

Estrategias para lanzar un plan de gobernanza de datos eficaz con Microsoft Purview

Seguridad integral de los datos

Pablo Liquez

SC-100, SC-200, SC- 900, AZ-300, AZ-301, AZ-500, AZ-104, MCT

Guatemala

Regional Cybersecurity Presales Architect



Inteligencia Artificial

Las empresas que utilizan la IA y la automatización para detectar y responder a las brechas de datos ahorran una media de 3 millones de dólares en comparación con las que no lo hacen.

En ambos bandos

En 2023, más delincuentes usarán los algoritmos de IA para identificar sistemas con una seguridad débil.

Para 2030 el mercado de productos de ciberseguridad con IA tendrá un valor cercano a los 139.000 millones de dólares, lo que supone un aumento de casi diez veces el valor del mercado de 2021.



Los 'piratas' de la 'Dark Web', al acecho del control de ChatGPT

tan sobre riesgos de 'ChatGPT'



Primera modificación: 03/03/2023 - 03:47

Home > Tecnología

He probado a 'hackear' ChatGPT para que se salte las políticas de OpenAI y este es el resultado

TECNOLOGÍA Carolina González Valenzuela | 23 abr. 2023 1:00h.



Noticias · 20/04/2023

Por 7 se multiplica el número de hackers que hablan en la dark web sobre cómo manipular ChatGPT



Redacción Tekios · lectura 1 min · 770 vistas

Pánico con ChatGPT

TECNOLOGÍA

Fake news, manipulación y hackeos: cómo ChatGPT es un "profundo riesgo para la libertad de expresión"

Por Matt Burgess, periodista de seguridad en el equipo de investigación de seguridad de la CIA

MATT BURGESS

SEGURIDAD 14 DE ABRIL DE 2023

ChatGPT: el hackeo apenas comienza

¿Pánico por chatGPT?

Principales preocupaciones sobre la seguridad de los datos



Los incidentes de seguridad de datos están muy extendidos

83%

de las organizaciones experimentan más de una violación de datos a lo largo de su vida

Los usuarios internos malintencionados representan el 20% de las violaciones de datos, lo que aumenta los costos

\$15.4M

Costo promedio total de las actividades para resolver amenazas internas durante un período de 12 meses²

La velocidad y la comodidad del trabajo suelen superar el riesgo percibido

90%

de los empleados que admitieron haber emprendido una serie de acciones inseguras, sabían que sus acciones aumentarían el riesgo para la organización y emprendieron las acciones de todos modos;³

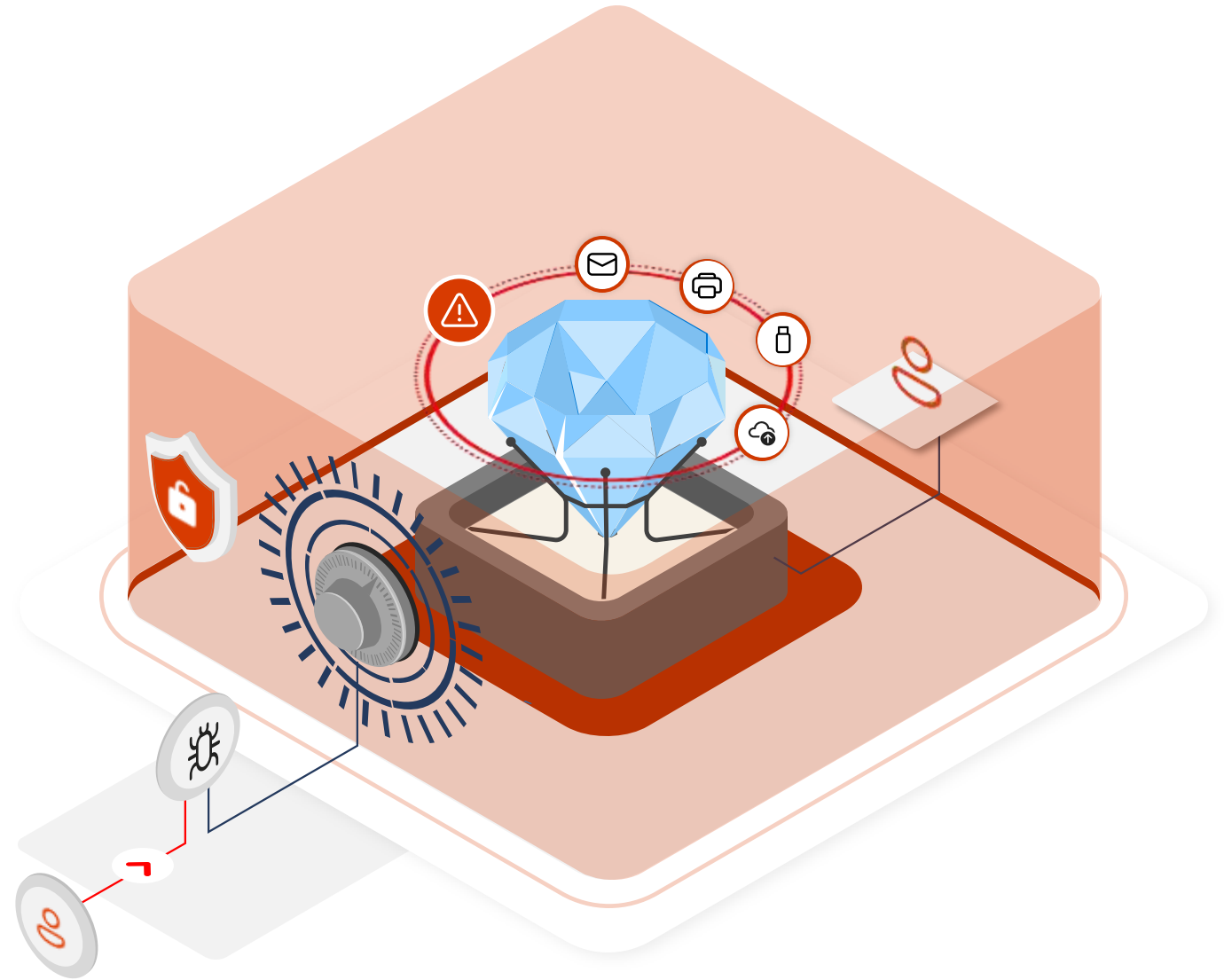
1. Cost of a Data Breach Report 2022, IBM

