



orange™

Cyberdefense



We are the trusted cyber partner committed to create value for all by delivering the safest digital space

€1.1 billion
 turnover in 2023
 +11% YtoY



Over 3,000
 multi-skilled cybersecurity experts



+9,000
 customers worldwide,
 best in class in all verticals



Leader in European Managed Security Services



+500
 sources continuously feed into our threat intelligence datalake

40,000
 suspicious websites closed every year

24/7/365
 continuous monitoring of security systems worldwide

Listed vendor in five reports:
 Managed Detection and Response, Incident Response and Digital Forensics, OT Security, Threat Intelligence & Managed Security Services

Gartner

129,000
 incidents analyzed in 2023

Our value alongside Microsoft

- **Unrivalled Threat Intelligence**

 - Attacker Infrastructure active probing

 - Dark Web and Ransomware leak sites

 - Takedown of fraudulent domains & phishing sites

- **Established leaders**

- **Co-innovation**

 - Member of Microsoft Intelligent Security Association (MISA) & Microsoft-verified MXDR solution badge holder.

- **Microsoft-certified**

 - More than 140 Microsoft certified experts over 3,000 cybersecurity people.



Microsoft Solutions



Azure

Architecture
Identity and Access
Management
Security Assessment
Security Hardening



Defender

Defender XDR
Defender for Cloud
Defender for IOT
Vulnerability Management



Sentinel

Integration services
Threat Hunting
Log Optimization
Managed SIEM



PurView

Consulting & Integration
Compliance Audits
Security Assessment



Copilot

M365 Security Readiness
Check

16 certified engineers in local Swiss team

Many more available from global teams

Early 2025

Dedicated
events coming
...

Our offerings for Microsoft security



	Defender for endpoint	Defender XDR	Defender for Cloud	Sentinel	Defender for IoT	Entra	Purview	Priva
	EDR	Unified Defense	CSPM CWP	SIEM SOAR	OT/IoT Defense	IAM	Data governance and security	Privacy posture
Managed Services	Managed Threat Detection							
	Managed Workspace protection		Managed multicloud protection		Managed industrial security	Managed secure access	Bespoke SOC	
	Managed vulnerability intelligence							
	Incident response retainer service							
Professional Services	Consulting, design, configuration, optimization							
	Security assessment, hardening, Pentesting							

Our Microsoft Advisory Services at a glance



Quick access to Microsoft experts at all times



Reassurance that your Microsoft products are correctly secured



Proactive and reactive management of Microsoft Defender and Sentinel



A strategic planning tailored on your needs after discuss delivery, report and feedback



Peace of mind with 24/7 Security Operations Centre



Hands-on implementation you can count on

More Information on our Website :

<https://www.orange cyberdefense.com/ch/offering/professional-services/microsoft-consulting-advisory>

Comprehensive data security



Top data security concerns



Data security incidents are widespread

83%

of organizations experience more than one data breach in their lifetime¹

Malicious insiders account for 20% of data breaches, adding to costs

\$15.4M

Total average cost of activities to resolve insider threats over 12 month period²

Organizations are struggling with a fragmented solution landscape

80%

of decision makers purchased multiple products to meet compliance and data protection needs³

1. Cost of a Data Breach Report 2022, IBM

2. Cost of Insider Threats Global Report 2022, Ponemon Institute

3. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

Data security incidents can happen anytime, anywhere



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

1

User falls prey to phishing attack, compromises user credentials

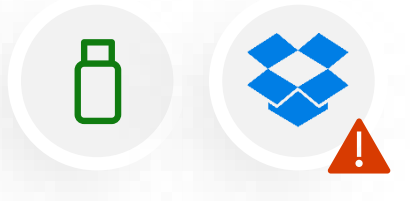


Data compromise by external threat



2

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



Data theft by malicious insider



3

User inadvertently shares the file copy with a few colleagues



Data exposure by negligent insider



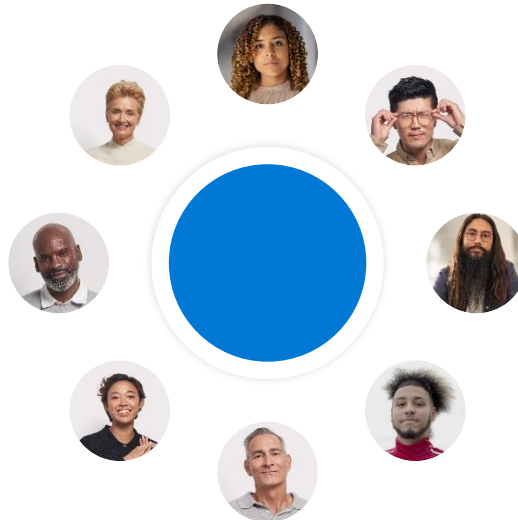
Organizations need to...



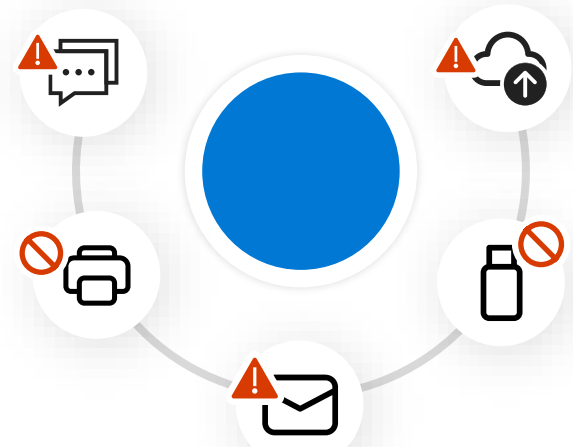
Discover and protect sensitive data throughout its lifecycle



Understand user activity context around the data and identify risks



Prevent data from unauthorized use across apps, services, and devices



Balance data security and productivity

Fortify data security with Microsoft Purview



Information Protection

- **Discover, classify, and protect** data at scale, using automation and ML
- Productivity tools with built-in **user-selectable sensitivity labels** for precise controls
- Data is **protected (encrypted) across environments**, throughout its lifecycle

Insider Risk Management

- Leverage **analytics, machine learning, sequencing** to understand user context and intent
- Investigate potential incidents with **curated, high-quality, and enriched** alerts and evidence
- Ensure user privacy while identifying **highest risk users**

Data Loss Prevention

- **Prevent unauthorized use**, like improperly saving, storing or printing sensitive data
- Create, deploy, and manage DLP policies **across all cloud, apps, and devices from a single location**
- Leverage data classification, labeling, and user **insights to finetune and adapt DLP policies**

Adaptive Protection

- Dynamically adjust data security controls based on user risk level

Adaptive Protection in Microsoft Purview

Optimize data security automatically

Context-aware detection

Identify the most critical risks with ML-driven analysis of both content and user activities

Dynamic controls

Enforce effective controls on high-risk users while others maintain productivity

Automated mitigation

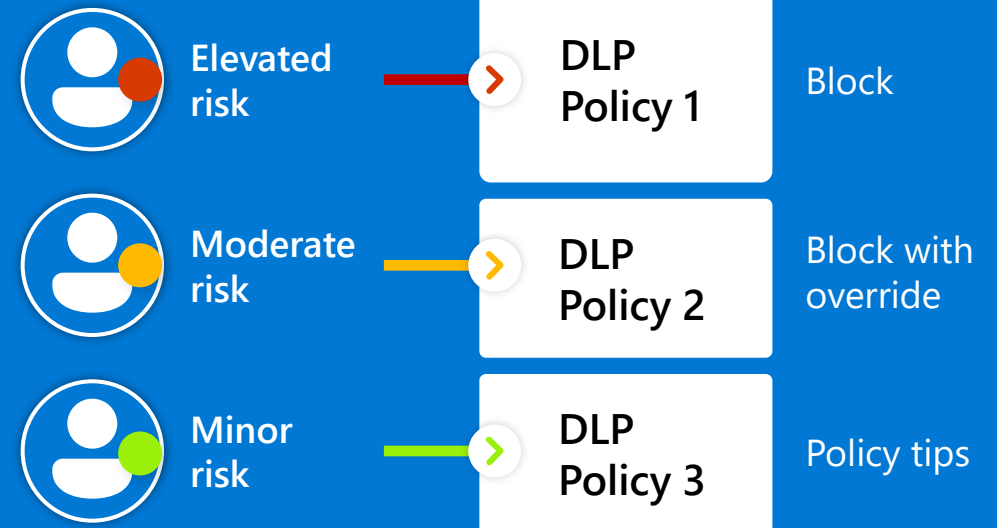
Minimize the impact of potential data security incidents and reduce admin overhead

Insider Risk Management

Detect risky users and assign risk levels

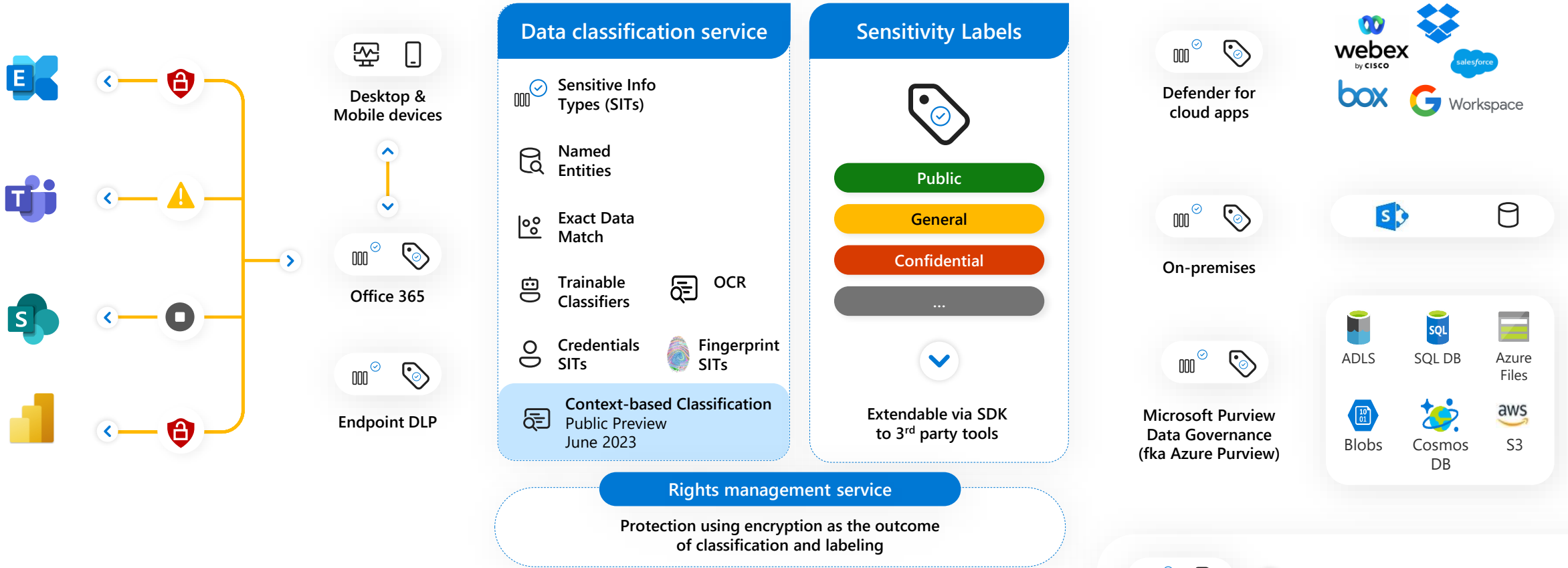
Data Loss Prevention

Dynamically apply preventative controls



Microsoft Purview Information Protection

Microsoft Purview Information Protection







Uniform content & context-based classification ●

Native integration with Microsoft 365 apps and services ●

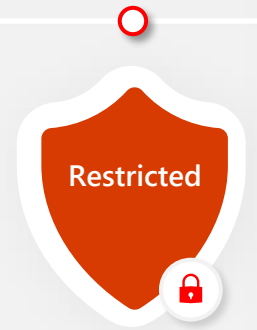
Broad support with 3rd party solutions, data repositories, and LOB applications ●

