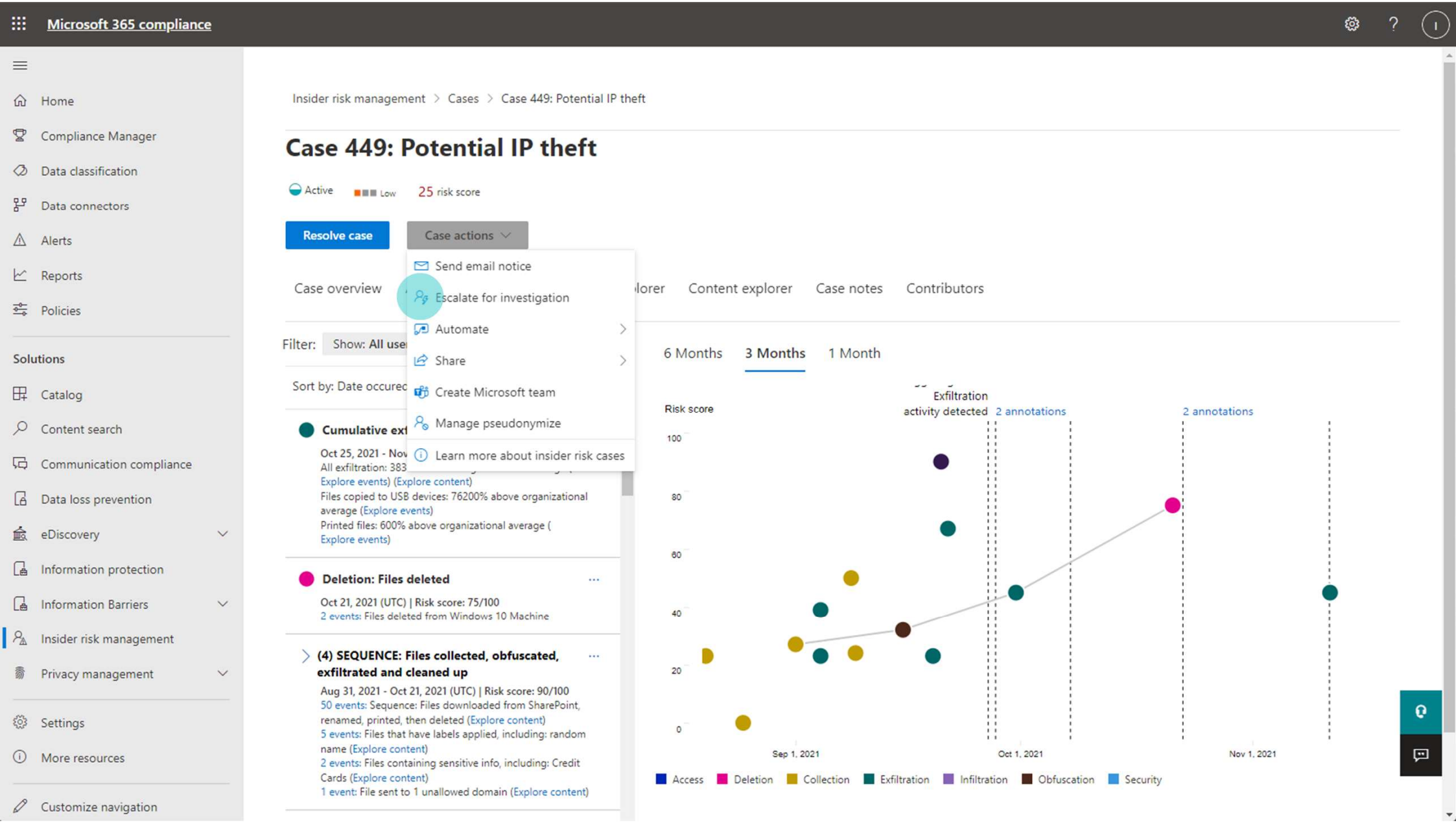
Deletion: Files deleted
Oct 21, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine