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

3. Predicts 2023: Cybersecurity Industry Focuses on the Human Deal

Los desafíos más urgentes de la seguridad de los datos

- **Descubrir** datos sensibles, ya sean estructurados o no estructurados, en las instalaciones o en las nubes
- **Configuración segura** para evitar ataques sofisticados
- Detectar cómo están los usuarios **interactuar con los datos** y
Identificación de **riesgos internos**
- Asegúrese de que sus datos permanezcan **seguros** frente a las **actividades de fuga** y exfiltración de **datos**



Una historia real de espionaje corporativo

Una empleada de confianza, Jane Doe, utilizó información confidencial robada para iniciar su propia empresa

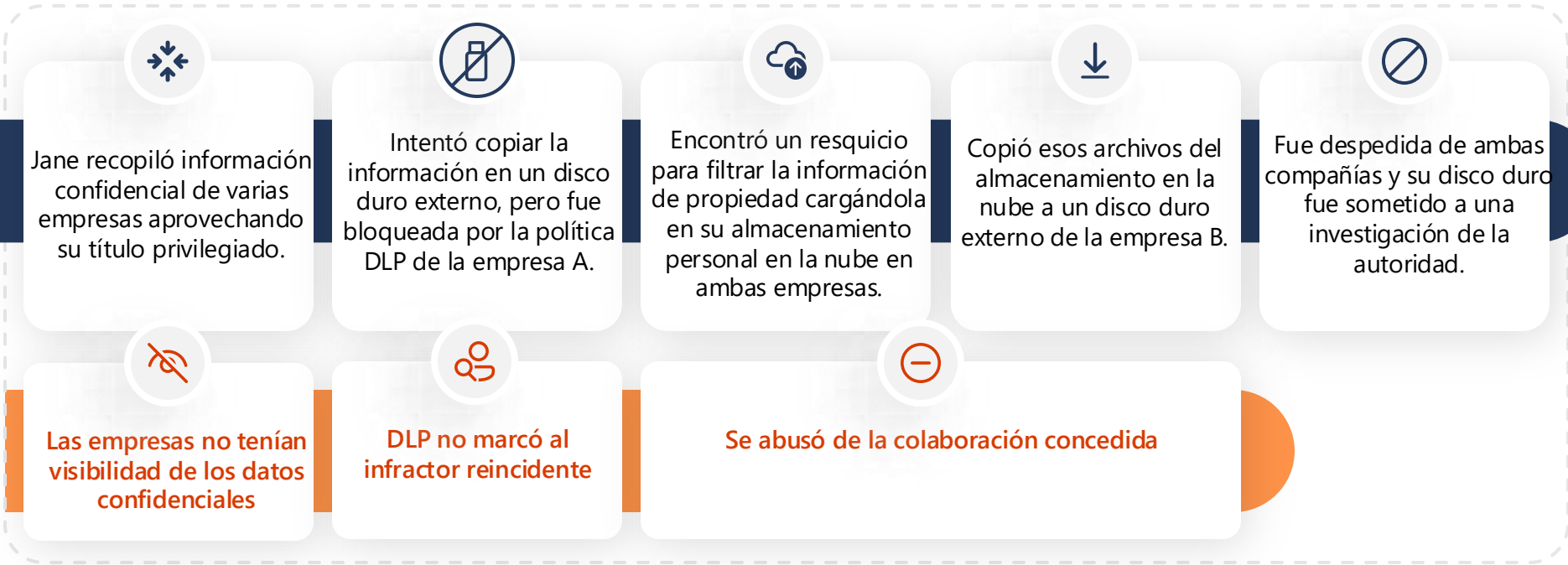
Sospechoso: Jane Doe

 2012-2018 >>

Director/Gerente en dos compañías Fortune 500 durante 5.5 años

 2021

Delincuente condenado



Jane fue condenada y acusada de fraude electrónico, espionaje económico y robo de secretos comerciales por recopilar información de secretos comerciales para solicitar fondos de gobiernos extranjeros e intentar iniciar su propia empresa.

"La propiedad intelectual **costó a las empresas casi \$120 millones** para desarrollarla."



Los incidentes de seguridad de datos pueden ocurrir en cualquier momento y en cualquier lugar



Los datos corren el riesgo de ser utilizados indebidamente si la organización no tiene visibilidad de su patrimonio de datos

1

El usuario es víctima de un ataque de phishing y compromete las credenciales del usuario



Compromiso de datos por amenazas externas



2

El usuario copia el archivo en un USB y, a continuación, lo sube a un Dropbox personal



Robo de datos por parte de personas malintencionadas



3

El usuario comparte datos confidenciales en aplicaciones de IA generativa



Exposición de datos por parte de una persona con información privilegiada



Reflexionemos sobre la seguridad de los Datos



¿Su organización conoce los tipos de información confidencial que tiene y dónde reside?



