

Microsoft Purview Insider Risk Management

Intelligently detect and mitigate
critical risks



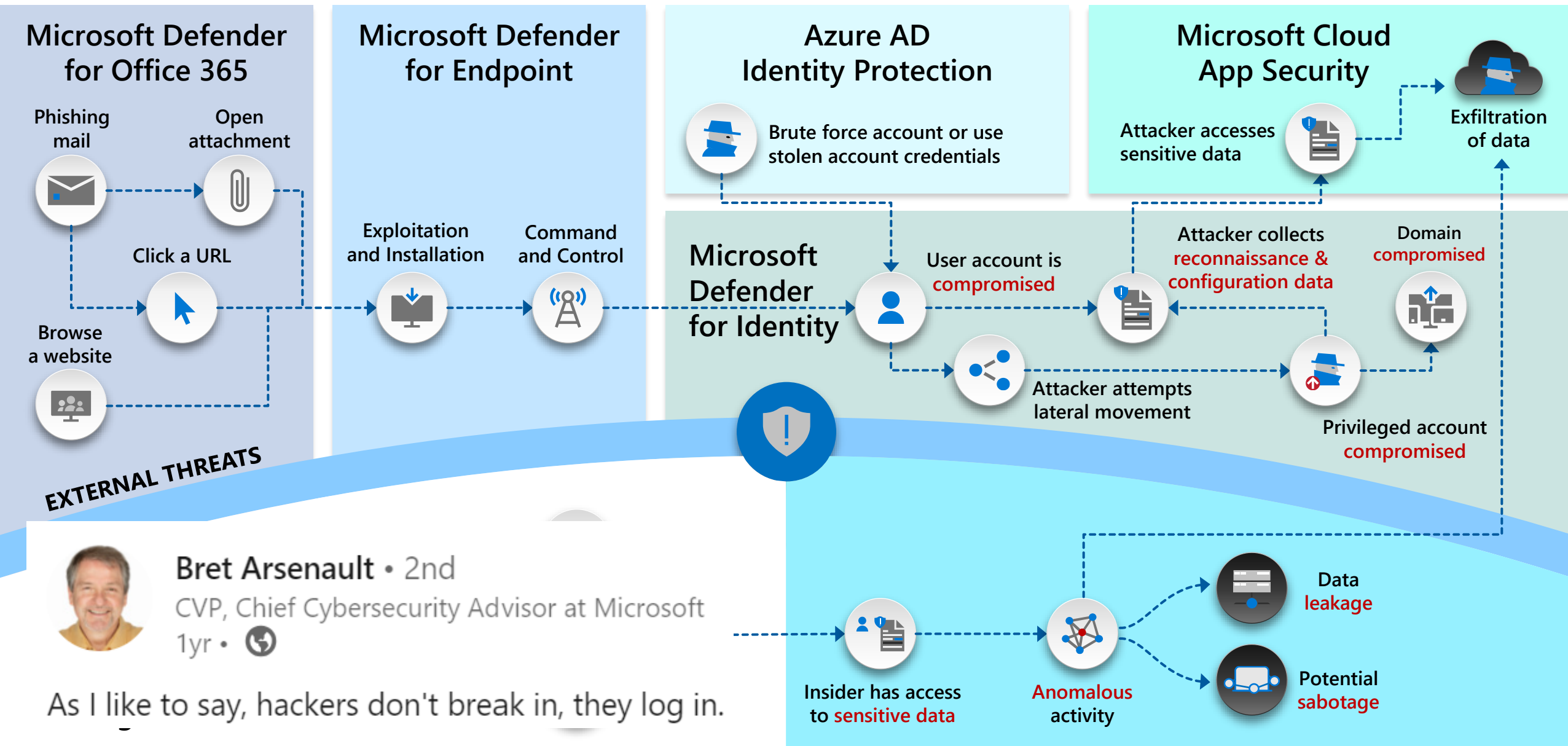


Ted Tøraasen
Compliance Technology Specialist
ted.toraasen@microsoft.com



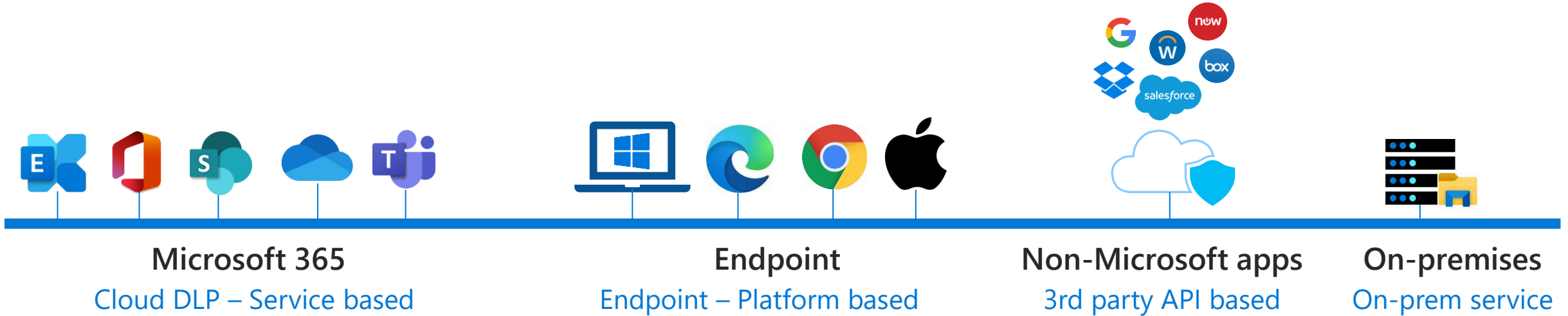
<https://www.linkedin.com/in/tedtoraasen/>