Advanced compliance solutions

- 
 eDiscovery (premium)
- 
 Insider risk management
- 
 Communication compliance
- 
 Microsoft Priva

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, audit label downgrades

Best-in-class classification technologies

Sensitive info types



200+ 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

Optical Character Recognition (OCR)



Expanded OCR for EXO, SPO, ODB, Teams & endpoint devices
Supports over 150 languages
Supports image files and images embedded in PDFs

AVAILABLE TODAY

Trainable classifiers



35+ pre-trained ready-to-use trainable classifiers
Create your own classifier based on business data

AVAILABLE TODAY

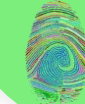
Credentials SITs



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

AVAILABLE TODAY

Fingerprint SITs



Detect exact or partial matching of sensitive intellectual property
Use in Exchange, SharePoint, Teams and Devices

AVAILABLE TODAY

Context-based classification



ODSP default site label
Service-side auto-labeling

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

ROADMAP ITEM

Policy simulation

1



2



3



4



Pick your scope

- Option 1: ALL – SharePoint sites, OneDrive accounts and Email users
- Option 2: Subset of sites or accounts – Can use PowerShell for longer lists

Supported in auto labeling and DLM today, DLP by Jun'23



Simulate in your production environment

- Simulation is fast – It normally takes a few hours to run depending on the size of your tenant
- Simulation is not intrusive – No actions are applied
- Simulation for EXO triggers in near real time on email activity (not emails at rest)
- Simulation for ODSP triggers on files at rest
- Insights are best achieved on real production data



Gain confidence in your protection policy

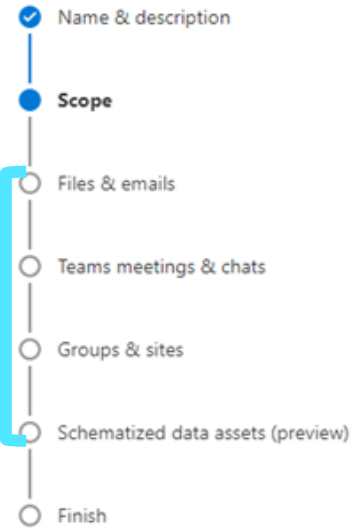
- Review simulation results (both aggregate and sample files)
- Iterate and experiment to improve accuracy



Turn on protection policies after validating simulation results

- Existing Office Files at rest (Word, Excel, PowerPoint) in OneDrive & SharePoint are automatically protected
- New files added after the policy is enforced are also protected
- Emails in transit are automatically scanned for sensitive information and protected
- *Cold data crawl: private preview coming in Q3'23*

New sensitivity label



Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

Files & emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

Meetings

Configure access and permission settings for Teams meetings and content restrictions for Teams chats.

Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

Schematized data assets (preview)

Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

- Compliance Manager
 - Data classification**
 - Data connectors
 - Alerts
 - Reports
 - Policies
 - Permissions
 - Trials
-
- Solutions**
- Catalog
 - App governance
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - eDiscovery
 - Data lifecycle management
 - Information protection

Data classification

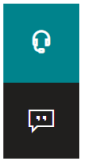
Overview Trainable classifiers Sensitive info types EDM classifiers Content explorer Activity explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

Filter on labels, info types, or categories

Sensitivity labels		All locations	
Highly Confidential/Merger and Acquisition	10	Export	4 items
Retention labels		<input type="checkbox"/> Name	Files
Retain 5yrs and Delete	75	<input type="checkbox"/> Exchange	1 >
PII Data - United States	9	<input type="checkbox"/> OneDrive	119 >
Trainable Classifiers		<input type="checkbox"/> SharePoint	74 >
Finance	201	<input type="checkbox"/> Teams	7 >
Targeted Harassment	89		
Agreements	60		
HR	54		
Legal Affairs	50		

Intelligence: Content explorer shows the exact list of documents & brings focus to blind spots



- Compliance Manager
- Data classification**
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Trials
- Solutions
 - Catalog
 - App governance
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - eDiscovery
 - Data lifecycle management
 - Information protection

Data classification

Overview Trainable classifiers Sensitive info types EDM classifiers Content explorer Activity explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

Filter on labels, info types, or categories

All locations > SharePoint > <https://m365x10870916.sharepoint.com/sites/Retail>

Ad Slogans.docx

Source Details

The actual number of items in this site/folder might be different from the calculated number that's displayed on the left

Export Search

Name	Sensitive info type	Trainable classifier
Contoso Electronic...	All Full Names	Finance
Electronics Store Tr...	All Full Names	Finance
<input checked="" type="checkbox"/> Ad Slogans.docx		Finance
CE Annual Report.d...	All Full Names	Finance
letter of intent_8.pdf	Types Of M... +1 more	Agreements
term sheet_4.pdf	Australian C... +5 more	Agreements
letter of intent_9.pdf	All Full Na... +2 more	Agreements
term sheet_1.pdf	All Full Na... +2 more	M&A

1 of 2

Content explorer with built in viewer, insights and analytics

Records management	Non disclosure agreement	1	term sheet_10.pdf	Agreements	Not a match	Match
--------------------	--------------------------	---	-------------------	------------	-------------	-------

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Trials

- Solutions**
- Catalog
 - App governance
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - eDiscovery
 - Data lifecycle management
 - Information protection
 - Information barriers
 - Insider risk management
 - Records management

Information protection > Finance (GLBA, FCRA, PCI, etc.)

Finance (GLBA, FCRA, PCI, etc.)

Turn on policy Restart simulation Edit policy Delete policy

Simulation overview Items to review

Review items that match your policy to decide whether the label will be applied to the right content. Files listed are a sample of the total matching files from each site included in the policy (up to 100 files per site). Matching emails will continue to appear here as they're sent to recipients.

Filter Reset Filters

Date match was detected: 1/2/2023-2/2/2023 Location: Any Rules: Any

Export Refresh 1 of 220 selected Customize columns

File name	Rule	Location	Sensitive info types
<input type="checkbox"/> SPDRquestforBidsEDUCATI...	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Finance
<input type="checkbox"/> Java_10.docx	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Finance
<input checked="" type="checkbox"/> Project Osiris Meeting Notes...	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Finance
<input type="checkbox"/> statement of wo... Project Osiris Meeting Notes.docx	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Statement of Work
<input type="checkbox"/> statement of work template ...	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Statement of Work
<input type="checkbox"/> statement of work template ...	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Statement of Work
<input type="checkbox"/> Python_47.docx	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Tax
<input type="checkbox"/> C#_18.docx	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Finance
<input type="checkbox"/> mark_taylor__24725__ClickIn...	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Finance
<input type="checkbox"/> richard_sanders__31773__Ice ...	Finance (GLBA, FCRA, PCI, etc.)	SharePoint	Finance

Project Osiris Meeting Notes.docx

Source Contextual Summary Metadata

Project Osiris Meeting Minutes
Osiris & Co.
(Board Meeting Minutes: April 21st, 2015)
(San Francisco, CA)

Project Members:
Present: Bhata Bhattacharia, Jon White Bear, Douglas Carver, Elizabeth Drucker, Pat Kyumoto, Jack Porter, Mary Rifkin and Leslie Zevon
Absent: Melissa Johnson
Quorum present? Yes

Others Present:
Exec. Director: Sheila Swanson
Other: Susan Johns, Consulting Accountant

Proceedings:
• Meeting called to order at 7:00 p.m. by Chair, Elizabeth Drucker
• (Last month's) meeting minutes were amended and approved

• Chief Executive's Report:
- Recommends that if we re-evaluate the performance of this month, the

Details

Policy name
Finance (GLBA, FCRA, PCI, etc.)

Status
Simulation complete

Simulation start date/time
01/11/2023

Description
1. Business - Finance 2. Business - Tax 3. Bank statements 4. Budgets 5. Financial audit reports 6. Financial statements 7. Loan agreements 8. Statements of work 9. Invoices

Label and policy settings
Label Confidential/Internal
Exchange overwrite label false

Trainable Classifier
Invoice
Statement of Work
Financial statement
Bank statement
Loan agreements and offer letters
Financial Audit Reports
Budget
Finance
Tax

Apply to content in these locations
Exchange email All
SharePoint sites All
OneDrive accounts All

Exclude content from these locations
Exchange email None
SharePoint sites None
OneDrive accounts None

Rules for auto-applying this label

Intelligence: Simulation mode to build confidence around effectiveness of policy before broad rollout



Communication site

TestLabelPublish

Share

Home Documents Pages MsoDataStore X-Tenant Labels DoclibDefaultGeneral DocDefaultLabel1 Bulk Download Test test UDP CoAuth ... Edit

+ New
Upload
Edit in grid view
Sync
Add shortcut to OneDrive
Pin to Quick access
Export to Excel
All Documents

Documents

Name	Modified	Modified By	Sensitivity	+ Add column
348-295-SchoollmmReqforParents2019-20...	June 7	Admin Admin	Highly Confidential \ High	
348-295-SchoollmmReqforParents2019-20...	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	
CC_1a.pdf	Sunday at 10:41 PM	Admin Admin	Highly Confidential \ High	
ContosoNoLabelUploadTest.pdf	July 4	Admin Admin	Gen	This file has been automatically labelled
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	

Autolabeling in PDF

Document12.docx	May 9	Admin Admin	General	
-----------------	-------	-------------	---------	--

AutoSave Off Document1 - Word Search Miriam Graham

File Home Insert Draw Design Layout References Mailings Review View Help

Comments Editing Share

Undo Clipboard Font Paragraph Styles Editing Voice 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