¿Cómo protege su organización los datos confidenciales en sus entornos?



¿Cómo gestiona su organización los riesgos internos en la actualidad?



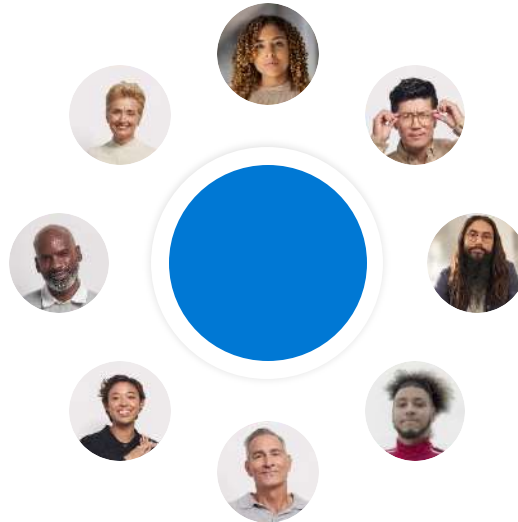
Las organizaciones deben...



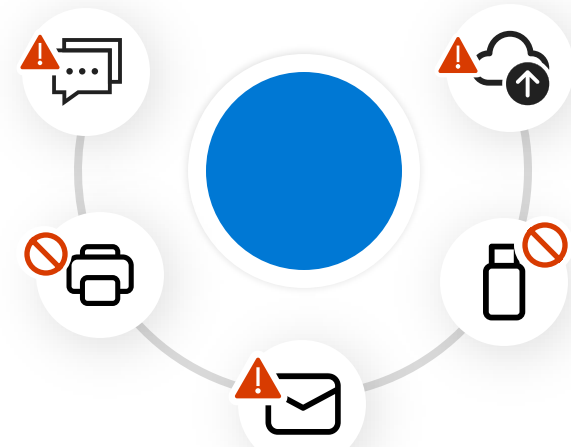
Descubra y proteja los datos confidenciales a lo largo de su ciclo de vida



Comprender la actividad del usuario
contexto en torno a los datos e
identificar los riesgos



Evite el uso no autorizado de
datos en aplicaciones, servicios
y dispositivos



Equilibre la seguridad de los datos y la productividad

Fortalezca la seguridad de los datos con un enfoque integrado



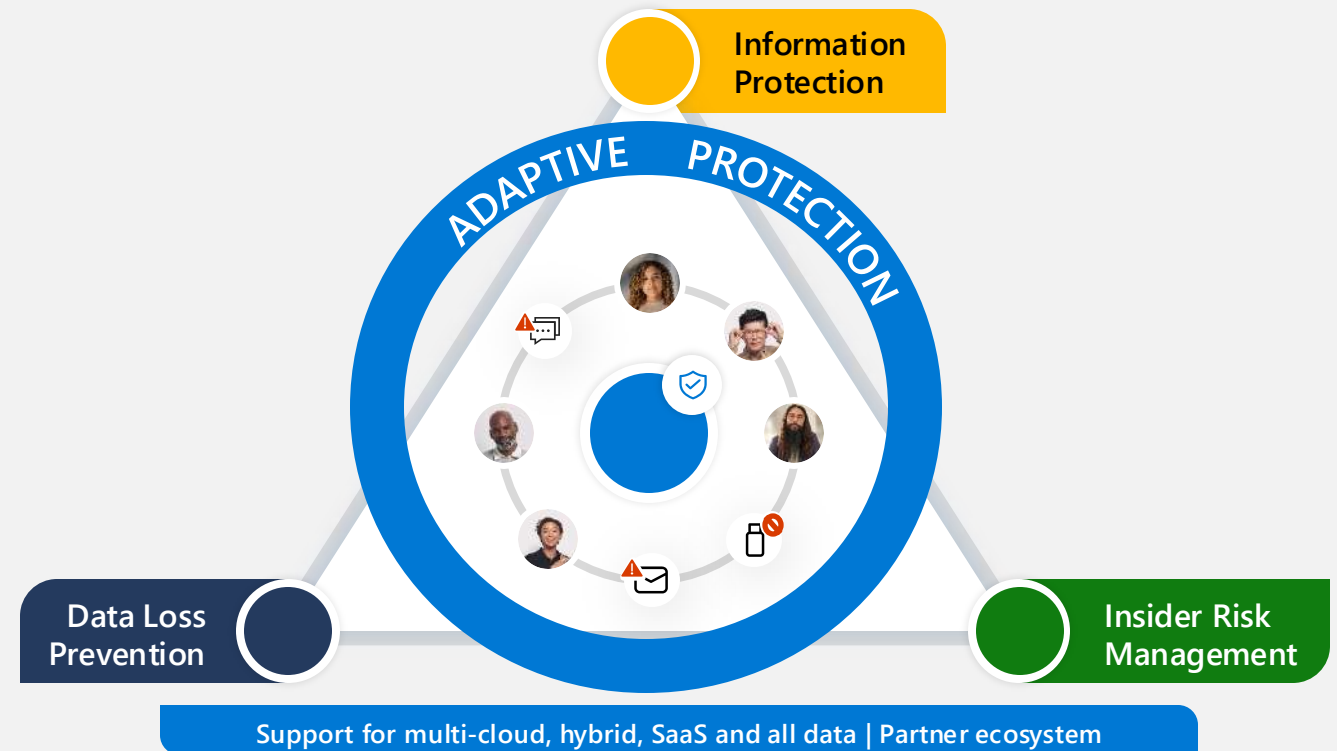
Detecte y clasifique automáticamente los datos y evite su uso no autorizado en aplicaciones, servicios y dispositivos