Internal and external protection across the threat kill chain



Microsoft Purview Data Loss Prevention

Prevent accidental or unauthorized sharing of sensitive data



Data in use

Data in motion

Data at rest

Guided onboarding

Unified & flexible policy management

Integrated with Microsoft Purview Information Protection

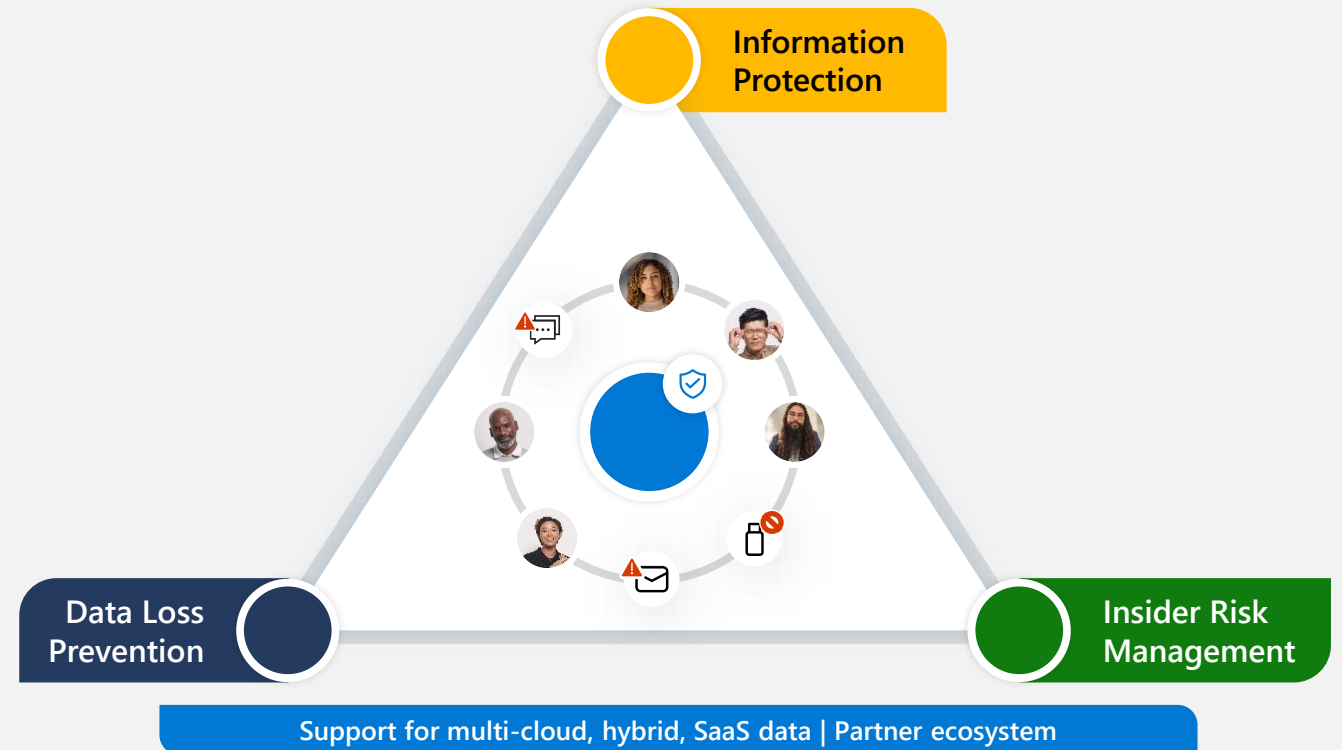
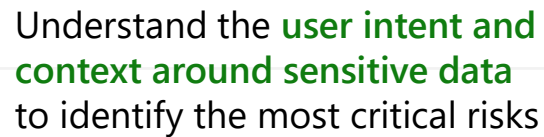
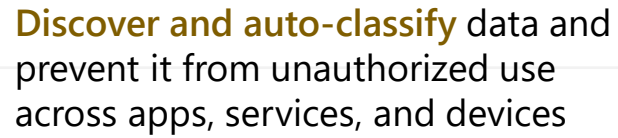
Unified alerting & remediation

Agentless and integrated within end user experiences

Why is this so challenging?



Fortify data security with an integrated approach



Best-in-class classification technologies

Sensitive info types

300+ out of the box info types like SSN, CCN
Clone, edit, or create your own
Supports regex, keywords, and dictionaries

AVAILABLE TODAY

Named entities

50+ entities covering person name, medical terms, and drug names
Best used in combination with other sensitive info types

AVAILABLE TODAY

Exact data match

Provides a lookup to exactly match content with unique customer data
Supports 100m rows and multiple lookup fields

AVAILABLE TODAY

Trainable classifiers

23 new pre-trained ready-to-use trainable classifiers in GA
15 more in product preview
Create your own classifier based on business data

AVAILABLE TODAY

Credentials SITs

42 new SITs for digital authentication credential types
Use in auto-labeling and DLP policies to detect sensitive credentials in files

AVAILABLE TODAY

Context-based classification

Service-side auto-labeling
ODSP default site label

- File extension
- Document name contains word
- Document property is
- Document size greater than
- Document created by

ROADMAP ITEM

Templates

- Provide pre-defined policies that use available classifiers
- Cover multiple industry and geographical regulatory requirements
- Easily customizable, can be edited to meet customer needs
- Get started easily with simulations, rerun as needed to fine tune

Categories	Templates	U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced
Enhanced	U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced	Helps detect the presence of information subject to Gramm-Leach-Bliley Act (GLBA), including information like social security numbers or credit card numbers. This enhanced template extends the original by also detecting people's full names, U.S./U.K. passport number, U.S. driver's license number and U.S. physical addresses. We have also enhanced this template with Trainable Classifier "Business-Finance" and "Business-Tax" which can detect financial information such as Budget proposal, Financial statements and Proposals and Reports and tax information such as Tax planning documents, Tax forms, Tax filing related documents and Tax regulation documents.
Financial	Australia Health Records Act (HRIP Act) Enhanced	
Medical and health	U.S. Health Insurance Act (HIPAA) Enhanced	
Privacy	Australia Privacy Act Enhanced	
Custom	General Data Protection Regulation (GDPR) Enhanced	
	Japan Personally Identifiable Information (PII) Data Enhanced	
	Japan Protection of Personal Information Enhanced	
	U.S. Patriot Act Enhanced	
	U.S. Personally Identifiable Information (PII) Data Enhanced	
	U.S. State Breach Notification Laws Enhanced	

Protect this information:

- Business - Tax
- Business - Finance
- Credit Card Number
- U.S. Bank Account Number
- U.S. Individual Taxpayer Identification Number (ITIN)
- U.S. Social Security Number (SSN)
- U.S. / U.K. Passport Number
- U.S. Driver's License Number
- All Full Names
- U.S. Physical Addresses

Sensitivity labels span your entire data estate

- They are a representation of your information taxonomy.
- They describe the priority assigned to your categories of sensitive information.



Content labels



Applied To: Office apps, Power BI reports, Azure Data

Protections: Encryption and visual markings

Automation: Can be applied either manually by users or automatically based on classification