Amazon S3 Client Secret Access Key

Samples:

```
string AmazonWebServicesSecretToken = "abcdefghijklmnpqrst0123456789/+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: Office document with popup notification of autolabeling action

Microsoft Purview Data Loss Prevention

Cloud native with built-in protection

Save cost and scale effectively



Cloud managed and delivered, no on-premise infrastructure or agents needed



Built-in experiences in Microsoft 365 apps and services, Windows endpoints, On-premises



Extend protection to non-Microsoft applications and platforms

Data classification service



Sensitive Info Types (SITs)
Trainable Classifiers
Context-based Classification
Coming to Private Preview Jan 2023

Named Entities
Exact Data Match
Credentials SITs

Sensitivity Labels



Public

Confidential

General

...

Microsoft 365



Endpoints



Non-Microsoft apps



On-premises

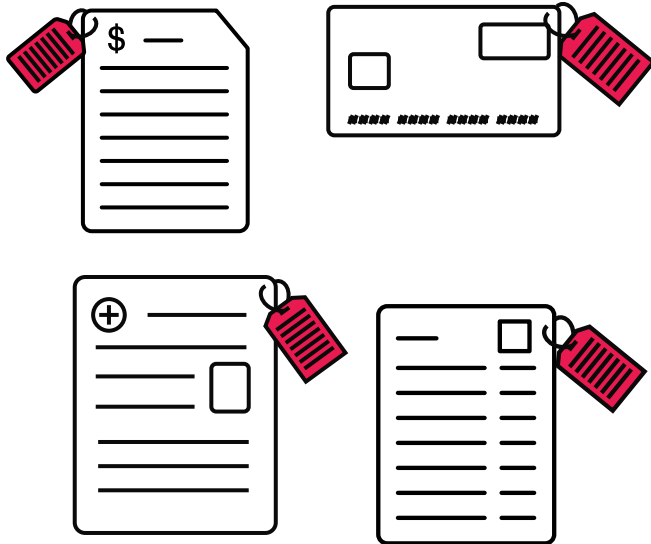


Integrated insights and alerting

Enrich policy and investigation with rich signals

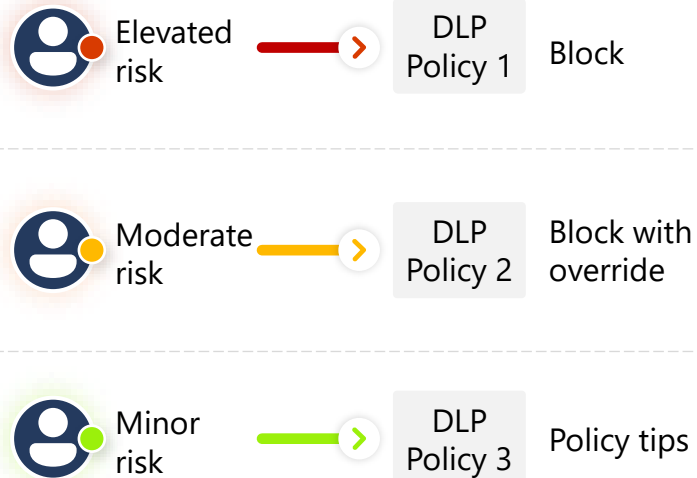
Know the context

Leverage classification and labeling on sensitive data from Information Protection



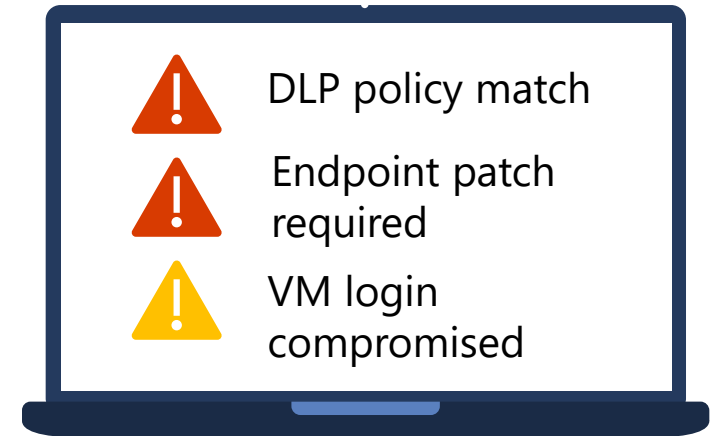
Understand the intent

Automatically apply risk insights from Insider Risk Management to DLP policies



Integrate alert investigation

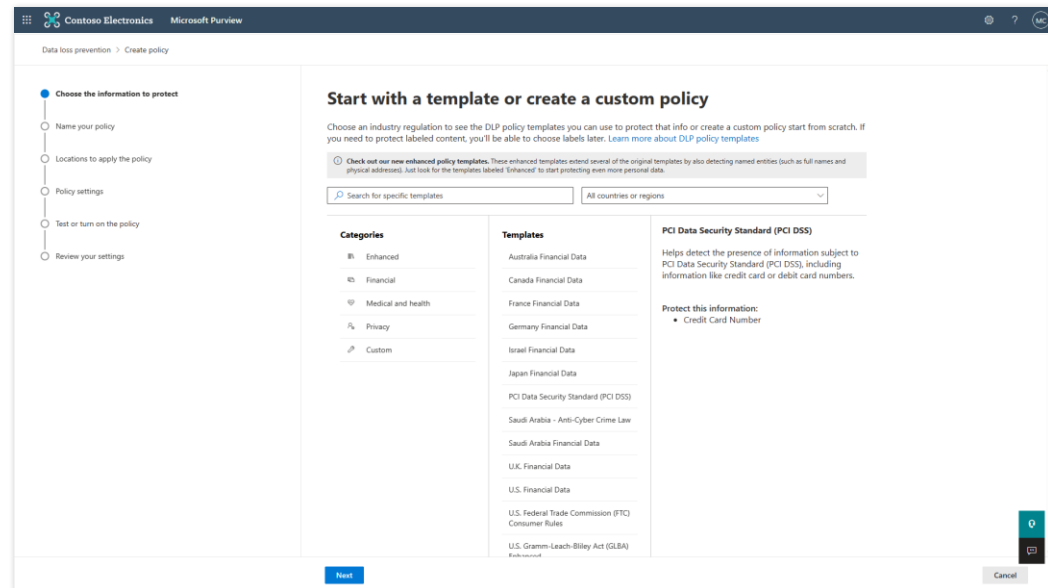
Integrate DLP alerts with Microsoft 365 Defender and Sentinel for richer investigation experience



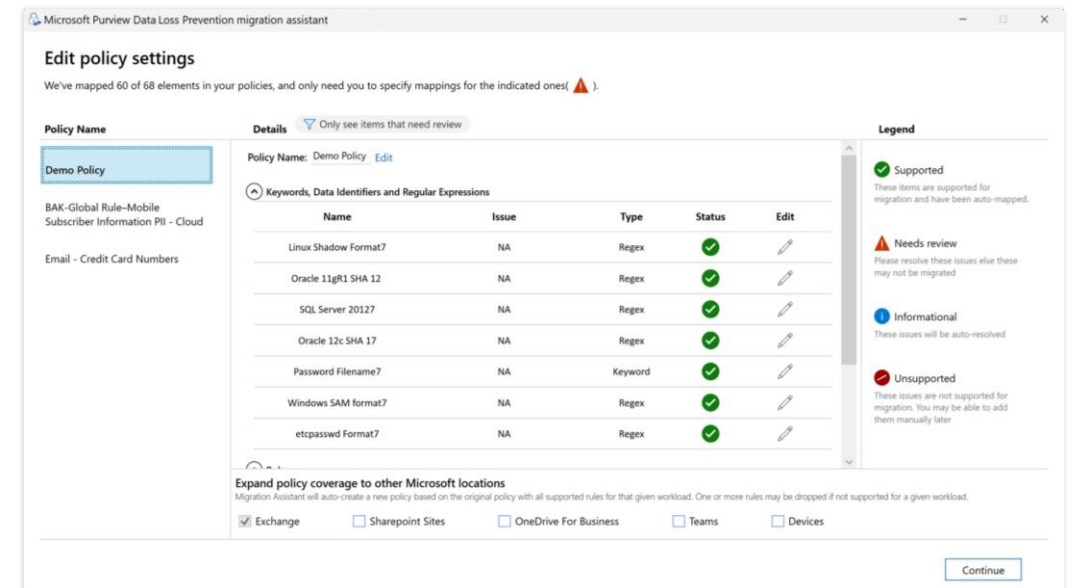
Easy to get started

Enrich policy and investigation with rich signals

Pre-built templates for common regulations such as GDPR, HIPAA, PCI-DSS with sensitive information types and default-policies



Migration assistant to help migrate existing Symantec DLP policies to Microsoft Purview DLP with minimal effort



- Choose the information to protect
- Name your policy
- Locations to apply the policy**
- Policy settings
- Test or turn on the policy
- Review your settings

Choose locations to apply the policy

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

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

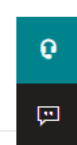
Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Devices	All Choose user or group	None Exclude user or group
<input checked="" type="checkbox"/> On	Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
<input checked="" type="checkbox"/> On	On-premises repositories	All Choose repositories	None Exclude repositories
<input type="checkbox"/> Off	Power BI (preview)		

Unified DLP policy that can work across all workloads

Back

Next

Cancel



- Choose the information to protect
- Name your policy
- Locations to apply the policy**
- Policy settings
- Test or turn on the policy
- Review your settings

Choose locations to apply the policy

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

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisites capability. [Learn more about the prerequisites](#)

Status	Location	Included
<input checked="" type="checkbox"/> On	Exchange email	1 distribution group Choose distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group
<input checked="" type="checkbox"/> On	Devices	All Choose user or group
<input checked="" type="checkbox"/> On	Microsoft Defender for Cloud Apps	All Choose instance
<input checked="" type="checkbox"/> On	On-premises repositories	All Choose repositories
<input type="checkbox"/> Off	Power BI (preview)	

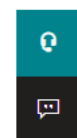
Microsoft Defender for Cloud Apps

0 items

Select all

- Box - Box - US
- Box - Box - General
- Salesforce - Salesforce - US
- Salesforce - Salesforce - EU
- Salesforce - Salesforce - General
- Dropbox - Dropbox - US
- Dropbox - DropBox [Deprecated]
- Dropbox - DropBox - EU
- Dropbox - box (depracated)
- Dropbox - Dropbox - General
- G Suite - G Suite - US
- G Suite - G Suite - General

Extending DLP policy to non-Microsoft apps through Microsoft Defender for Cloud Apps



- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings**
- Advanced DLP rules
- Test or turn on the policy
- Review your settings

Create rule

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely

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 D

Upload to a restricted cloud service domain or access from an unallowed browsers

+ Configure sensitive service domain exceptions

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

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