Comprender la intención y el contexto del usuario en torno a los datos confidenciales para identificar los riesgos más críticos



Habilite la protección adaptativa para asignar políticas DLP apropiadas a los usuarios de alto riesgo



Adaptive Protection en Microsoft Purview

Optimice la seguridad de los datos automáticamente

Detección sensible al context

Identifique los riesgos más críticos con el análisis basado en ML tanto del contenido como de las actividades de los usuarios

Controles dinámicos

Aplique controles efectivos a los usuarios de alto riesgo mientras otros mantienen la productividad

Mitigación automatizada

Minimice el impacto de posibles incidentes de seguridad de datos y reduzca la sobrecarga de administración

Insider Risk Management

Detecte usuarios de riesgo y asigne niveles de riesgo

Data Loss Prevention

Aplique controles preventivos de forma dinámica



Elevated risk



DLP Policy 1

Bloquear



Moderate risk



DLP Policy 2

Bloquear con anulación



Minor risk



DLP Policy 3

Consejos de política

Volvamos a Jane Doe...

Este incidente ilustra las brechas de protección de datos para las que Microsoft Purview fue diseñado



Una persona con información privilegiada utilizó información confidencial robada para iniciar su propia empresa.



Jane Doe



Jane recopiló información confidencial de varias empresas aprovechando su título privilegiado.



Intentó copiar la información en un disco duro externo, pero fue bloqueada por la política DLP de la empresa A.



Encontró un resquicio para filtrar la información de propiedad cargándola en su almacenamiento personal en la nube en ambas empresas.



Copió esos archivos del almacenamiento en la nube a un disco duro externo de la empresa B.



Fue despedida de ambas compañías y su disco duro fue sometido a una investigación de la autoridad.

Microsoft Purview
data security



Use clasificadores entrenables de ML integrados en **Information Protection** para detectar y etiquetar automáticamente la propiedad intelectual. La información propietaria puede protegerse mediante políticas de encriptación y acceso.

Utilice 100+ indicadores listos para usar y modelos de ML en las políticas de fuga/robo de datos de **Insider Risk Management** para detectar a Jane Doe como reincidente y realizar una investigación exhaustiva y tomar medidas.

Use Adaptive Protection para aplicar una directiva de bloqueo de prevención de pérdida de datos en usuarios de alto riesgo. Las acciones de Jane para cargar archivos en un almacenamiento en la nube y copiarlos en un disco duro se pueden bloquear dinámicamente, mientras que otras podrían funcionar como de costumbre.

Aceleró la investigación con información inteligente y capacidades de investigación en **Insider Risk Management**.

¿Por qué elegir Microsoft Purview para la seguridad de los datos?

Simplifica lo complejo con protección de extremo a extremo, lo que le permite ahorrar tiempo y dinero.



Visibilidad completa

Obtenga información sobre el contexto y los datos de los usuarios, tanto estructurados como no estructurados, en Microsoft Azure, AWS, aplicaciones en la nube y aplicaciones de IA generativa con capacidades de seguridad de datos líderes en la industria.



Integración sin problemas

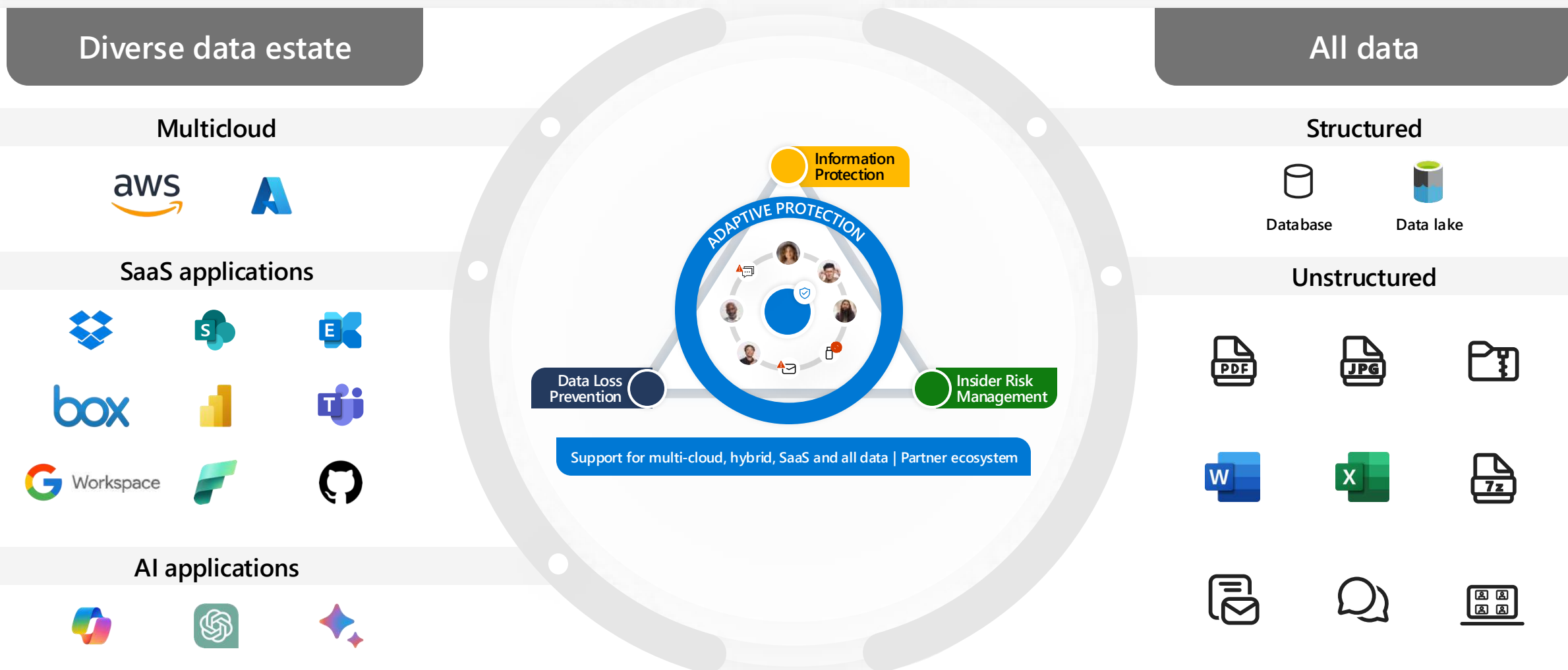
Proteja los datos de extremo a extremo utilizando soluciones creadas en una única plataforma que incluye un mapa de datos unificado, clasificación inteligente de datos, extensos registros de auditoría y un motor de políticas optimizado.