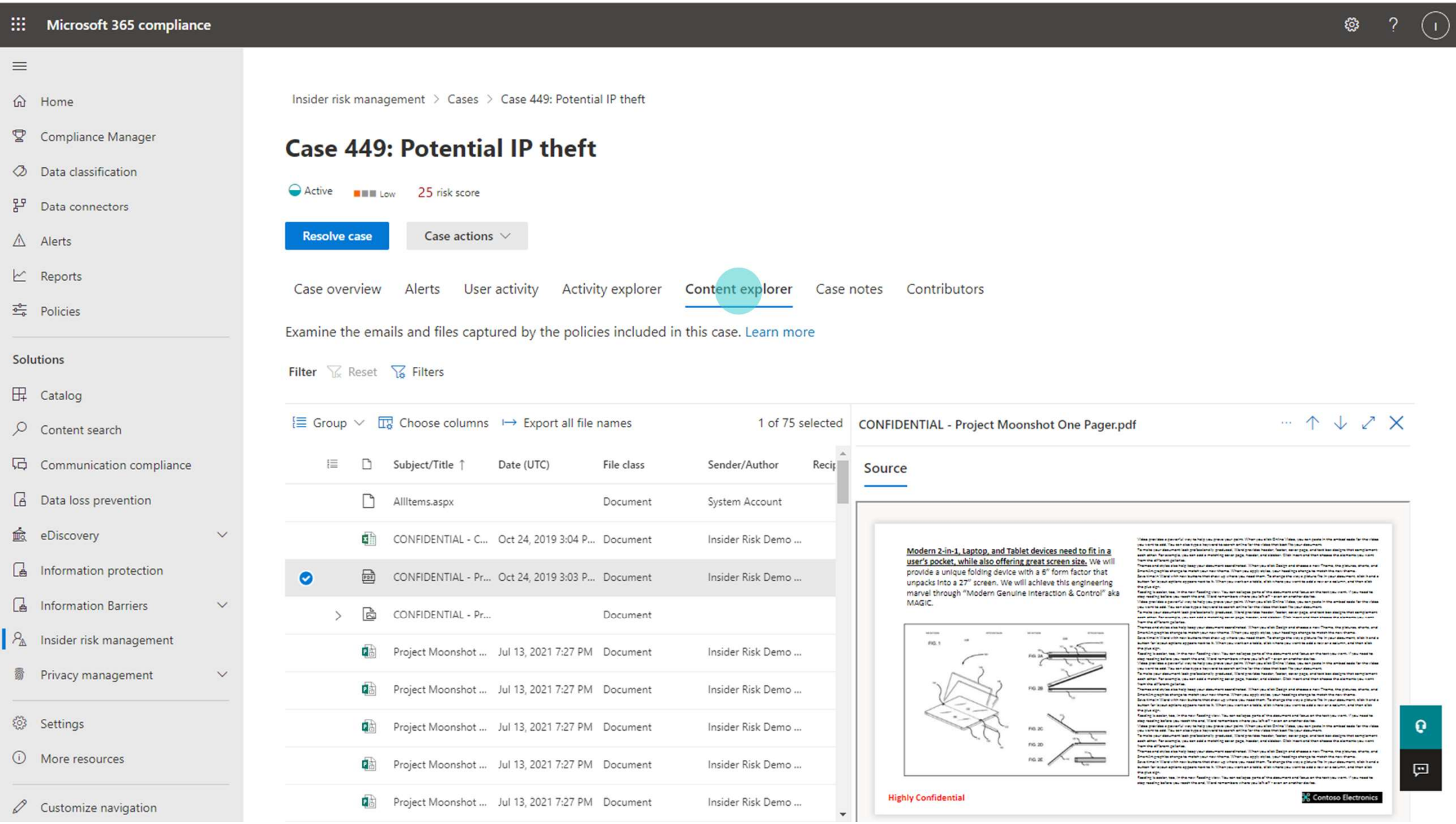
(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
Aug 31, 2021 - Oct 21, 2021 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted (Explore content)
5 events: Files that have labels applied, including: random name (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
1 event: File sent to 1 unallowed domain (Explore content)