Copy to clipboard

+ Choose different copy to clipboard restrictions

Copy to a USB removable media

+ Choose different USB removable media restrictions

Copy to a network share

+ Choose different network share restrictions

Print

+ Choose different print restrictions

Configure USB removable media restrictions

When this activity is detected on devices, you can configure exceptions to the overall enforcement action with network exceptions or USB removable media group restrictions.

Network exceptions

Name	Action
<input type="checkbox"/> Corporate network	Audit only
<input type="checkbox"/> VPN	
<input type="checkbox"/> Apply to all activities	

But USB group G1 is configured to block

Removable media group restrictions

+ Add group Reorder Clear selection

Group	Priority	Action
<input type="checkbox"/> G1	1	Block

Copy to USB activity is default Audit

Ability to create groups of USBs and apply different restrictions to each groups

Save Cancel

Save Close



- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Locations to apply the policy
- Policy settings**
- Advanced DLP rules
- Test or turn on the policy
- Review your settings

Create rule

Name *

GLBA

Description

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Default

Any of these

Add

Sensitive info types

Sensitivity labels

Trainable classifiers

Exceptions

We won't apply this rule to content that matches any of these exceptions.

+ Add exception

Actions

Use actions to protect content when the conditions are met.

+ Add an action

Save

Cancel

Leveraging SITs and advanced classification techniques in DLP policies



- ✓ Name your policy
- ✓ Locations to apply the policy
- **Advanced DLP rules**
- Test or turn on the policy
- Review your settings

Create rule

Name *

Description

Conditions

Quick summary

Content contains any of: Credit Card Number

And

Not

RecipientDomainMatch: fabrikam.com

Or

FromMemberOf: FinanceTeam@contoso.com

Configured to detect the presence of credit card numbers in an email unless the email is either sent from the Finance team or is sent to a whitelisted recipient domain fabrikam.com

Actions

Use actions to protect content when the conditions are met.

+ Add an action

User notifications

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

Off

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

User overrides

Allow overrides from M365 services

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

Ability to create composite conditions in DLP policy rules

Save Cancel



Incidents

Email notification New incidents queue

Most recent incidents and alerts

Manage incidents

Search for name or ID

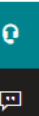
Filter

Customize columns

30 Days

<input type="checkbox"/>	<input type="checkbox"/>	Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service Sources	Detection Sources	First activity	Last
<input type="checkbox"/>	>	Exfiltration incident involving one user	227		Low	1 investigation states	Exfiltration	admin	2/2	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 30, 2022 4:17 AM	May
<input type="checkbox"/>	>	Exfiltration incident involving one user	225		Low	1 investigation states	Exfiltration	admin	2/2	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 23, 2022 10:16 AM	May
<input type="checkbox"/>	>	Exfiltration incident involving one user	222		Low	1 investigation states	Exfiltration	admin	2/2	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 18, 2022 9:28 AM	May
<input type="checkbox"/>	>	DLP policy (customPolicyTip) matched for email with subject (Cr...	224		Low	1 investigation states	Exfiltration	admin	1/1	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 13, 2022 7:36 PM	May
<input type="checkbox"/>	>	DLP policy (customPolicyTip) matched for email with subject (Cr...	221		Low	1 investigation states	Exfiltration	admin	1/1	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 12, 2022 5:11 PM	May
<input type="checkbox"/>	>	DLP policy (customPolicyTip) matched for email with subject (Cr...	220		Low	1 investigation states	Exfiltration	admin	1/1	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 11, 2022 10:07 AM	May
<input type="checkbox"/>	>	DLP policy (IP Address Policy) matched for email with subject (T...	219		Medium	1 investigation states	Exfiltration	admin	1/1	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 10, 2022 1:50 AM	May
<input type="checkbox"/>	>	Exfiltration incident involving one user	217		Low	1 investigation states	Exfiltration	admin	2/2	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 8, 2022 11:13 PM	May