Seguridad impulsada por IA

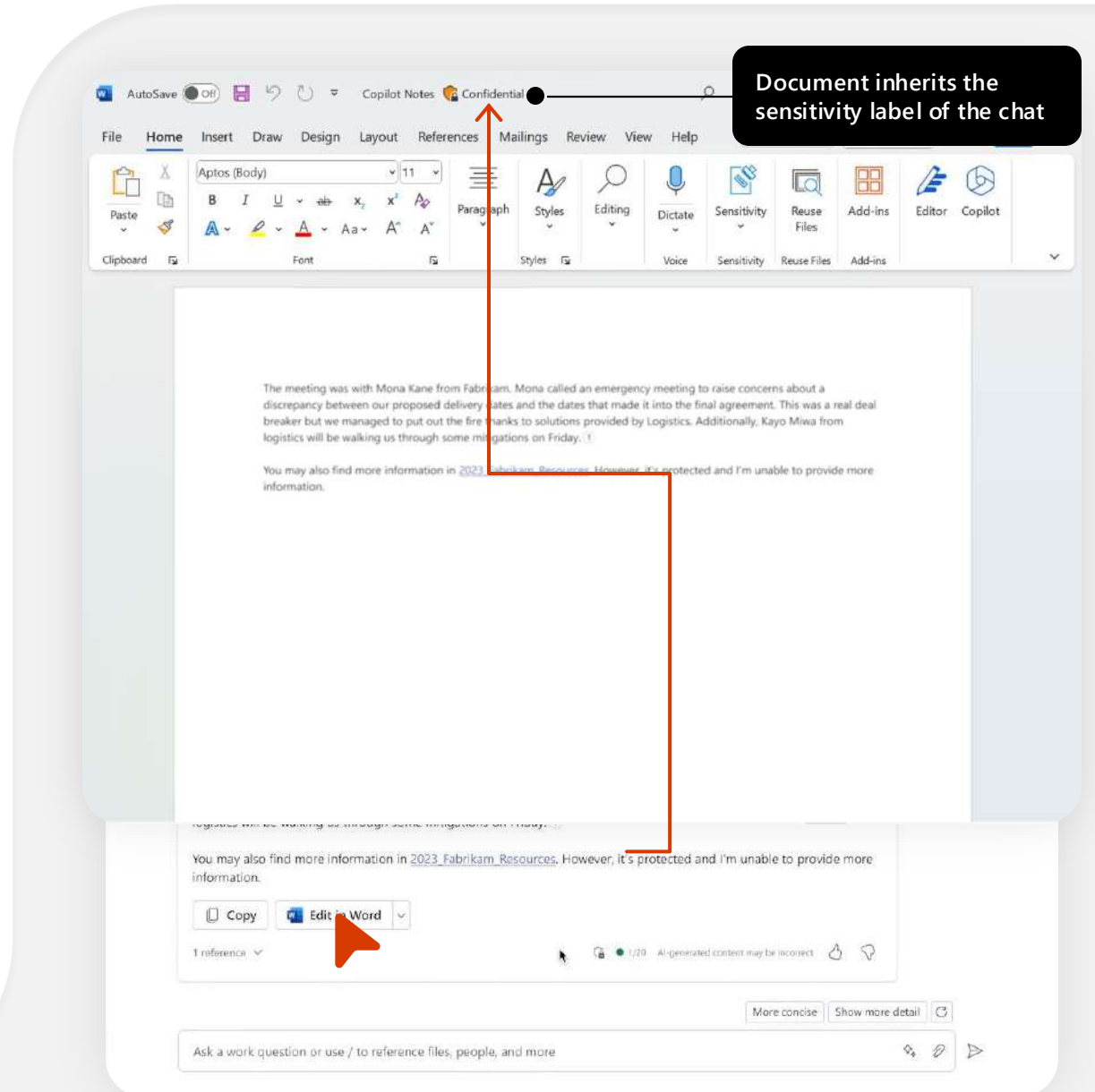
Descubra los riesgos ocultos y adelántese a posibles incidentes de seguridad de datos con Security Copilot, clasificadores de datos impulsados por IA, detección de riesgos y protección adaptable al riesgo.