Container labels



Applied To: SharePoint sites, Teams channels, Microsoft 365 groups

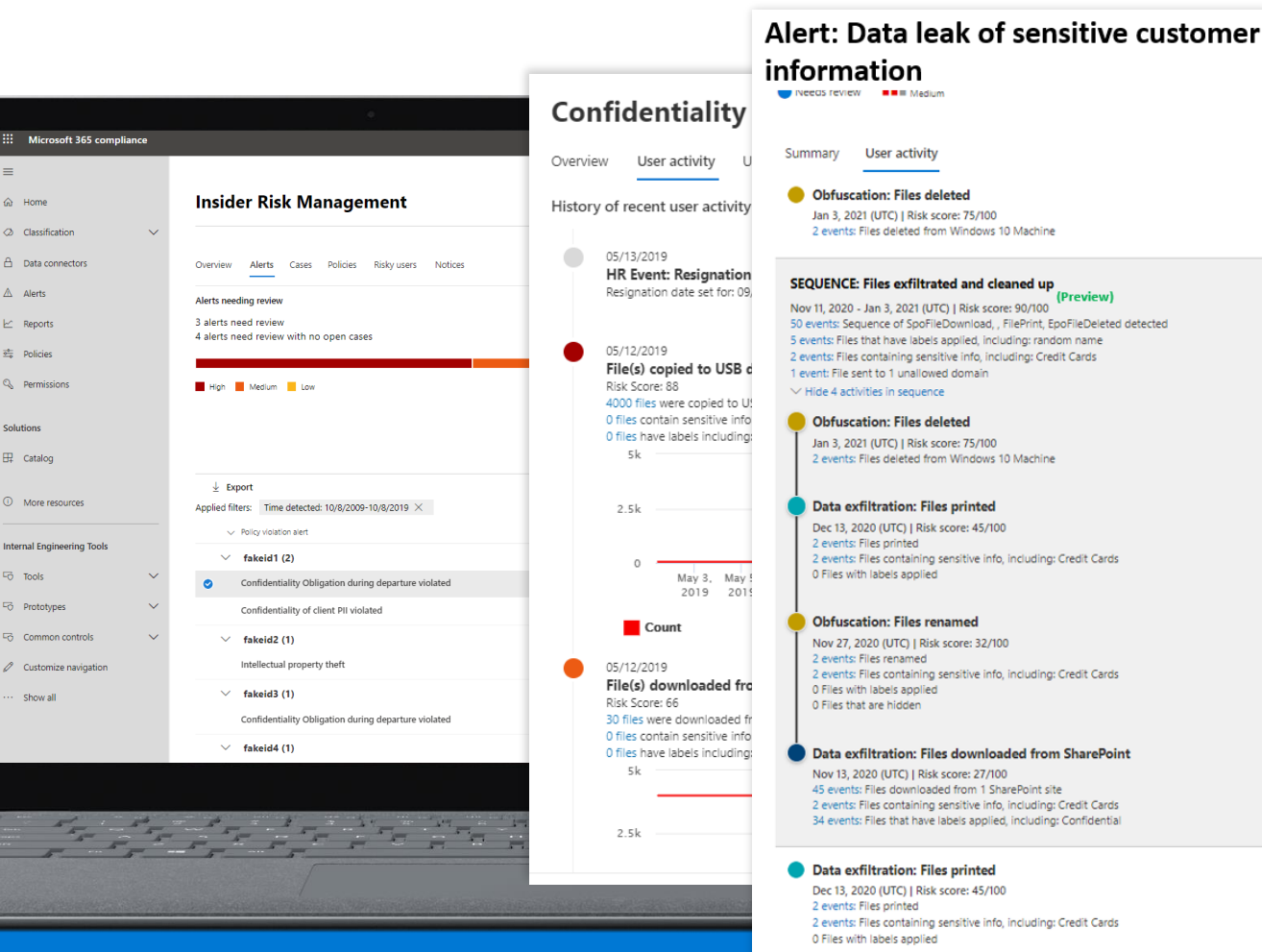
Protections: Access control, privacy settings, conditional access

Automation: Can be applied manually by site/Team or group owners

Powerful controls that ensure labels are applied where needed
Apply labels by default, make them mandatory, prevent label downgrades

Insider Risk Management

Microsoft helps you quickly identify and act on insider risks with an integrated end-to-end approach



Rich insights

Identify hidden risks with customizable ML templates requiring no endpoint agents.



Privacy built in

Pseudonymization and strong controls help appropriately manage data about risks.



End-to-end investigations

Integrated investigation workflows allow for collaboration across Security, HR, and Legal.

Leveraging **machine learning** to identify the most critical insider risks among noisy signals

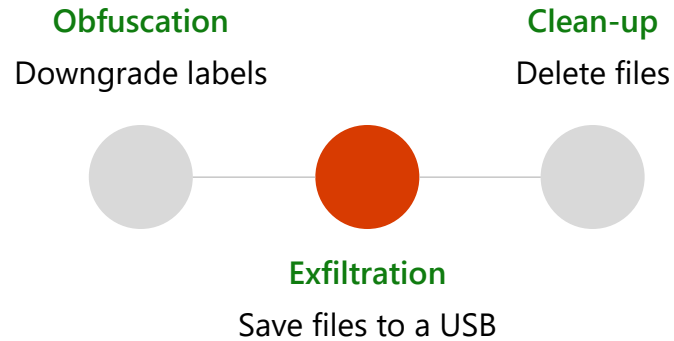
Know the context

Correlate data signals



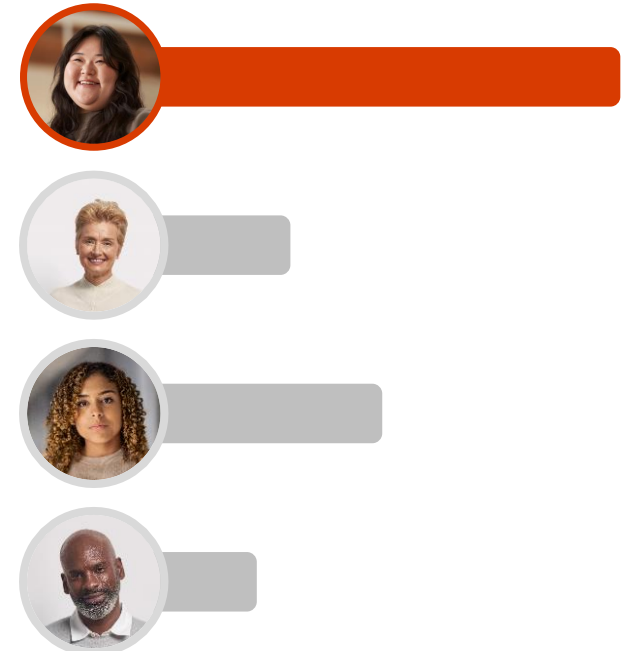
Understand the intent

Sequence detection



Benchmarking

Anomaly detection

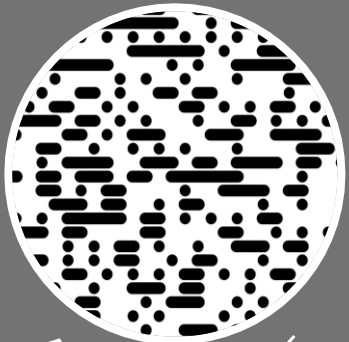


Protect user **trust** with privacy built in

User privacy is maintained every step of the way

Pseudonymization

Prevent bias by removing identifiable user details, on by default



Anony8SKF-34DF

Role-based access controls

Only authorized admins can access alerts and insights



Opt-in

Admin explicitly opts-in users to enable policies, with all indicators off by default