6 Months 3 Months 1 Month

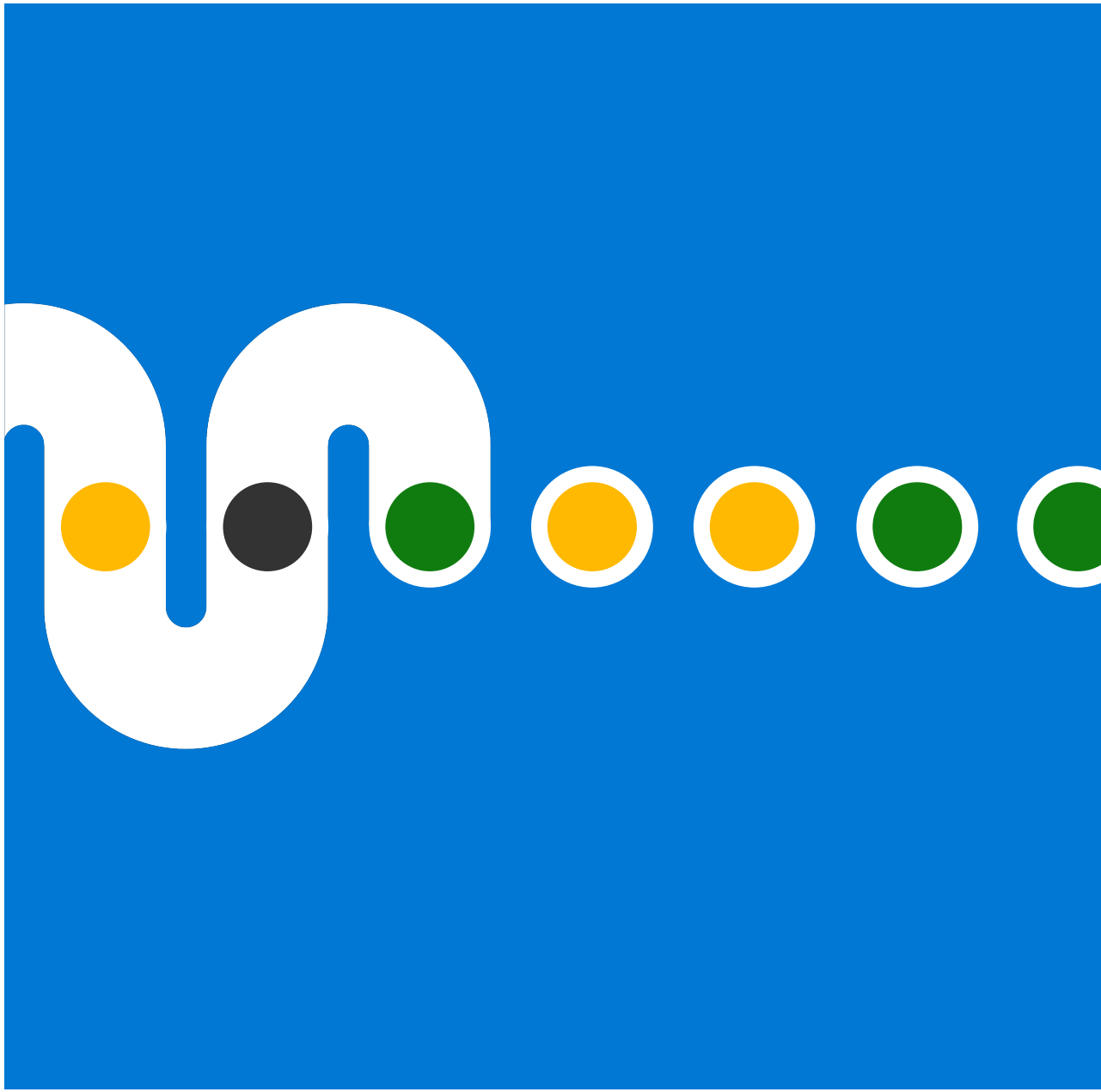



Microsoft 365 compliance
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Solutions
Catalog
Content search
Communication compliance
Data loss prevention
eDiscovery
Information protection
Information Barriers
Insider risk management
Privacy management
Settings
More resources
Customize navigation
Insider risk management > Cases > Case 449: Potential IP theft
Case 449: Potential IP theft
Active
Low
25 risk score
Resolve case
Case actions
Case overview
Alerts
User activity
Activity explorer
Content exp
Filter:
Show: All user activity
Sort by: Date occured
Cumulative exfiltration activities
Oct 25, 2021 - Nov 11, 2021 (UTC) | Risk score: 45/100
All exfiltration: 38350% above organizational average (Explore events) (Explore content)
Files copied to USB devices: 76200% above organizational average (Explore events)
Printed files: 600% above organizational average (Explore events)
Deletion: Files deleted
Oct 21, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine
(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
Aug 31, 2021 - Oct 21, 2021 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted (Explore content)
5 events: Files that have labels applied, including: random name (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
1 event: File sent to 1 unallowed domain (Explore content)
(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
Aug 31, 2021 - Oct 21, 2021 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted (Explore content)
5 events: Files that have labels applied, including: random name (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
1 event: File sent to 1 unallowed domain (Explore content)
Deletion: Files deleted
Oct 21, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine
Exfiltration: Files printed
Sep 30, 2021 (UTC) | Risk score: 45/100
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards
Obfuscation: Files renamed
Sep 15, 2021 (UTC) | Risk score: 32/100
2 events: Files renamed
2 events: Files containing sensitive info, including: Credit Cards