<input type="checkbox"/>	>	DLP policy (Credit card Policy) matched for email with subject (...)	216		Low	1 investigation states	Exfiltration	admin	1/1	Microsoft Data Loss Pr...	Microsoft Data Loss Pr...	May 5, 2022 10:35 PM	May

DLP alerts in Microsoft 365 Defender portal to facilitate a unified incident investigation



Incidents > DLP policy (Credit card policy) matched for document (Credit Card.pdf) in a device

- The MDE SIEM API deprecation that was announced earlier this year has been postponed for now, more details expected in Q3, 2022.
- Part of incident: DLP policy (Credit card policy) matched for document (Credit Card.pdf) in a device on one endpoint [View incident page](#)

admin desktop-7t4agd3
Windows11

ALERT STORY

What Happened

ShortEvidence2 DLP was involved in DLP policy violations.

Policy description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

[View policy \(tab out\)](#)

Policy matches found in this violation

Info type	Matches
Credit Card Number	1

Related events

Event	User	Time detected	Location
Sensitive info in 'Credit Card.pdf' - File...	admin@ShortEviden...	Sep 9, 2022 2:34 AM	Endpoint

Back to alert details

Sensitive info in 'Credit Card.pdf' - File printed

Details Sensitive info types

Info ty...	Matched sensitive content	Surrounding characters
Number	4485 3647 3952 7352	Credit card Visa: 4485 3647 3952 7352 Expires: 2/2009

Matched sensitive content in Alerts view for quick triage and investigation

Microsoft Purview Insider Risk Management

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.



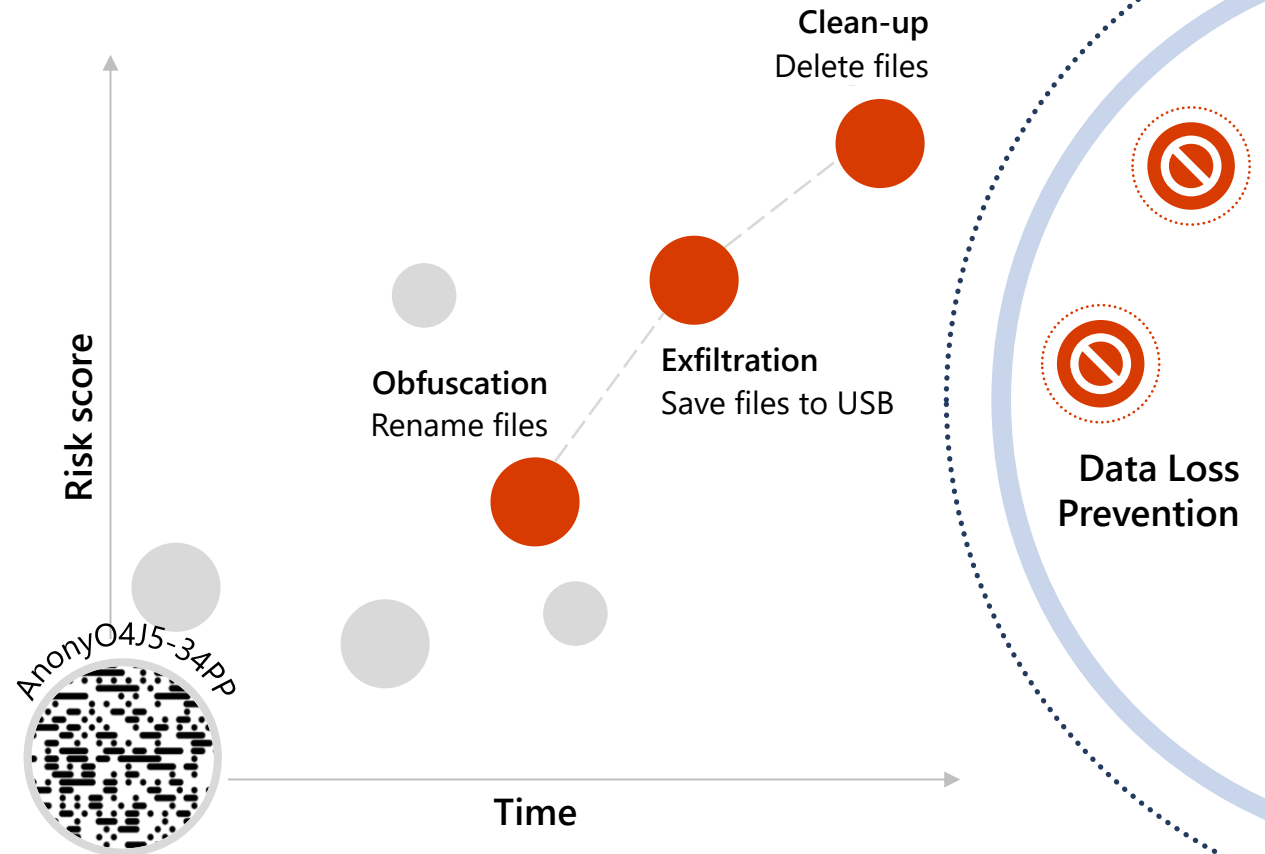
Simplicity

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.

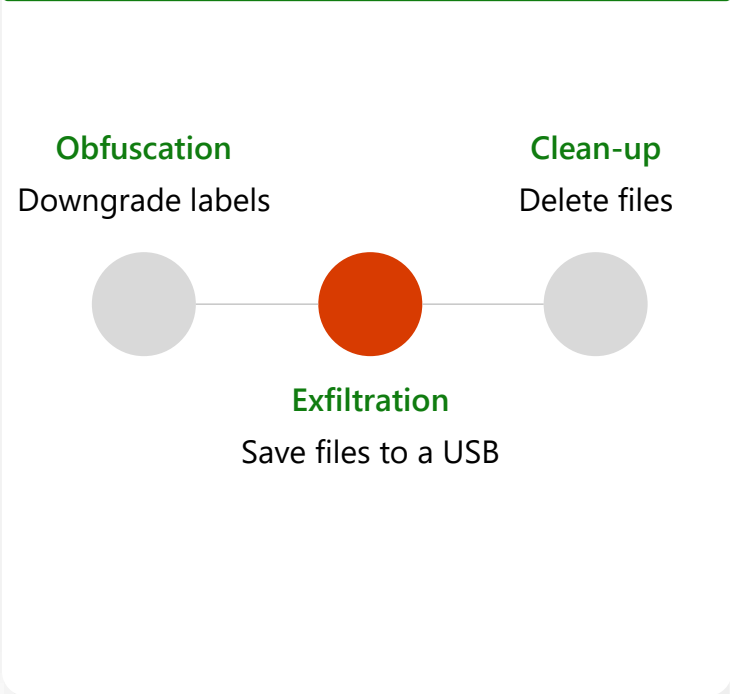


Leveraging machine learning to identify the most critical insider risks among noisy signals

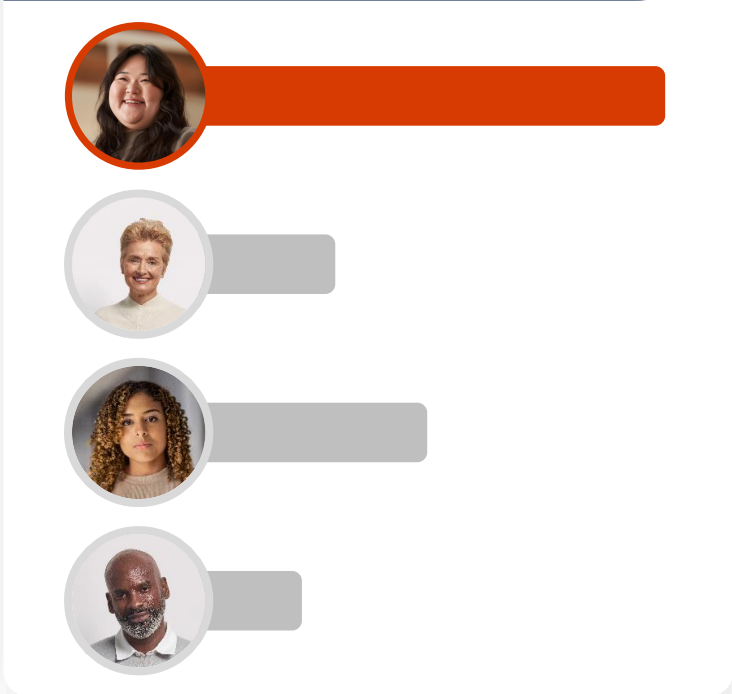
Know the context Correlate data signals



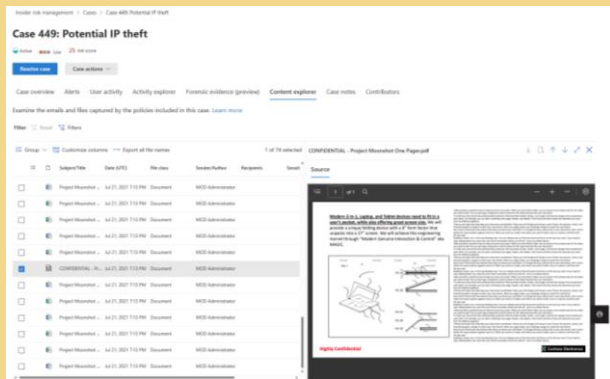
Understand the intent Sequence detection



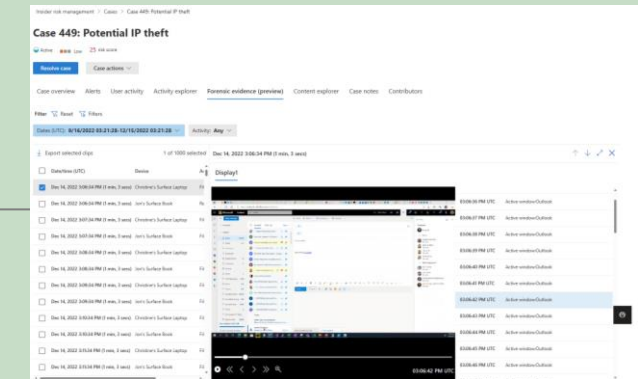
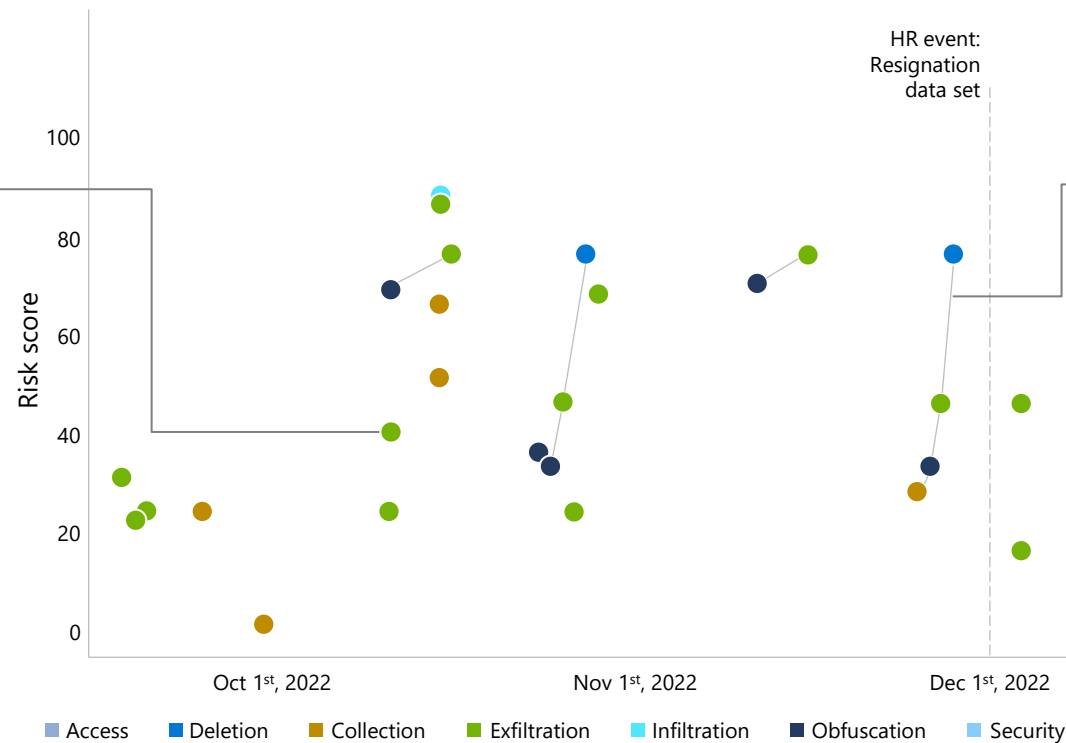
Benchmarking Anomaly detection



Enable thorough investigations with **interactive and enriched visual insights**



Admins can easily understand what content was exfiltrated



Get and collect forensic evidence to gain visual insights into user activities that may lead to security incidents

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](#)

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

1.1% of users per
0.8% of users dow
0.7% of users sha
organization

4.6% of users with
involving sensitive
3.2% of users with
files
2.7% of users with
with people outsid

Potential data theft activities

[Close panel](#)

The exfiltration activities below might be related to data theft by departing users near their resignation or termination date. After reviewing them, consider setting up the recommended policy to help address potential risks.

What we detected

The following is recent activity based on a scan of 219 users who are leaving your organization.

5.9% of users with a resignation date performed exfiltration activities

- 5% of users with a resignation date showing anomalous exfiltration activity volume
- 4.6% of users with a resignation date performed activities involving sensitive info
- 3.7% of users with a resignation date performed sequential activities that might indicate suspicious exfiltration behavior
- 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
- 2.3% of users with a resignation date shared SharePoint folders with people outside your organization
- 2.3% of users with a resignation date emailed people outside your organization
- 1.8% of users with a resignation date copied content to USB
- 1.8% of users with a resignation date printed a large number of files
- 1.4% of users with a resignation date shared SharePoint files with people outside your organization
- 1.4% of users with a resignation date copied sensitive content to personal cloud
- 0.9% of users with a resignation date shared files across network

Recommendation

Create a 'Data theft by departing users' policy that detects data theft by users near their resignation or termination date, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

[Get started](#)

[Close](#)

Quick start with one click to see insights in 48 hours

User privacy is protected as results are presented as aggregated insights

Easy to get started with recommended quick policies