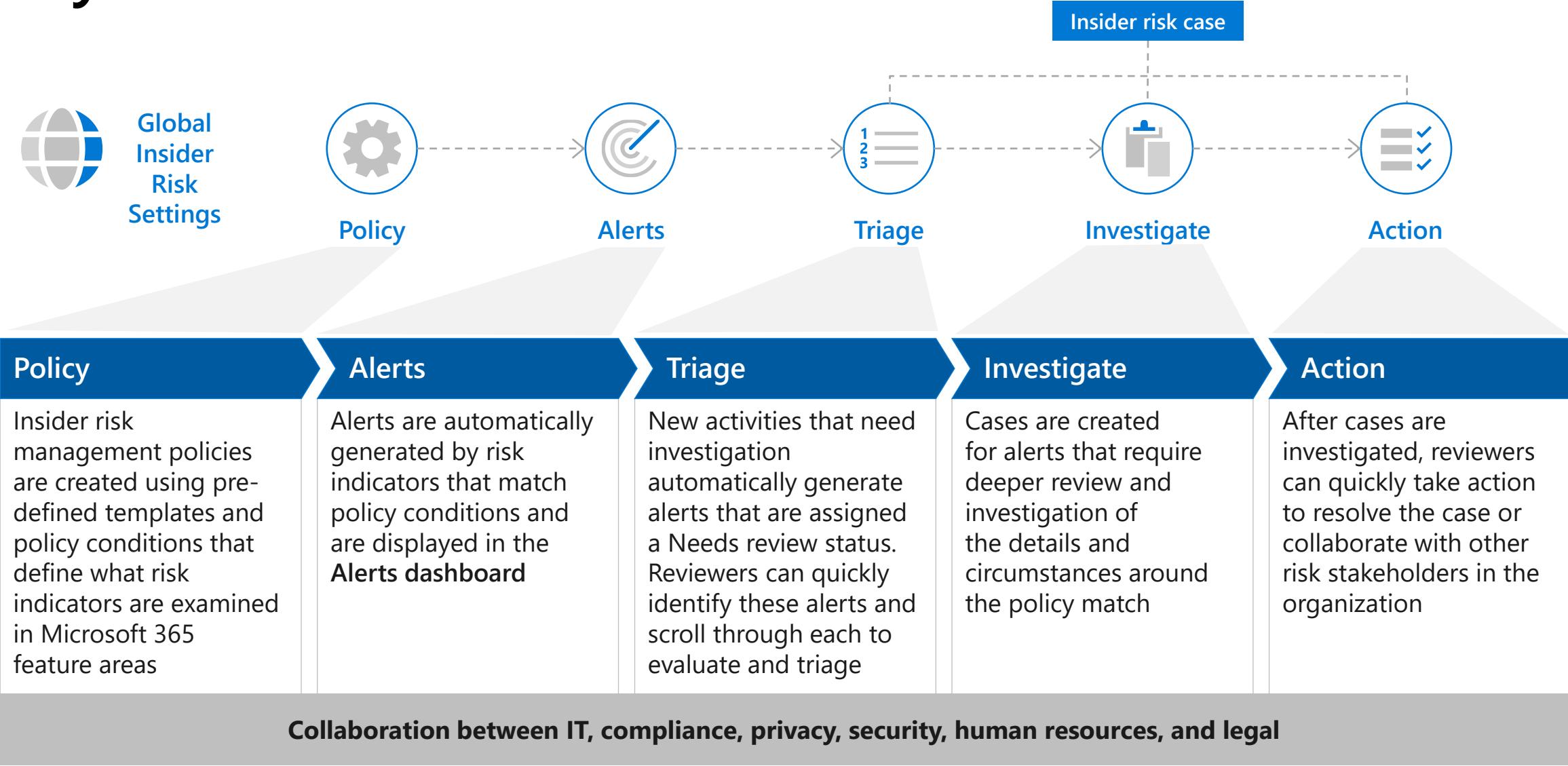


Audit logs

Every action – from policy configuration to remediation actions is logged in audit reports



Key workflow and solution elements



Case 449: Potential IP theft

 Active

 Low

25 risk score

Resolve case

Case actions

Case overview

Alerts

User activity

Activity explorer

Forensic evidence (preview)

Content explorer

Case notes

Contributors

Filter:

Risk category: Any

Activity Type: Any

Reset all

Sort by: Date occurred

- Cumulative exfiltration activities

Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 15/100

467 events: All exfiltration activities with prioritized content: More events than 90% compared to teammates. Priority content includes: 1 SharePoint sites and 2 file extensions.

(Explore content)

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

(Explore content)

21 events: All exfiltration activities: More events than 30% compared to users with same job title.

(Explore content)
- Cumulative exfiltration activities

Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 45/100

467 events: All exfiltration activities with prioritized content: More events than 90% compared to teammates. Priority content includes: 1 SharePoint sites and 2 file extensions.

(Explore content)

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

(Explore content)

21 events: All exfiltration activities: More events than 30% compared to users with same job title.

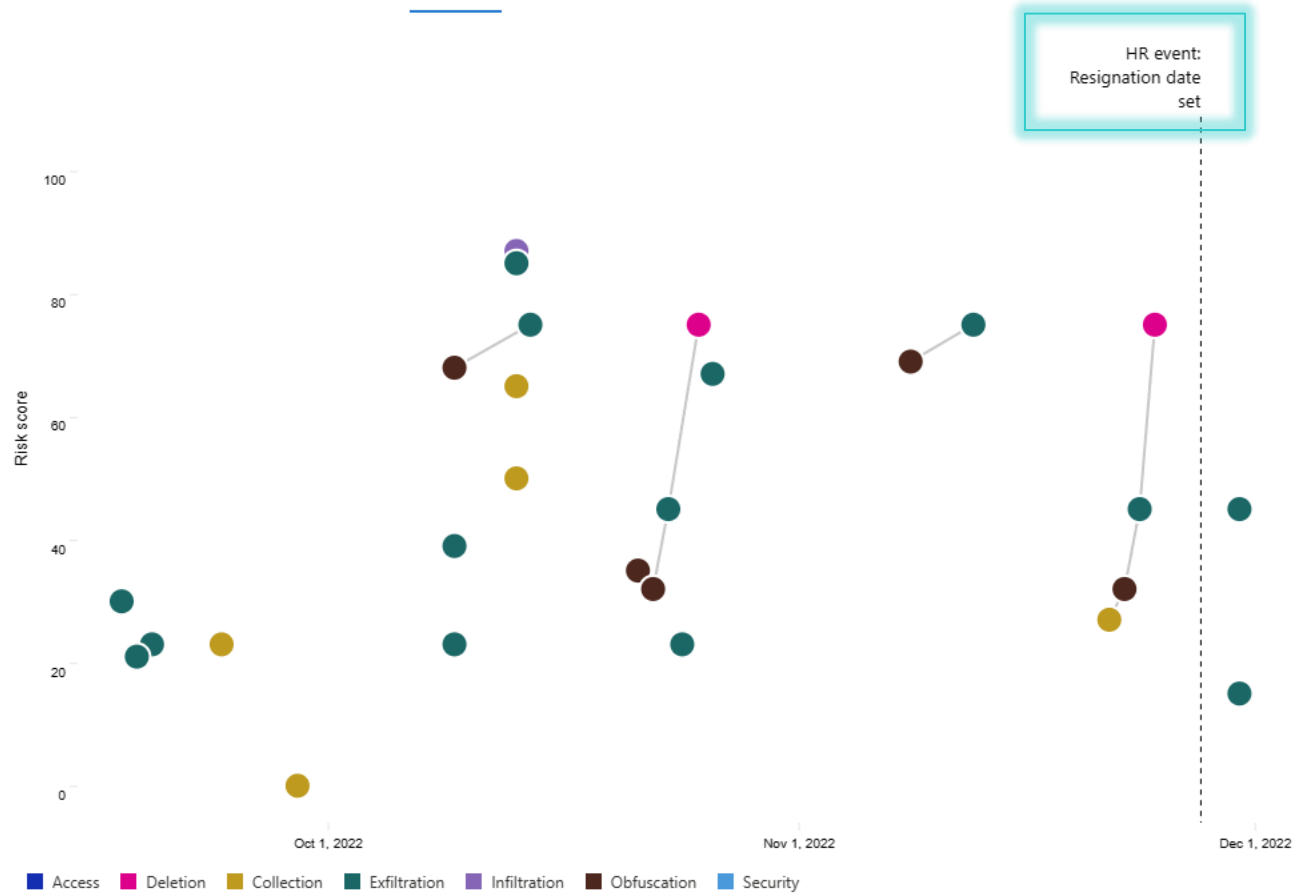
(Explore content)

User activity scatter plot

6 Months

3 Months

1 Month



Deletion: Files deleted

Microsoft Purview

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Roles & Scopes

Trials

Solutions

Catalog

App governance

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Information barriers

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

Forensic evidence (preview)

Content exp

Filter:

Risk category: Any

Activity Type: Any

Reset all

Sort by: Date occurred

User activity scatter plot

6 Months

3 Month

Cumulative exfiltration activities

Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 15/100

467 events: All exfiltration activities with prioritized content: More events than 90% compared to teammates. Priority content includes: 1 SharePoint sites and 2 file extensions.