Seguridad integral: proteja su diverso patrimonio de datos

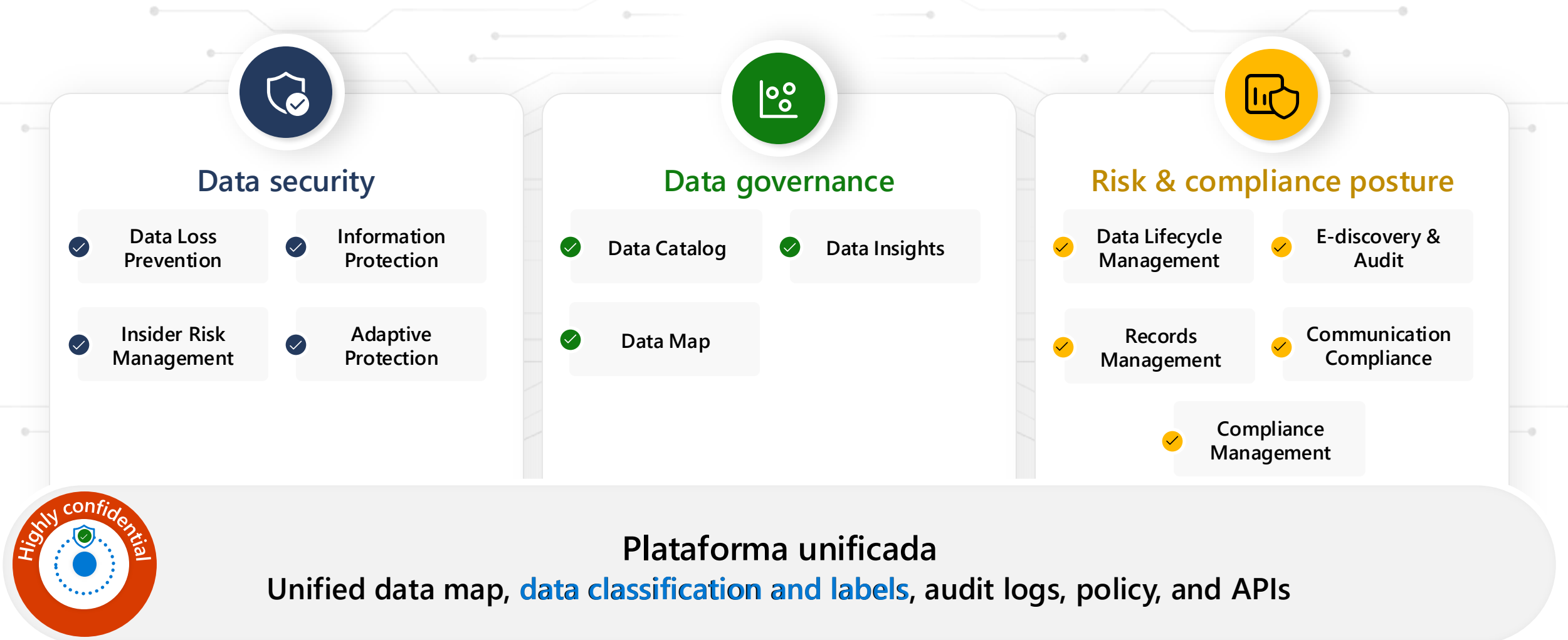


Protección de datos en aplicaciones de IA generativa con Microsoft Purview

- Descubra, clasifique y **etiquete automáticamente sus datos confidenciales** para facilitar el uso seguro de las aplicaciones de IA.
- Proteja los datos confidenciales generados por Copilot para Microsoft 365 **con directivas de etiquetas persistentes, que van desde archivos hasta mensajes individuales.**
- Evite la **divulgación no autorizada de datos etiquetados en aplicaciones de IA** de forma dinámica en función del nivel de riesgo del usuario.



Integración perfecta: una plataforma unificada para **proteger, gobernar y gestionar de forma coherente el cumplimiento de los datos** de extremo a extremo



Seguridad impulsada por IA

Security Copilot: Llegue a lo crítico a la velocidad de la máquina

Security Copilot

Alert summary

October 1st, 2023, 2:41 PM

The alert with Id:7bbc3040 is a high severity Insider Risk Management alert involving user Jane Doe

(jdoe@ediscosdf.onmicrosoft.com) that was detected on September 28, 2023. The policy "Data loss prevention" was triggered when the user imported a file containing sensitive information into a remote desktop session. This alert is getting generated. The user is considered high risk and has 3 alerts and 1 case associated with them. This alert is in a confirmed state and is being investigated by Bob Dylan. The alert also has a case: "DepartingUser_Investigation" associated with it.

AI generated. Verify for accuracy.

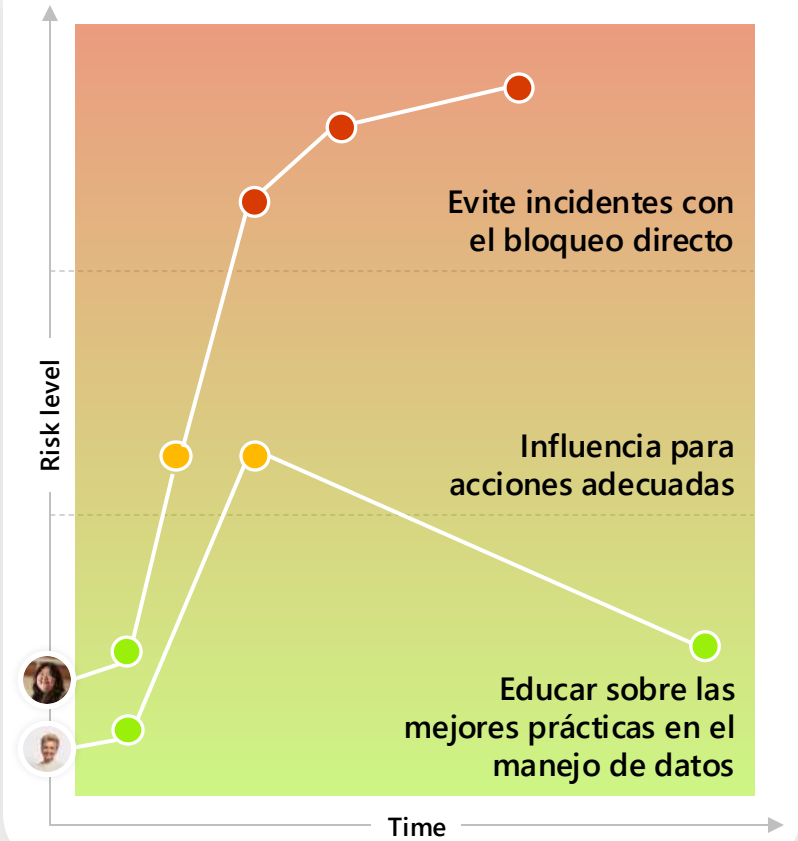
Clasificadores impulsados por IA: descubre las joyas de la corona