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Roles & Scopes
- Trials

Insider risk management > Alerts > Alert: Confidentiality obligation during departure

Alert: Confidentiality obligation during departure

Needs review [Confirm alert to an existing case](#) [Dismiss alert](#)

High Risk score: 87/100 Alert created on Feb 22, 2022

Activity that generated this alert [Reduce alerts for this activity](#)

Data infiltration: Files downloaded from unallowed site
 87/100 High severity | May 16, 2022 (UTC) | [View forensic evidence](#)
 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 ⓘ

Feb 21, 2022 (UTC)
 An HR connector imported a resignation date for this user.

User details

High potential impact - boosts alert score by 10 points

Anony85KF-34DF

[View all details](#)

User alert history

Last 30 days

No alert history

[View full user history](#)

Potential high-impact users

All risk factors Activity explorer User activity Forensic evidence (preview)

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 detection

Cumulative exfiltration activities ⓘ

High severity cumulative exfiltration activities detected (Risk score: 82/100)

User activity detected ranges from 05/15 - 05/16

All exfiltration activities with prioritized content		Shared SharePoint files externally	
More events than 90% compared to teammates.		More events than 99% compared to users that access same SharePoint sites.	
User	467	User	20
Teammates	2	Users who access same SharePoint sites	9

[View all cumulative exfiltration activities](#)

Sequences of activity

1 sequence activity

[View all sequence activity](#)

Leverage machine learning to identify critical risks

No activity is considered unusual for this user

No activity includes events with priority content

Unallowed domains

2 activities include events with unallowed domains

- 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

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.

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**

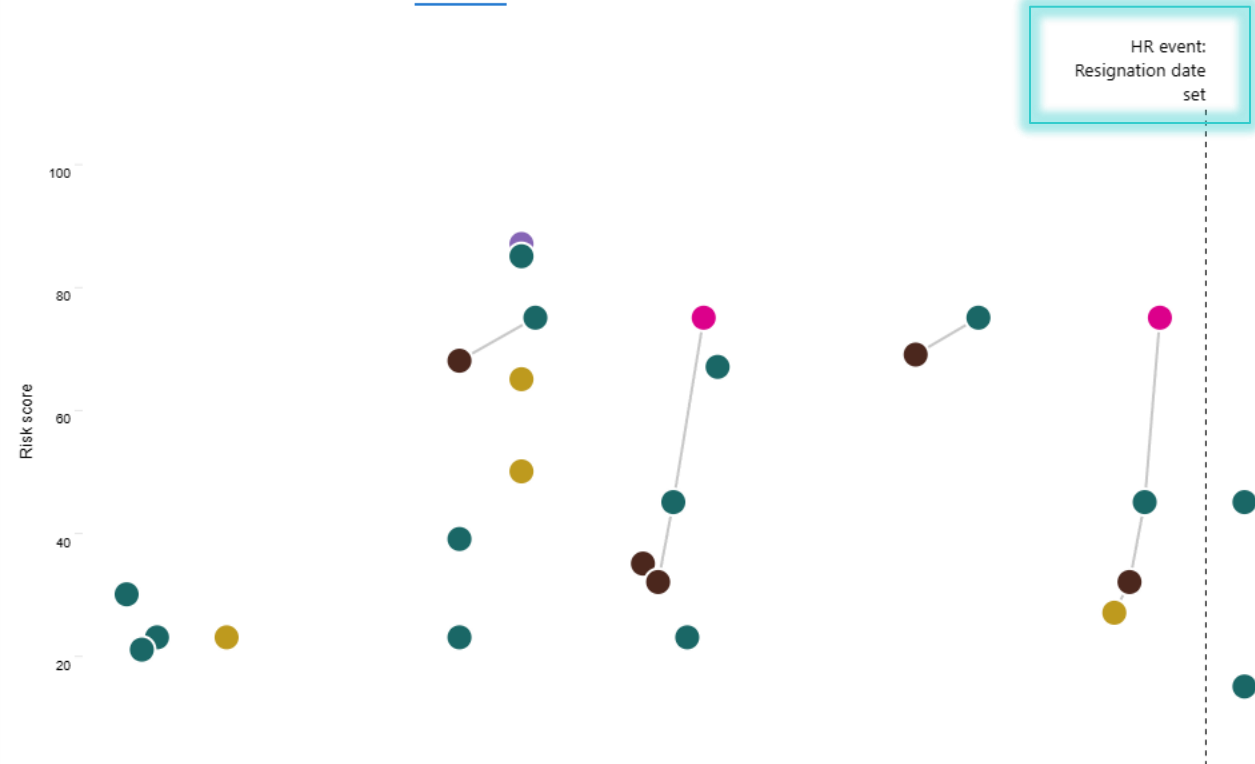
Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 45/100

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.

21 events: All exfiltration activities: More events than 78% compared to users with same job title.

User activity scatter plot 6 Months 3 Months 1 Month



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

Case 449: Potential IP theft

Active Low 25 risk score

Resolve case Case actions

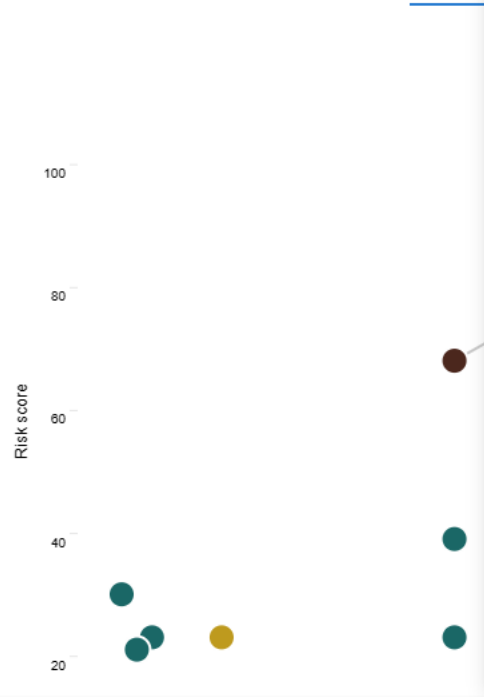
Case overview Alerts User activity Activity explorer Forensic evidence (preview) Content exp

Filter: Risk category: Any Activity Type: Any Reset all

Sort by: Date occurred

User activity scatter plot 6 Months 3 Months

- 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.



(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 (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)
2 events: Files with priority file extensions, including: docx (Explore content)

Deletion: Files deleted
Nov 24, 2022 (UTC) | Risk score: 75/100 | View forensic evidence
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 | View forensic evidence
2 events: Files printed
2 events: Files containing sensitive info, including: Credit Cards

Obfuscation: Files renamed
Nov 22, 2022 (UTC) | Risk score: 32/100 | View forensic evidence
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 (Explore content)
2 events: Files containing sensitive info, including: Credit Cards (Explore content)
34 events: Files that have labels applied, including: Confidential (Explore content)

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	Sensit
<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		
<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.

Highly Confidential

Contoso Electronics

Review the exfiltrated content easily in its native view

- 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

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 explorer Case notes Contributors

Filter Reset Filters

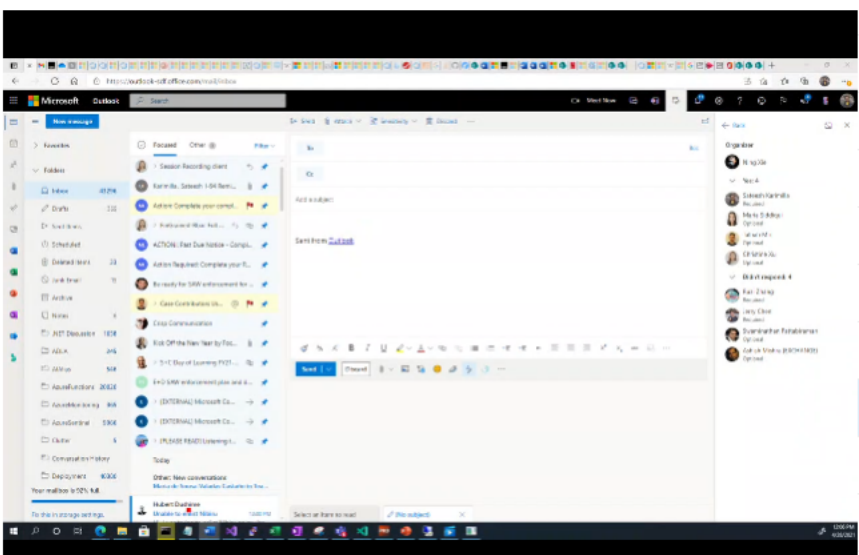
Dates (UTC): 9/16/2022 03:21:28-12/15/2022 03:21:28 Activity: Any

Export selected clips 1 of 1000 selected

<input type="checkbox"/>	Date/time (UTC)	Device	Action
<input checked="" type="checkbox"/>	Dec 14, 2022 3:06:34 PM (1 min, 3 secs)	Christine's Surface Laptop	File
<input type="checkbox"/>	Dec 14, 2022 3:06:34 PM (1 min, 3 secs)	Jon's Surface Book	Re
<input type="checkbox"/>	Dec 14, 2022 3:07:34 PM (1 min, 3 secs)	Christine's Surface Laptop	File