Collection: Files downloaded from SharePoint
Sep 1, 2021 (UTC) | Risk score: 27/100
45 events: Files downloaded from 1 SharePoint site (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
34 events: Files that have labels applied, including: Confidential (Explore content)
6 Months
3 M
Risk score
2 annotations
100
80
60
40
20
0
Sep 1, 2021
Oct 1, 2021
Nov 1, 2021
Access
Deletion
Collection
Exfiltration
Infiltration
Obfuscation
Security


Microsoft 365 compliance
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Solutions
Catalog
Content search
Communication compliance
Data loss prevention
eDiscovery
Information protection
Information Barriers
Insider risk management
Privacy management
Settings
More resources
Customize navigation
Insider risk management > Cases > Case 449: Potential IP theft
Case 449: Potential IP theft
Active
Low
25 risk score
Resolve case
Case actions
Send email notice
Escalate for investigation
Automate
Share
Create Microsoft team
Manage pseudonymize
Learn more about insider risk cases
Case overview
Content explorer
Case notes
Contributors
Filter:
Sort by: Date occured
Cumulative ext
Oct 25, 2021 - Nov
All exfiltration: 383
Explore events) (Explore content)
Files copied to USB devices: 76200% above organizational average (Explore events)
Printed files: 600% above organizational average (
Explore events)
Deletion: Files deleted
Oct 21, 2021 (UTC) | Risk score: 75/100
2 events: Files deleted from Windows 10 Machine
(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up
Aug 31, 2021 - Oct 21, 2021 (UTC) | Risk score: 90/100
50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted (Explore content)
5 events: Files that have labels applied, including: random name (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
1 event: File sent to 1 unallowed domain (Explore content)
6 Months
3 Months
1 Month
Risk score
Exfiltration activity detected
2 annotations
2 annotations
100
80
60
40
20
0
Sep 1, 2021
Oct 1, 2021
Nov 1, 2021
Access
Deletion
Collection
Exfiltration
Infiltration
Obfuscation
Security