INTELLECTUAL PROPERTY

SOURCE CODE

FINANCIAL STATEMENTS

Seguridad de datos: responda a los riesgos de forma dinámica

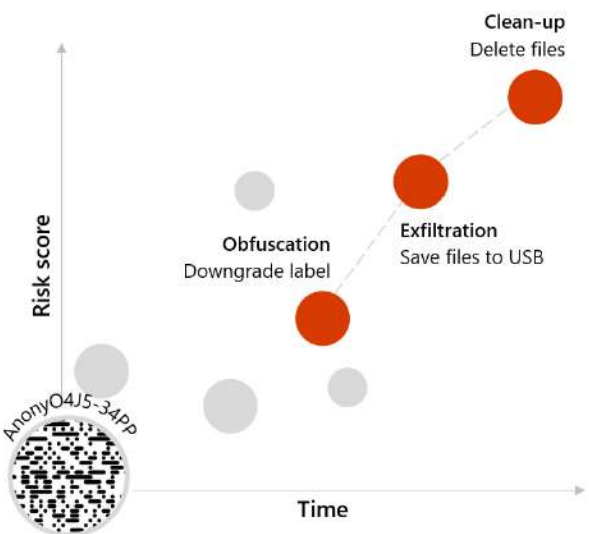


Veamos un escenario ...



Adelántese a los riesgos de seguridad de sus datos para la exfiltración

Con el tiempo, el usuario se involucra en actividades que ponen en riesgo los datos



Identifique la intención del usuario a través de la detección de secuencias

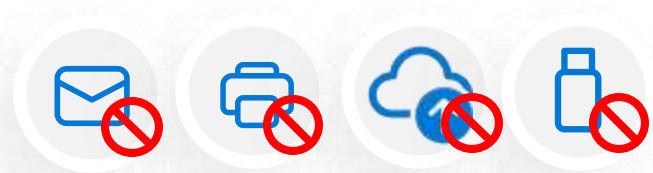
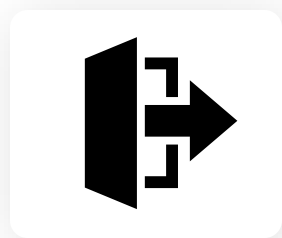
Como resultado, al usuario se le asigna una puntuación de riesgo de Riesgo elevado

-  **Elevated risk**  **Block**
-  **Moderate risk**  **Block w/ override**
-  **Minor risk**  **Policy tip**



La directiva DLP se implementa dinámicamente para evitar el robo de datos

El usuario presenta su renuncia, Ir a un competidor de primer nivel



Proteger los datos para que no se lleven a la competencia



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

Microsoft Purview

https://purview.microsoft.com

Contoso | Microsoft Purview

Search

Try the new Microsoft Purview

Security Copilot

Home

Insider Risk Management

Overview

Alerts

Cases

Policies

Users

Notice templates

Adaptive protection (preview)

Solutions

Related

Communication compliance

Data Loss Prevention

Information barriers

(7bbc3040) Data theft by departing users

AssignNeeds reviewSummarizeDismiss alertConfirm alert

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

Activity that generated this alert

Reduce alerts for this activity

Data infiltration: Files downloaded from unallowed site

87/100 High severity | Sept 28, 2023 (UTC)

12 events: Files downloaded from 1 unallowed site

8 events: Files that have labels applied, including: Project Alpha

Factors that impacted risk score

Includes unallowed domains (1 event)

View all activity

Triggering event

Sept 28, 2023 (UTC)

An HR connector imported a resignation date for this user.

User details

jdoo@ediscodf.onmicrosoft.com

View all details

User alert history

Last 30 days

Data theft for departing employees3 alerts

Sensitive data leaks1 alert

Security violations2 alerts

Summary

Activity explorer

User activity

Forensic evidence

Risk factors

Top exfiltration activities

1.9K exfiltration activities

Files uploaded to cloud storage1,181

Files copied to USB342

Files shared externally181

View all exfiltration activities

Cumulative exfiltration activities

High severity cumulative exfiltration activities detected from 9/24-9/28

File downloads from SharePoint Online

More events than 99% of other users

User5,240

Org average838

Files copied to USB

More events than 95% of other users

User1,272

Org average324

Documents printed

More than 92% of other users

User342

Org average120

View all cumulative exfiltration activities

Sequences of activity

No sequences detected

Unusual activity for this user

3 patterns of unusual

Priority content

No priority content detected

Unallowed domains

4 unallowed domains

Security Copilot resume las alertas de riesgo interno, mostrando varios factores de las actividades de los usuarios