<input type="checkbox"/>	Dec 14, 2022 3:07:34 PM (1 min, 3 secs)	Jon's Surface Book	File
<input type="checkbox"/>	Dec 14, 2022 3:08:34 PM (1 min, 3 secs)	Christine's Surface Laptop	File
<input type="checkbox"/>	Dec 14, 2022 3:08:34 PM (1 min, 3 secs)	Jon's Surface Book	File
<input type="checkbox"/>	Dec 14, 2022 3:09:34 PM (1 min, 3 secs)	Christine's Surface Laptop	File
<input type="checkbox"/>	Dec 14, 2022 3:09:34 PM (1 min, 3 secs)	Jon's Surface Book	File
<input type="checkbox"/>	Dec 14, 2022 3:10:34 PM (1 min, 3 secs)	Christine's Surface Laptop	File
<input type="checkbox"/>	Dec 14, 2022 3:10:34 PM (1 min, 3 secs)	Jon's Surface Book	File

Dec 14, 2022 3:06:34 PM (1 min, 3 secs) ↑ ↓ ↗ ✕

Display1



03:06:36 PM UTC	Active window:Outlook
03:06:37 PM UTC	Active window:Outlook
03:06:38 PM UTC	Active window:Outlook
03:06:39 PM UTC	Active window:Outlook
03:06:40 PM UTC	Active window:Outlook
03:06:41 PM UTC	Active window:Outlook
03:06:42 PM UTC	Active window:Outlook
03:06:43 PM UTC	Active window:Outlook
03:06:44 PM UTC	Active window:Outlook
03:06:45 PM UTC	Active window:Outlook
03:06:46 PM UTC	Active window:Outlook
03:06:47 PM UTC	Active window:Outlook

Get visual insights into potential security incidents from managed devices

Enable Adaptive Protection with Microsoft Purview

Optimize data protection automatically

Context-aware detection

Identify the most critical risks with ML-driven analysis in Insider Risk Management

Dynamic controls

Enforce effective DLP controls on high-risk users while others maintain productivity

Automated mitigation

Minimize the impact of potential data security incidents and reduce admin overhead

Insider Risk Management

Detect risky users and assign risk levels

Data Loss Prevention

Dynamically apply preventative controls



DLP Policy 1



DLP Policy 2



DLP Policy 3



Rebecca, a marketing manager who's working on a confidential launch campaign for Contoso corporation.



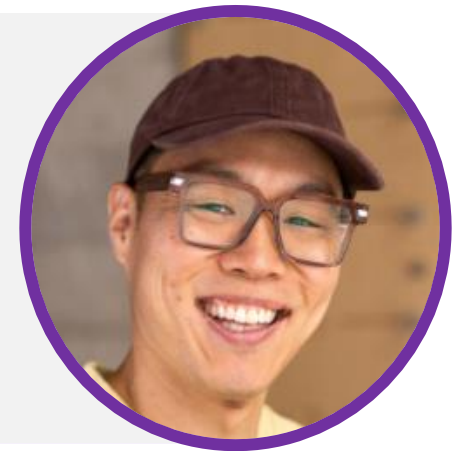
Rebecca printed confidential information and was blocked with the right to override

Why did the same action result in two different controls?

Chris printed confidential information and was blocked



Chris, a data admin who's working on the same confidential project for Contoso corporation.

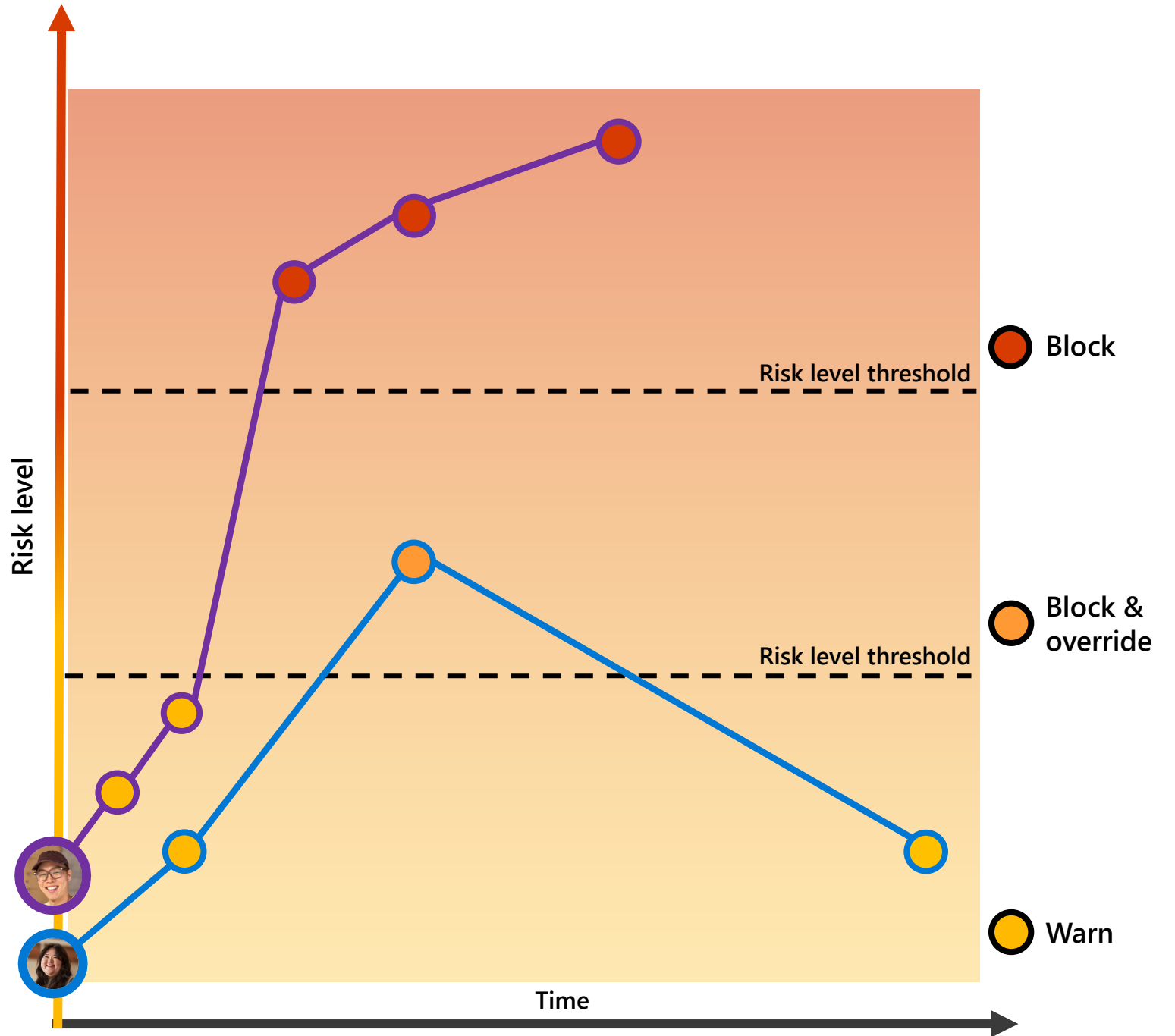




- » Detected as a potential high impact user due to his level in the organization and the Azure Active Directory admin role
- » Downgraded sensitivity labels on an unusual volume of SharePoint files prior to downloading them
- » Submitted resignation
- » Tried to print confidential files
- » Tried to copy confidential files to an USB drive



- » Shared an unusual volume of sensitive information via Teams
- » Printed confidential files and override the block with a valid business justification
- » Emailed a confidential file to a PR agency after a period of non-concerning activities



Insider risk management

- Overview
- Alerts
- Cases
- Policies
- Users
- Forensic evidence requests
- Notice templates
- Adaptive protection

- Summary
- Insider risk levels**
- Users in scope
- DLP policies

Insider risk levels

Configure your settings and insider risk conditions for adaptive protection

Select the insider risk management policy to use for the risk levels

Test DRP IRM Policy

Configure risk levels

You can select an out-of-box level configuration, or you can customize for each level.

	Elevated risk level	Custom elevated risk level
	Moderate risk level	Custom moderate risk level
	Minor risk level	Custom minor risk level

Past activity detection

Determines how far back adaptive protection will go to detect if a user meets the conditions for a risk level. This only applies for risk levels that are based on a user's daily activity.

7 days of previous activity

Insider risk level timeframe

Determines how long an insider risk level will remain assigned to a user before it is reset. (Maximum 30 days)

30 days

Data loss prevention > Edit policy

- Name your policy
- Locations to apply the policy
- Advanced DLP rules**
- Test or turn on the policy
- Review your settings

Create rule

Use rules to define the type of sensitive information you data protect. If content matches many rules, the most restrictive one will be enforced.

Name *

Description

Conditions

We'll apply this policy to content that matches these conditions.

Risk levels for Adaptive Protection