Microsoft 365 compliance
Home
Compliance Manager
Data classification
Data connectors
Alerts
Reports
Policies
Solutions
Catalog
Content search
Communication compliance
Data loss prevention
eDiscovery
Information protection
Information Barriers
Insider risk management
Privacy management
Settings
More resources
Customize navigation
Insider risk management > Cases > Case 449: Potential IP theft
Case 449: Potential IP theft
Active
Low
25 risk score
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
Filter
Reset
Filters
Group
Choose columns
Export all file names
1 of 75 selected
Subject/Title
Date (UTC)
File class
Sender/Author
AllItems.aspx
Document
System Account
CONFIDENTIAL - C...
Oct 24, 2019 3:04 P...
Document
Insider Risk Demo ...
CONFIDENTIAL - Pr...
Oct 24, 2019 3:03 P...
Document
Insider Risk Demo ...
CONFIDENTIAL - Pr...
Document
Project Moonshot ...
Jul 13, 2021 7:27 PM
Document
Insider Risk Demo ...
CONFIDENTIAL - Project Moonshot One Pager.pdf
Source
Modern 2-in-1, Laptop, and Tablet devices need to fit in a user's pocket, while also offering great screen size. We will provide a unique folding device with a 6" form factor that unpacks into a 27" screen. We will achieve this engineering marvel through "Modern Genuine Interaction & Control" aka MAGIC.
Highly Confidential
Contoso Electronics

Best Practices and Learnings from Customer References



Stakeholders and Process

Legal+Compliance

Business Unit

Data Privacy Officer

Human Resources

Workers Council

Security

Legal+Compliance Legal actions and regulatory compliance

Business Unit of the user Impact on the business

Data Privacy Officer Privacy concerns

Human Resources Corporate policies, healthy workplace

Workers Council Employee privacy concerns

Security Risk management, intellectual property protection

Security

Policy Definition

Agreement with all stakeholders on:
- Users in scope
- policies + triggers
- prioritized content
- prioritized uses

should be activated.

No alert

System does not create any analytics related to a specific user.

Alert

Goal: filter out obvious false positives
User identity undisclosed (pseudonymization on).
Only metadata of content visible.

Case

Goal: look at details and history of user behavior; collaborative conclusion about relevance and severity of the case. Filtering out remaining false positives.

Investigation

Goal: preserve evidence and decide which disciplinary actions are taken against confirmed misbehavior of the user.
User identity disclosed.
Full visibility about content involved.

Lessons Learned

Goal: what needs to be changed to prevent the next similar case? Refine policies. What went well and what needs to be improved?

How to Run an Insider Risk Management Program

Key Questions

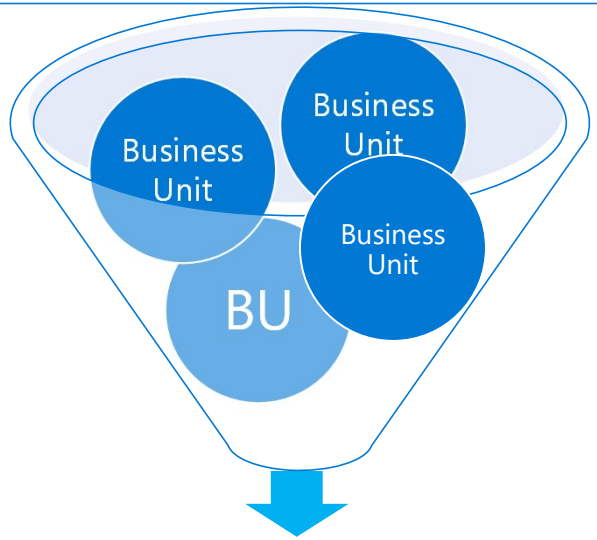
- **What are the major risks?** ➔ Definition of risk scenarios and priority use cases.
- **What do you want to protect?** ➔ What are my critical assets? Which groups/departments are in focus? Which region is in scope?
- **Who are the key stakeholders?** ➔ Ensure that key stakeholders are involved and commit support in the program. Ensure required approvals to proceed.

Key Challenges

- Each business unit needs to understand their specific data risks
- Alignment with **HR, legal/compliance** and **workers council**
- **Identifying critical assets**/priority groups
- Insider risks can't be solved by **tools** alone
- Define what is a **"malicious"** behavior and what is a risky user?
- Tweaking policies to **reduce false positives**
- Definition of **processes** and **responsibilities** of involved parties

Insider Risk Management results of a pilot over 7 months

Pilot with 13.500 Users in 4 business units



2500 Alerts

10 confirmed cases

Prime Example (Leaver)
Employee resigned and moved to a competitor.
Copied 2500 files (140 GB) which were classified as company confidential to external hard drive. User had access to 23000 such classified files.
Strategy, concepts and methodology information from the business area.
Interview conducted; File transfer was admitted. No cooperation to return the data (storage device supposedly destroyed). Criminal notification made. Competitor was informed about the case.