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

21 events: All exfiltration activities: More events than 30% compared to users with same job title.

Cumulative exfiltration activities

Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 45/100

467 events: All exfiltration activities with prioritized content: More events than 90% compared to teammates. Priority content includes: 1 SharePoint sites and 2 file extensions.

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

Risk score

100

80

60

40

20

0

Access

Deletion

Collection

Exfiltration

Initiation

Obfuscation

Security

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

Nov 21, 2022 - Nov 24, 2022 (UTC) | Risk score: 90/100

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

5 events: Files that have labels applied, including: random name

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

Nov 24, 2022 (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

Nov 23, 2022 (UTC) | Risk score: 45/100

2 events: Files printed

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

Obfuscation: Files renamed

Nov 22, 2022 (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

Nov 21, 2022 (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

HR event: designation date set

Understand user intent with sequence detection, which automatically identify and connect a series of related activities

Case 449: Potential IP theft

Active Low 25 risk score

Resolve case

Case actions 











Case overview Alerts User activity Activity explorer Forensic evidence (preview) **Content explorer** Case notes Contributors

Examine the emails and files captured by the policies included in this case. [Learn more](#)

Filter Reset Filters

Group Customize columns Export all file names

1 of 74 selected

		Subject/Title	Date (UTC)	File class	Sender/Author	Recipients	Sensi
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input checked="" type="checkbox"/>		CONFIDENTIAL - Pr...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		
<input type="checkbox"/>		Project Moonshot ...	Jul 21, 2021 7:13 PM	Document	MOD Administrator		

CONFIDENTIAL - Project Moonshot One Pager.pdf

Source

1

of 1

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.

Video provides a powerful way to help you prove your point. When you click Online Videos, you can paste in the embed code for the video you want to add. You can also type a keyword to search online for the video that best fits your document.

To make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you can add a matching cover page, header, and sidebar. Click Insert and then choose the elements you want from the different galleries.

Themes and styles also help keep your document coordinated. When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you apply styles, your headings change to match the new theme. Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it and a button for layout options appears next to it. When you work on a table, click where you want to add a row or a column, and then click the plus sign.

Reading is easier, too, in the new Reading View. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off - even on another device.

Video provides a powerful way to help you prove your point. When you click Online Videos, you can paste in the embed code for the video you want to add. You can also type a keyword to search online for the video that best fits your document.

To make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you can add a matching cover page, header, and sidebar. Click Insert and then choose the elements you want from the different galleries.

Themes and styles also help keep your document coordinated. When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you apply styles, your headings change to match the new theme.

Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it and a button for layout options appears next to it. When you work on a table, click where you want to add a row or a column, and then click the plus sign.

Reading is easier, too, in the new Reading View. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off - even on another device.

Video provides a powerful way to help you prove your point. When you click Online Videos, you can paste in the embed code for the video you want to add. You can also type a keyword to search online for the video that best fits your document.

To make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you can add a matching cover page, header, and sidebar. Click Insert and then choose the elements you want from the different galleries.

Themes and styles also help keep your document coordinated. When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you apply styles, your headings change to match the new theme.

Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it and a button for layout options appears next to it. When you work on a table, click where you want to add a row or a column, and then click the plus sign.

Reading is easier, too, in the new Reading View. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off - even on another device.

Video provides a powerful way to help you prove your point. When you click Online Videos, you can paste in the embed code for the video you want to add. You can also type a keyword to search online for the video that best fits your document.

To make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you can add a matching cover page, header, and sidebar. Click Insert and then choose the elements you want from the different galleries.

Themes and styles also help keep your document coordinated. When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you apply styles, your headings change to match the new theme.

Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it and a button for layout options appears next to it. When you work on a table, click where you want to add a row or a column, and then click the plus sign.

Reading is easier, too, in the new Reading View. You can collapse parts of the document and focus on the text you want. If you need to stop reading before you reach the end, Word remembers where you left off - even on another device.