You must select at least one insider risk level. This policy will then be scoped to match the custom insider risk management levels in adaptive protection.

Select one or more insider risk levels

Select at least one level

- Elevated risk level – risk level is defined in Insider Risk Management
- Moderate risk level – risk level is defined in Insider Risk Management
- Minor risk level – risk level is defined in Insider Risk Management

Exceptions

We won't apply this rule to content that matches any of these exceptions.

+ Add exception

Actions

Use actions to protect content when the conditions are met.

+ Add an action

User notifications

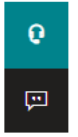
Use notifications to inform your users and help educate them on the proper use of sensitive info.

Off

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

User overrides

Set up Adaptive Protection to mitigate the most critical risks with the most effective DLP policy, saving security teams valuable time while ensuring better data security



Secure data in the age of AI with Microsoft Purview

Unparalleled visibility

Understand risks associated with sensitive data usage and user activity context across AI applications in your environment

Comprehensive protection

Employ ready to use and customizable policies to prevent data loss in AI prompts and protect data in AI responses

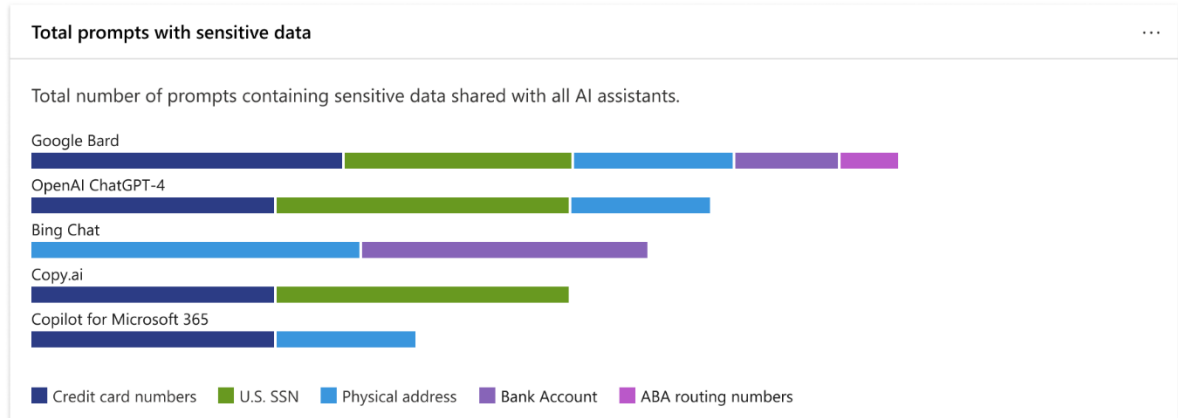
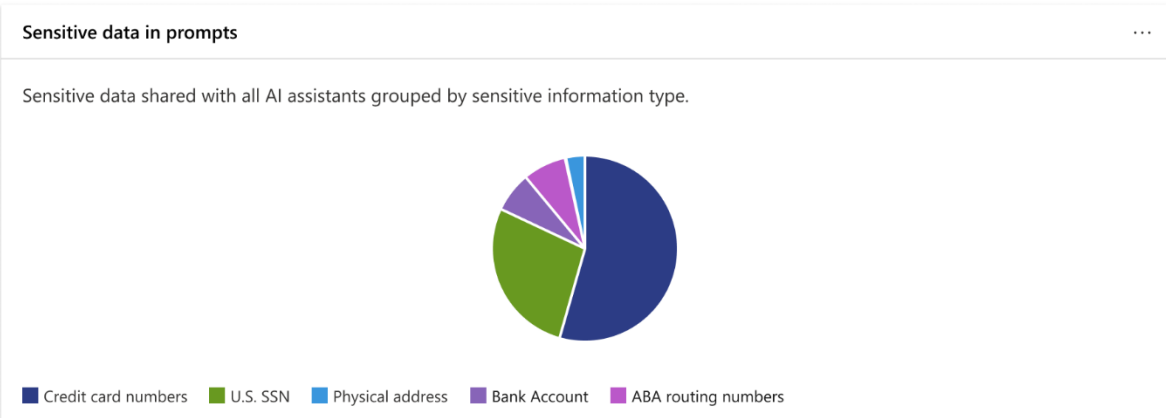
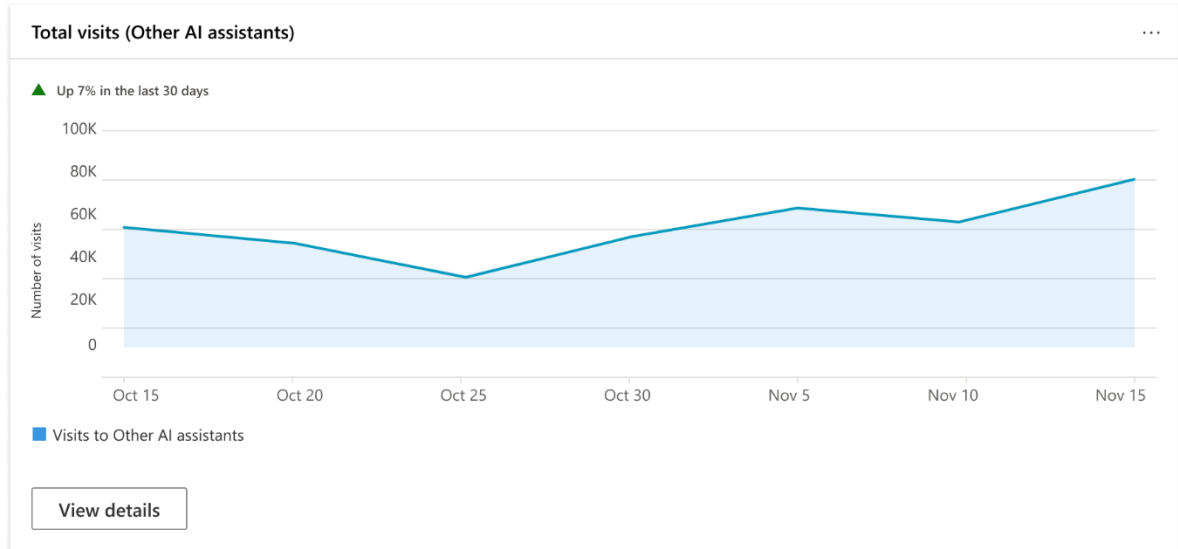
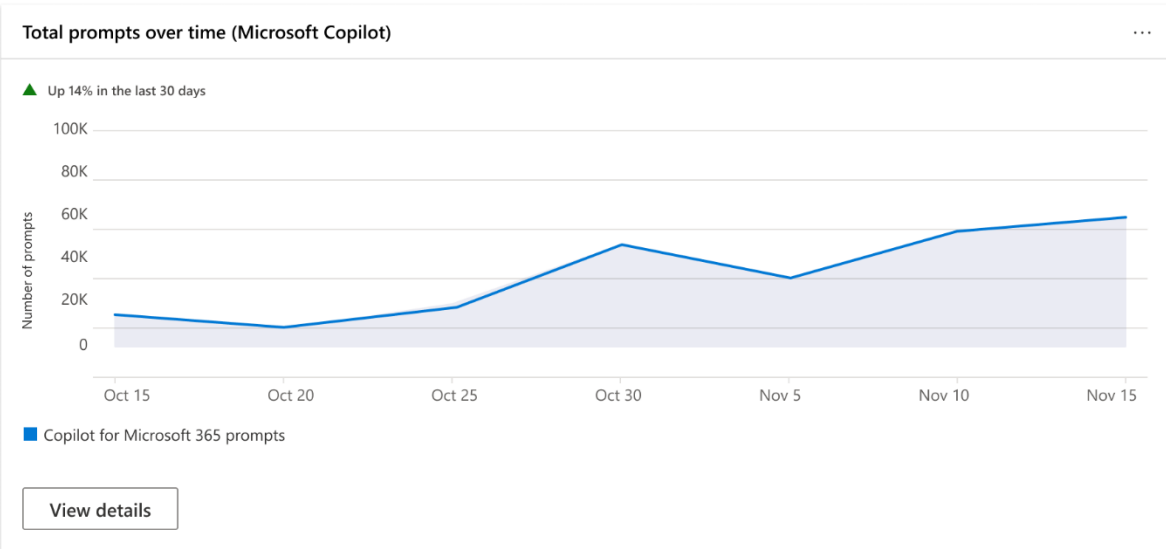
Compliance controls

Apply optimal data handling and storing policies to help meet business and regulatory requirements

AI hub (preview)

Analytics Policies Activity explorer

AI hub in Microsoft Purview provides insights to help security teams gain comprehensive visibility into data security risks.



Solutions

Catalog

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Insider risk management

Records management

Privacy risk management

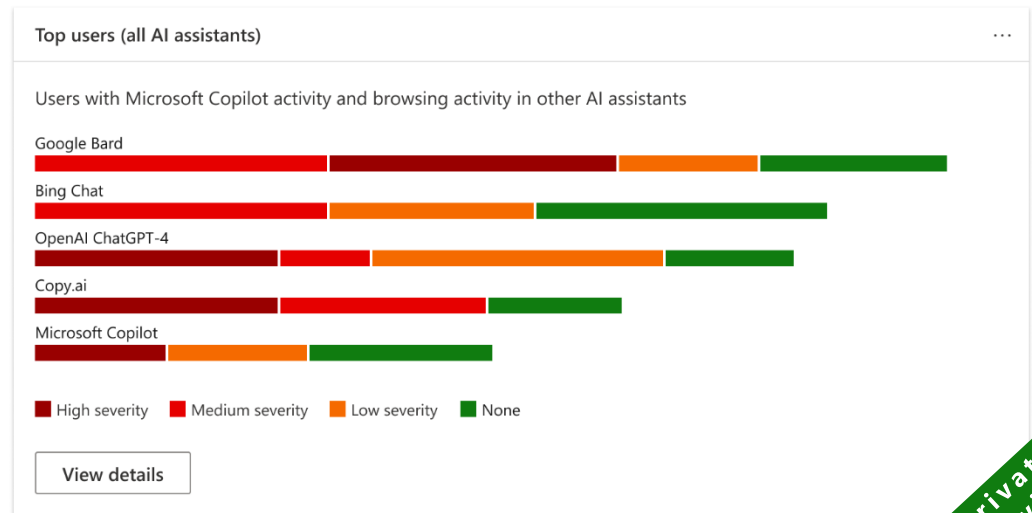
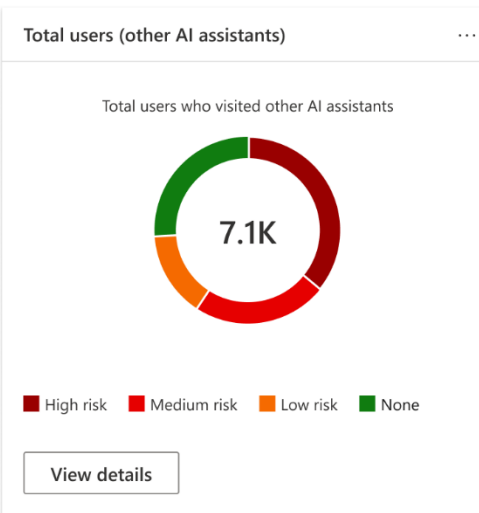
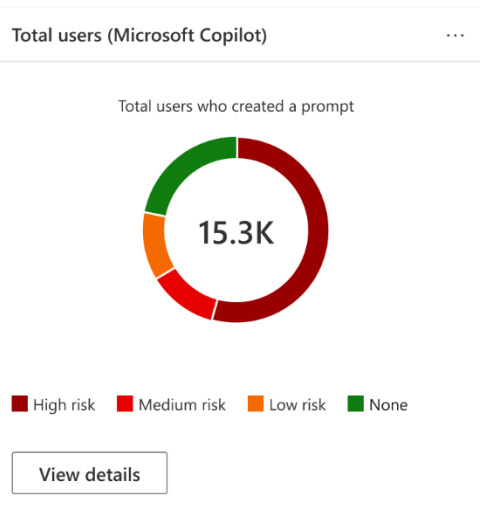
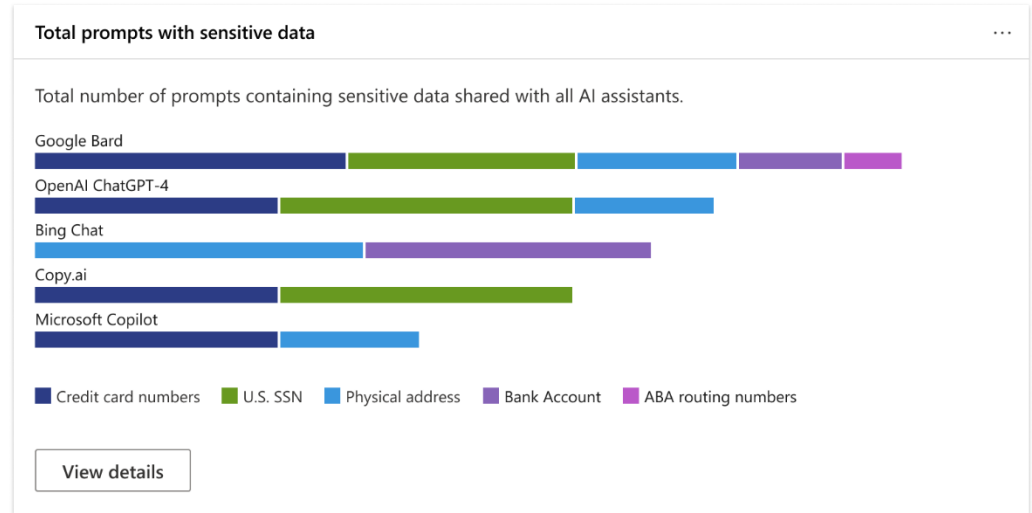
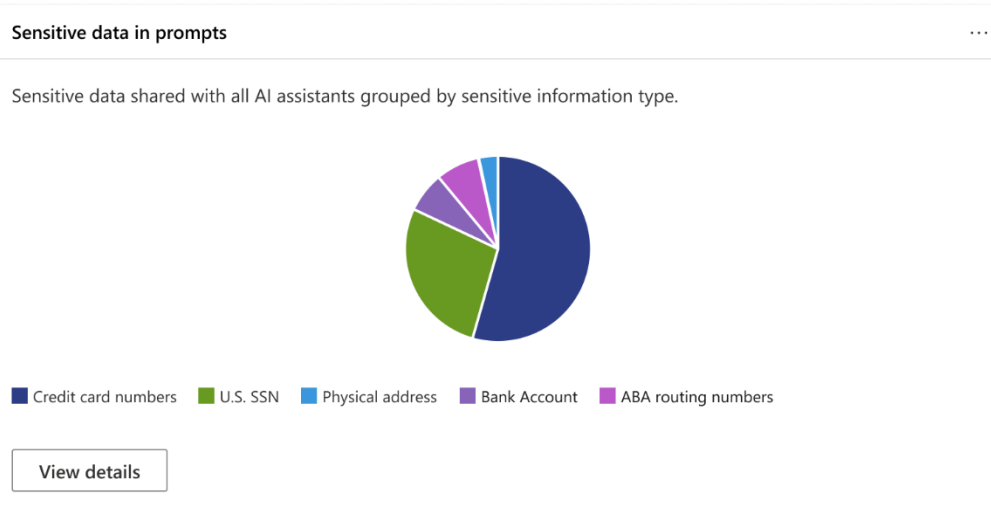
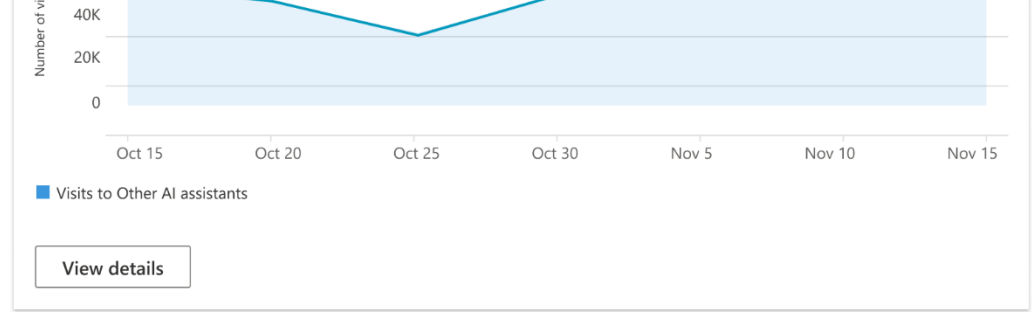
Subject rights request

Settings

More resources

Customize navigation

Show less



- Home
- Ai Hub**
- Compliance Manager
- Data classification
- Data Connectors
- Alerts
- Reports
- Policies
- Permissions

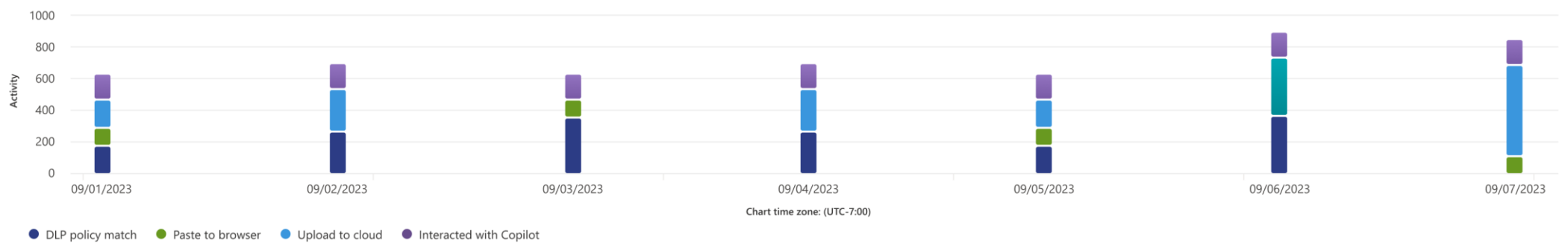
- Solutions**
- Catalog
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - eDiscovery
 - Data lifecycle management
 - Information protection
 - Insider risk management
 - Records management

AI hub (preview)

Recommended actions Settings Learn more

Analytics Policies Activity explorer

Activity: All values User: All values DLP policy matched: All values Sensitive info type: All values Add filter Reset all



<input type="checkbox"/>	Activity	User	Time happened	Device full name	Enforcement mode	Sensitive info type	File sensitivity label	DLP policy matched	DLP rules matched	File name
<input type="checkbox"/>	File upload to cloud	Mona Kane	Sep 01, 2023 3:54 PM	Desktop-3453HD	Audit	Credit card number	Confidential	AI hub – Data Protection	Audit-UploadToCloud	CCnumbers_08-2023.txt
<input type="checkbox"/>	Paste to browser	Dean Renzo	Sep 01, 2023 3:54 PM	Desktop-363345HD	Audit	Social security number		AI hub – Data Protection	Audit-PasteToBrowser	
<input type="checkbox"/>	File upload to cloud	Edison Gili	Sep 02, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidential	AI hub – Data Protection	Audit-UploadToCloud	AddressList_08-2022.xls
<input type="checkbox"/>	Interacted with Copilot	Sarah Terry	Sep 03, 2023 3:54 PM		Audit	Credit card number				
<input type="checkbox"/>	File upload to cloud	Posie Par	Sep 03, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidential	Purview for AI – Data Protection	Audit-UploadToCloud	AddressList_08-2022.xls
<input type="checkbox"/>	Interacted with Copilot	Dean Renzo	Sep 05, 2023 3:54 PM		Audit	Social security number				
<input type="checkbox"/>	Paste to browser	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account		Purview for AI – Data Protection	Audit-PasteToBrowser	
<input type="checkbox"/>	Interacted with Copilot	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account		Purview for AI – Data Protection	Audit-PasteToBrowser	
<input type="checkbox"/>	Paste to browser	Mona Kane	Sep 13, 2023 3:54 PM	Desktop-ASFD213	Audit	Credit card number		AI hub – Data Protection	Audit-UploadToCloud	