Microsoft Security

Vision for Adaptive Protection: **Balance productivity with security**

CONTROL PLANES	ADAPTIVE CONTROLS
Feb 2023	**Purview: Data Loss Prevention** Warning, block & override, block
Dec 2023	**Entra: Access Management – Conditional Access** Block access and require terms of use acceptance
April 2024	**Entra: Identity Management – Entra ID Governance** Access review for high risk users
May 2024	**Purview: Data Lifecycle Management** Proactive retention when users might sabotage content
	Intune: Application Management – Intune MAM Warn, block or wipe managed apps
	Further integrations to be announced soon

Zusammenfassung

1. Insiderrisiken werden oft vernachlässigt, obwohl sie wichtig sind.
2. Man kann eine gute Balance finden zwischen Privatsphäre der Mitarbeitenden und dem berechtigten Interesse der Organisation, ihren Wettbewerbsvorsprung zu sichern.
3. Vorab die Regeln zu definieren, nach denen man handeln wird und wer beteiligt wird, ist unerlässlich für schnelles Eingreifen.
4. So kann nicht nur IP-Diebstahl, sondern auch Sabotage eingedämmt oder verhindert werden.

Getting started with Insider Risk Management

Try it: Start a Free Trial of Microsoft Purview: https://learn.microsoft.com/en-us/purview/purview-trial

Read more: Insider Risk Marketing Page: http://aka.ms/insiderriskblog
Insider Risk in the online documentation: https://aka.ms/irmanalytics

Get in touch: **Microsoft ist auf dem**
ZRK-Koop-Partner Stand, Nr. 17-20

How to run Insider Risk Management

1. Start with a limited scope (users, business) for easier / quicker approval processes
2. Align with each business unit, IT, human resources, cybersecurity, data protection, workers council and upper management
3. Start with small number of policies and use standard templates to get quick results. Turn almost all available risk indicators on.
4. Identification of priority groups and target locations to reduce false positives
5. Align end to end process and responsibilities
6. Run a Proof of Concept
    - Improve the alert triage to determine the severity of the thread and if it's impactful enough to be escalated
    - Policy re-adjustment in accordance to the risk levels
    - Run end to end process (alerting, monitoring, investigation and disciplinary actions)
7. Present results to upper management and get decision for broader rollout

Run a Successful IRM Implementation

Key takeaways from reference customers

- IP theft is the most relevant use case. And leavers represent nearly 50% of the risky users.
  - Some DPOs find the leaver scenario problematic as a trigger because leaving is a legitimate process. But: in anonymous studies, more than 50% of leavers admit that they are taking company content with them. That can be a justification to enable it nonetheless.
  - Some customers turn IRM on when they sell parts of the business (spin-off).
- Finance, consulting, product development, technology projects are the most affected areas for data leakage.
- Insiders do not follow the same pattern. Cases are not country, age, job function or gender specific.
- A user risk behavior can be understood differently depending on the culture, country and business.
- Data privacy is key to get approval from workers council to be able to conduct investigations.
- When you catch insiders, they do argue that they made copies only as personal backups. ➔ Make sure that your policies clearly states that you don't allow personal backups and communicate that regularly.
- Advanced audit log with longer history of the user activities is helpful for long running investigations (more than 90 days).
- Getting an agreement from legal, compliance and workers council can take some time.
- You can start with Insider Risk Management even without labeling and data loss prevention but it becomes sharper when you have content classified and DLP policies enabled.

Licensing Insider Risk Management

Every person, who is part of a policy, needs a license.

For Information Workers:	**Insider Risk Management E5 (list price starts at $12 per user per month or Compliance E5 or Microsoft 365 E5**
For Frontline Workers:	**F1/F3 + F5 Compliance or F1/F3 + F5 Security+Compliance**