Highly Confidential

Contoso Electronics

Review the exfiltrated content easily in its native view

Insider Risk Management

An integrated end-to-end approach for insider risks from Microsoft 365

Insider Risk Management +

Data Loss Prevention

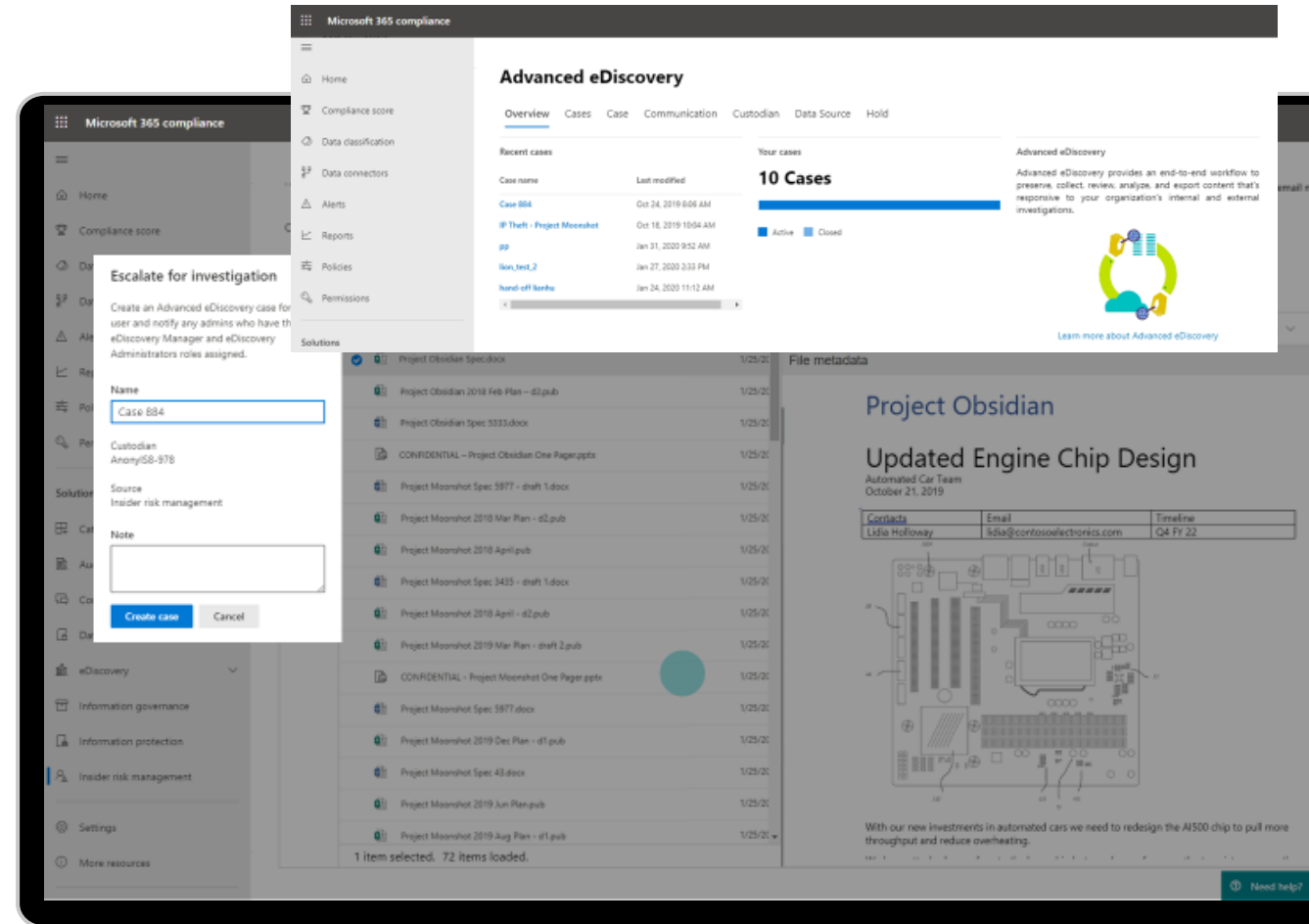
Information Protection

Communication Compliance

Advanced eDiscovery

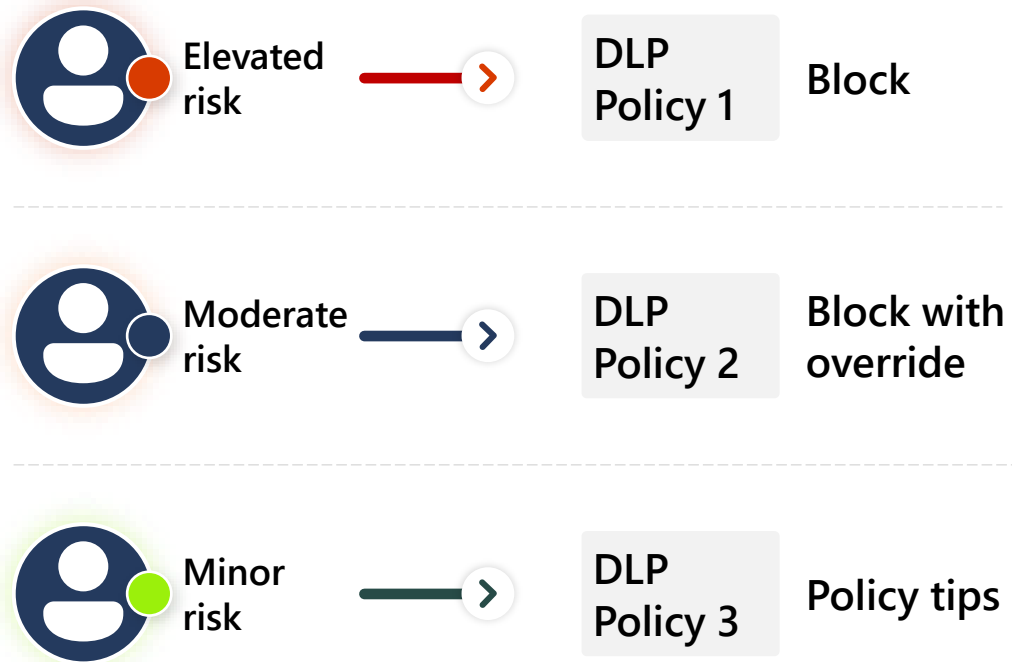
Legal collaboration

Integrated workflows provide seamless investigation handoff

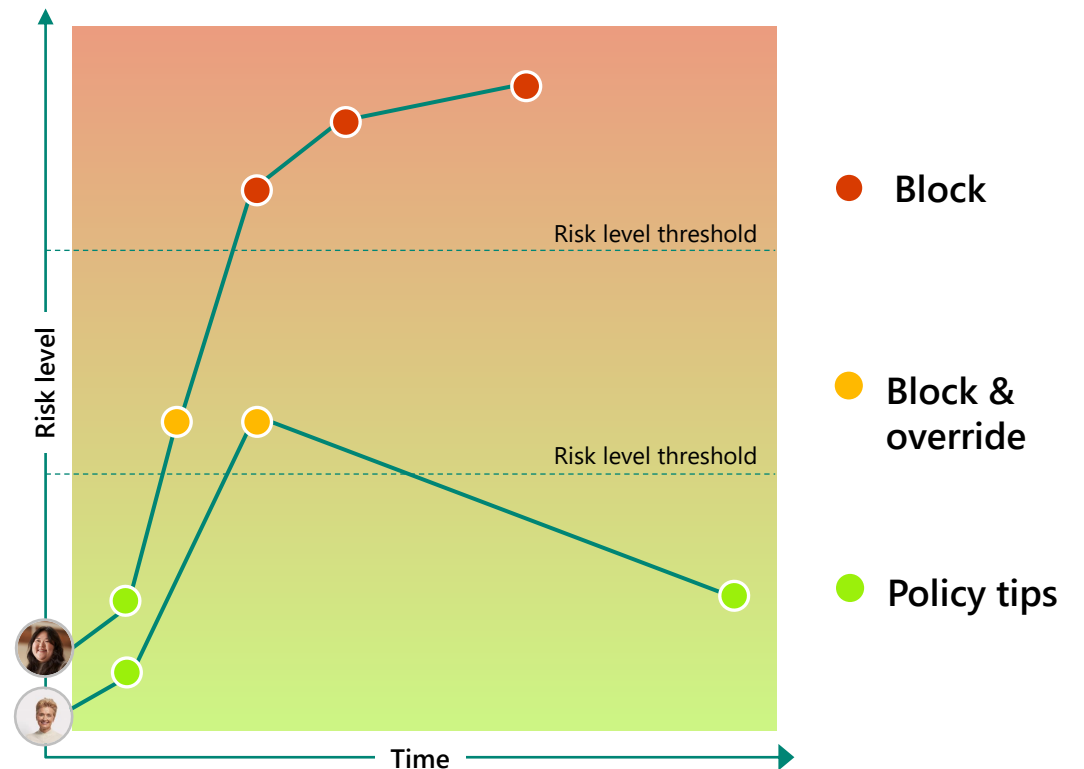


Optimize data security with Adaptive Protection

Leverages [machine learning](#) to understand how users are interacting with data, assign risk levels, and automatically tailor Data Loss Prevention controls.



Each user has [tailored protection controls](#) that are continuously adjusted over time. High risks are automatically mitigated while low-risk users can work as usual and be educated on data handling best practices.



Manage insider risks across your digital landscape

Organizations can bring in detections and incorporate insider risk management into existing incident management processes



Prefer having a dedicated insider risk management solution?



Bring in signals to have a holistic view of an insider risk alert

HR systems



Physical badging systems

Non-Microsoft applications



SIEMs



Microsoft Defender for Cloud Apps

Connectors

Microsoft Purview Insider Risk Management



100+ ready-to-use indicators and machine learning models across Microsoft 365 apps and services, endpoints, Defender, Entra, and more.

Prefer centralizing all security incidents insights?



Export curated high-quality insider risks alerts to where your team works



Office 365
Mgmt. APIs



Sentinel



splunk>

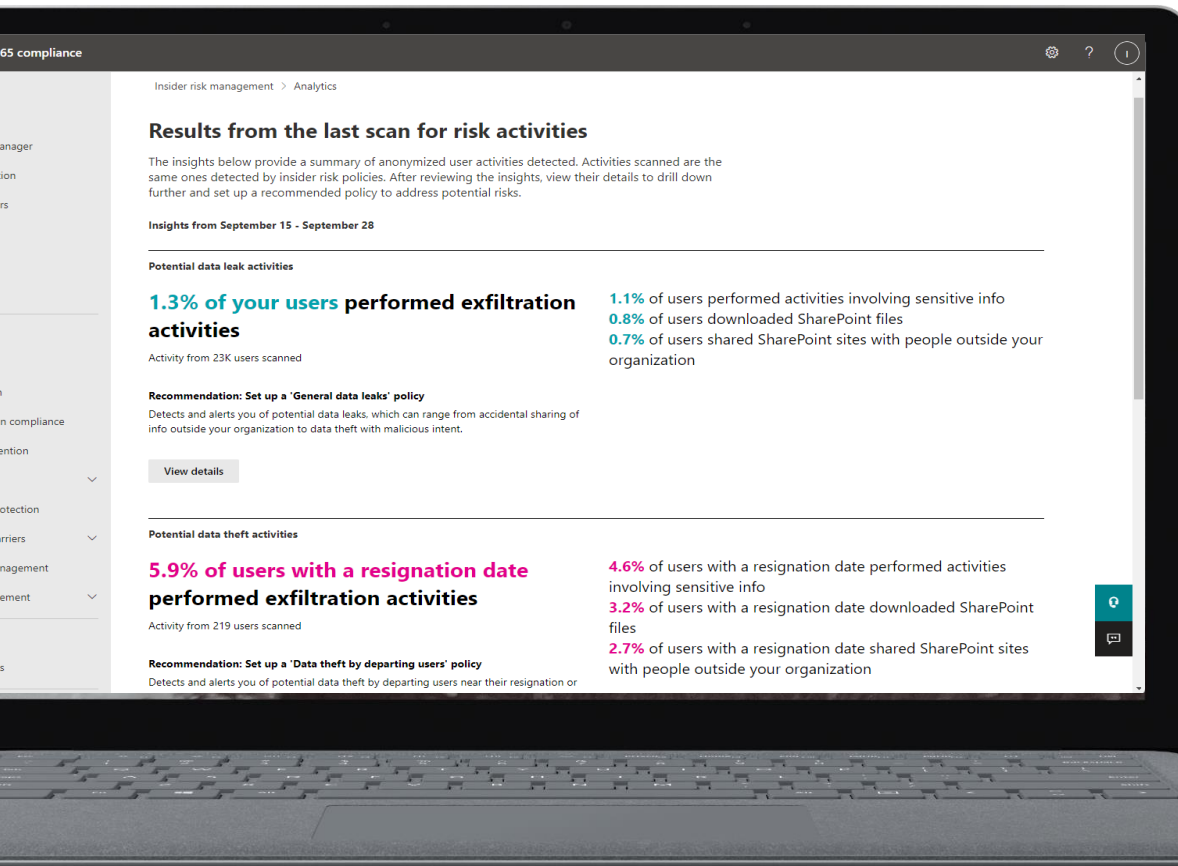


Exabeam

SIEMs

Insider Risk Management Analytics

Quickly gain insights into insider risks in your organization



Easy setup

Quick start by clicking "Run scan" in Analytics or enabling analytics in Insider risk settings



Privacy by default

Scan results and insights are returned as aggregated, anonymized user activity

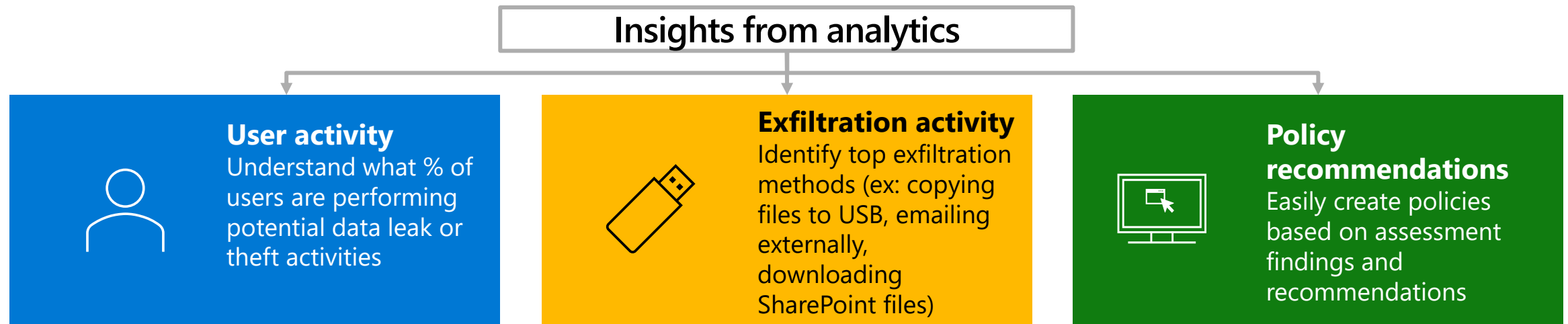
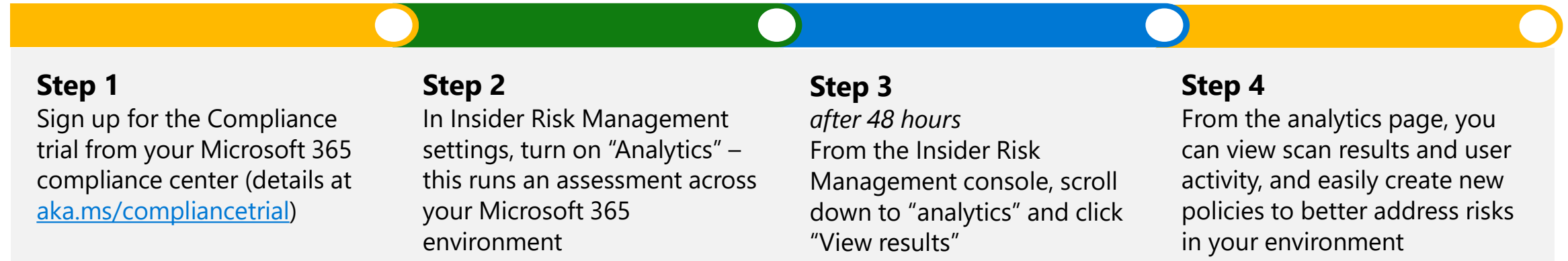


Consolidated insights

Results can help you quickly identify potential risk areas and which policies would be best to help mitigate these risks

Setting up analytics in Insider Risk Management

Analytics is easy to set up and run, and helps you quickly detect risky user behavior with a baseline assessment



Results from the last scan for risk activities

The insights below provide a summary of anonymized user activities detected. Activities scanned are the same ones detected by insider risk policies. After reviewing the insights, view their details to drill down further and set up a recommended policy to address potential risks.

Insights from September 15 - September 28

Potential data leak activities

1.3% of your users performed exfiltration activities

Activity from 23K users scanned

Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

[View details](#)

- 1.1% of users performed activities involving sensitive info
- 0.8% of users downloaded SharePoint files
- 0.7% of users shared SharePoint sites with people outside your organization

Potential data theft activities

5.9% of users with a resignation date performed exfiltration activities

Activity from 219 users scanned

Recommendation: Set up a 'Data theft by departing users' policy

Detects and alerts you of potential data theft by departing users near their resignation or

- 4.6% of users with a resignation date performed activities involving sensitive info
- 3.2% of users with a resignation date downloaded SharePoint files
- 2.7% of users with a resignation date shared SharePoint sites with people outside your organization



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

Insider risk management > Analytics (preview)

Results from the last scan for risk activities

The insights below provide a summary of anonymized user activities detected. Activities scanned same ones detected by insider risk policies. After reviewing the insights, view their details to drill further and set up a recommended policy to address potential risks.

Insights from September 15 - September 28

Potential data leak activities

1.3% of your users performed exfiltration activities

Activity from 23K users scanned

Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

View details

Potential data theft activities

5.9% of users with a resignation date performed exfiltration activities

Activity from 219 users scanned

Recommendation: Set up a 'Data theft by departing users' policy

Detects and alerts you of potential data theft by departing users near their resignation or

Potential data leak activities

The exfiltration activities below might be related to data leakage. After reviewing the results, consider setting up the recommended policy to help address potential risks.

What we detected

The following is recent activity based on a scan of 23K users.

1.3% of users performed exfiltration activities

1.1% of users performed activities involving sensitive information

0.8% of users downloaded SharePoint files

0.7% of users shared SharePoint sites with people outside your organization

0.5% of users shared SharePoint files with people outside your organization

0.5% of users shared SharePoint folders with people outside your organization

0.4% of users copied sensitive content to personal cloud

0.4% of users shared files across network

0.3% of users emailed people outside your organization

0.2% of users copied content to USB

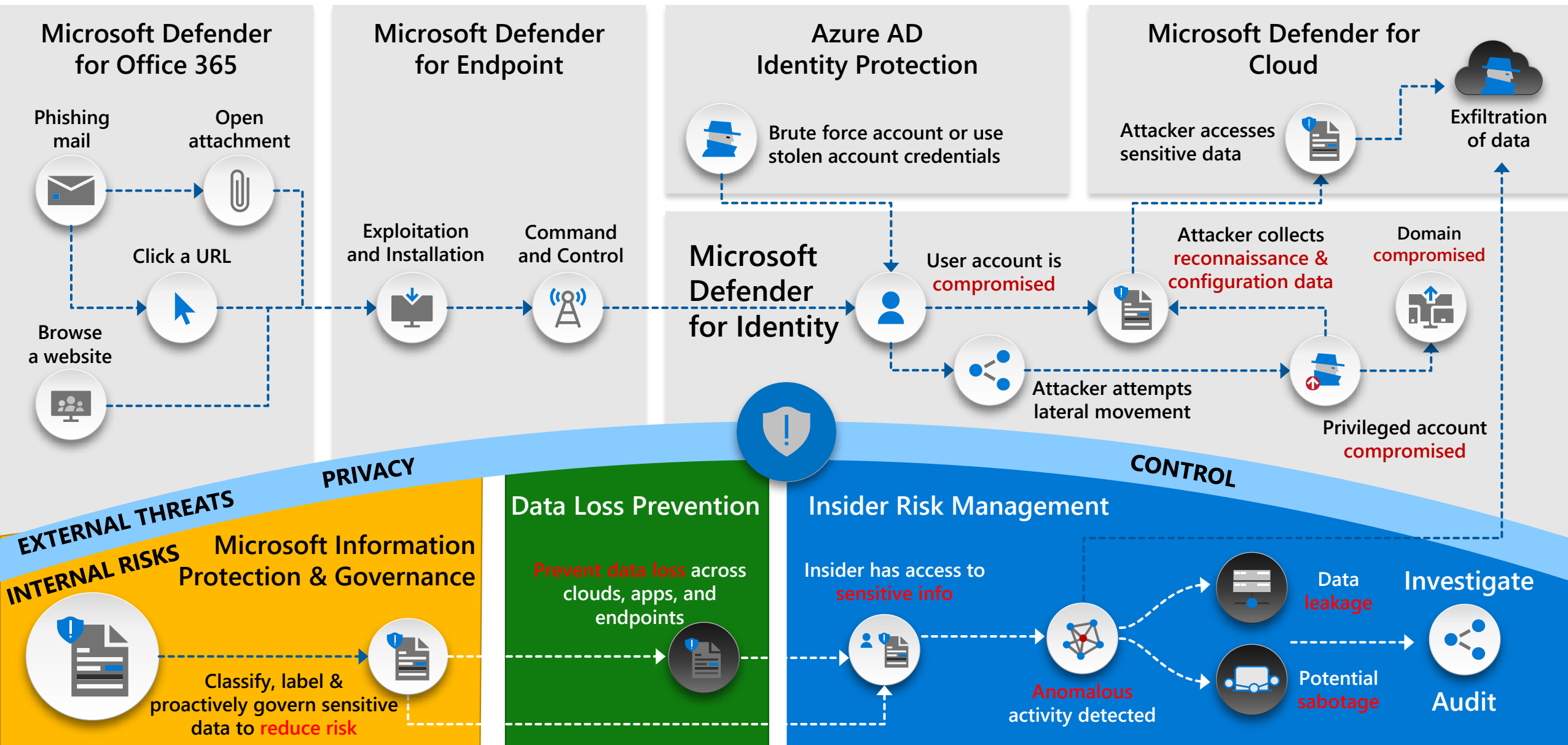
0.1% of users printed a large number of files

Recommendation

Create a 'General data leaks' policy that detects and alerts you of potential data leaks by users, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

Create policyClose

Microsoft security and compliance solution integration



Get started today



Turn on Analytics in Insider Risk Management:

aka.ms/insiderrisk/analytics



Create a quick policy:

aka.ms/insiderrisk/quickpolicy



Turn on Adaptive Protection in one click:

aka.ms/adaptiveprotection/docs



Sign up for Microsoft Purview trial :

aka.ms/PurviewTrial



Resources

Insider Risk Management

- Technical documentation: <https://aka.ms/insiderriskdocs>
- Mechanics video: <https://aka.ms/insiderriskmechanics>
- Latest announcement: <https://aka.ms/insiderriskblog>

Adaptive Protection

- Technical documentation: <https://aka.ms/adaptiveprotection>
- Mechanics video: <https://aka.ms/adaptiveprotection/mechanics>
- Latest announcement: <https://aka.ms/adaptiveprotection/blog>