Microsoft Purview

Search

Alert history

Full user history

2 events: Files downloaded from 1 unallowed site

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

Factors that impacted risk score:

- Includes unallowed domains (1 event)

View all activity

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

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

Sort by: Date occurred

(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

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: Project Obsidian

Obfuscation: Files renamed

Nov 22, 2022 (UTC) | Risk score: 32/100

19 events: Files renamed

2 events: Files containing sensitive info, including: Project Obsidian

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

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

User activity scatter plot 6 Months 3 Months 1 Month

Risk score

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

Jan 22, 2023 - Mar 14, 2023 (UTC) | Risk score: 90/100

50 events: Sequence: Files downloaded from unallowed domain, archived, 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 or received with 1 unallowed domain

Deletion: Files deleted

Apr 13, 2023 (UTC) | Risk score: 75/100

2 events: Files deleted from Windows 10 Machine

Exfiltration: Files printed

Apr 11, 2023 (UTC) | Risk score: 45/100 | View forensic evidence

2 events: Files printed

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

Obfuscation: Labels of sensitive files downgraded on SharePoint

Apr 9, 2023 (UTC) | Risk score: 35/100

30 events: Labels of SharePoint files downgraded

12 events: Files containing sensitive info, including: Credit Cards, SensitiveInfoType2

11 events: Files that have labels applied, including: Project Falcon

Infiltration: Files downloaded from unallowed site

Apr 1, 2023 (UTC) | Risk score: 87/100

20 events: Files downloaded from 1 unallowed site

2 events: Files that have labels applied, including: Project Alpha

15 events: Files with priority file extensions, including: xml, txt, docx, ppt, 7z

Comprenda la intención del usuario con la detección de secuencias, que identifica y conecta automáticamente una serie de actividades relacionadas

Insider risk management

 Recommended actions

 What's new ?

 Insider risk settings

 Insider risk audit log

 Learn about insider risk management

Overview

Alerts

Cases

Policies

Users

Forensic evidence (preview)

Notice templates

Adaptive protection (preview)

Dashboard

Risk levels for Adaptive Protection

Users assigned risk levels

DLP policies

Adaptive Protection settings

Risk levels for Adaptive Protection

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

Insider risk policy

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

Adaptive Protection policy for Insider Ris... ▾

Define conditions for risk levels

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



Elevated risk level

Custom elevated risk level ▾

Edit



Moderate risk level

Custom moderate risk level ▾

Edit



Minor risk level

Custom minor risk level ▾

Edit

Past activity detection

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

7 days of previous activity ▾

Risk level timeframe

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

30 days ▾

Configurar Adaptive Protection para configurar los niveles de riesgo en función de las prioridades de riesgo de su organización

Insider risk management

Recommended actions

What's new ?

Insider risk settings

Insider risk audit log

Learn about insider risk management

- Overview
- Alerts
- Cases
- Policies
- Users
- Forensic evidence (preview)
- Notice templates
- Adaptive protection (preview)

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

Users assigned risk levels

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

Refresh

3 items

Filter

Reset

Filters

Risk level: Any

☐ Users	Risk level	Assigned to user	Risk level resets	Active alerts	Cases confirmed as violation	Case
☐ #Anonymized#EAAAAGHcWoMDaFMT3oOkRFY1I6v47pUH6um...	Elevated	25 days ago	in a month	1	0	asgfagagadgdsg
☐ #Anonymized#EAAAAG+ft2YHjvJbXwTzWKfJ2US7+wkgkvRO...	Elevated	21 days ago	in a month	1	0	Case Test
☐ #Anonymized#EAAAAG+aft2YHjvJbXwTzWKfJ2US7+wkgkvRO...	Minor	7 days ago	in a month	1	0	

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

Edit rule

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

AND

Sender domain is

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

competitor.com

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

+ Add

+ Add condition Add group

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

- ☒ Block everyone.
- ☐ Block only people outside your organization.

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

Edit rule

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

AND

Sender domain is

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

competitor.com

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

+ Add

AND

User's risk level for Adaptive Protection is

Risk levels for Adaptive Protection are defined in insider risk management. They determine how risky a user's activity is and can be based on conditions such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. If insider risk management detects that a user matched the risk level condition, the DLP policy will enforce any actions you configure below. [Learn more about risk levels for Adaptive Protection](#)

Select one or more risk levels

☐ Elevated risk level

☐ Moderate risk level

☒ Minor risk level

Use actions to protect content when the conditions are met.

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

Edit rule

ⓘ + Add

AND

^ User's risk level for Adaptive Protection is

Risk levels for Adaptive Protection are defined in insider risk management. They determine how risky a user's activity is and can be based on conditions such as how many exfiltration activities they performed or whether their activity generated a high severity insider risk alert. If insider risk management detects that a user matched the risk level condition, the DLP policy will enforce any actions you configure below. [Learn more about risk levels for Adaptive Protection](#)

Elevated risk level

+ Add condition

⌵ Add group

^ Actions

Use actions to protect content when the conditions are met.

^ Restrict access or encrypt the content in Microsoft 365 locations

✓ Restrict access or encrypt the content in Microsoft 365 locations

☒ Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

☒ Block everyone. ⓘ

☐ Block only people outside your organization. ⓘ

+ Add an action

^ User notifications

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

☐ Off

Ajustar las acciones de los usuarios, como impedir que los usuarios realicen acciones específicas

✓ **Alert: Confidentiality obligation during departure**

- Needs review

Confirm alert to an existing case

Dismiss alert

All risk factors Activity explorer User activity

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

Sort by: Date occurred 

User activity scatter plot 6 Months 3 Months 1 Month

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

> (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
- 1 event: File 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

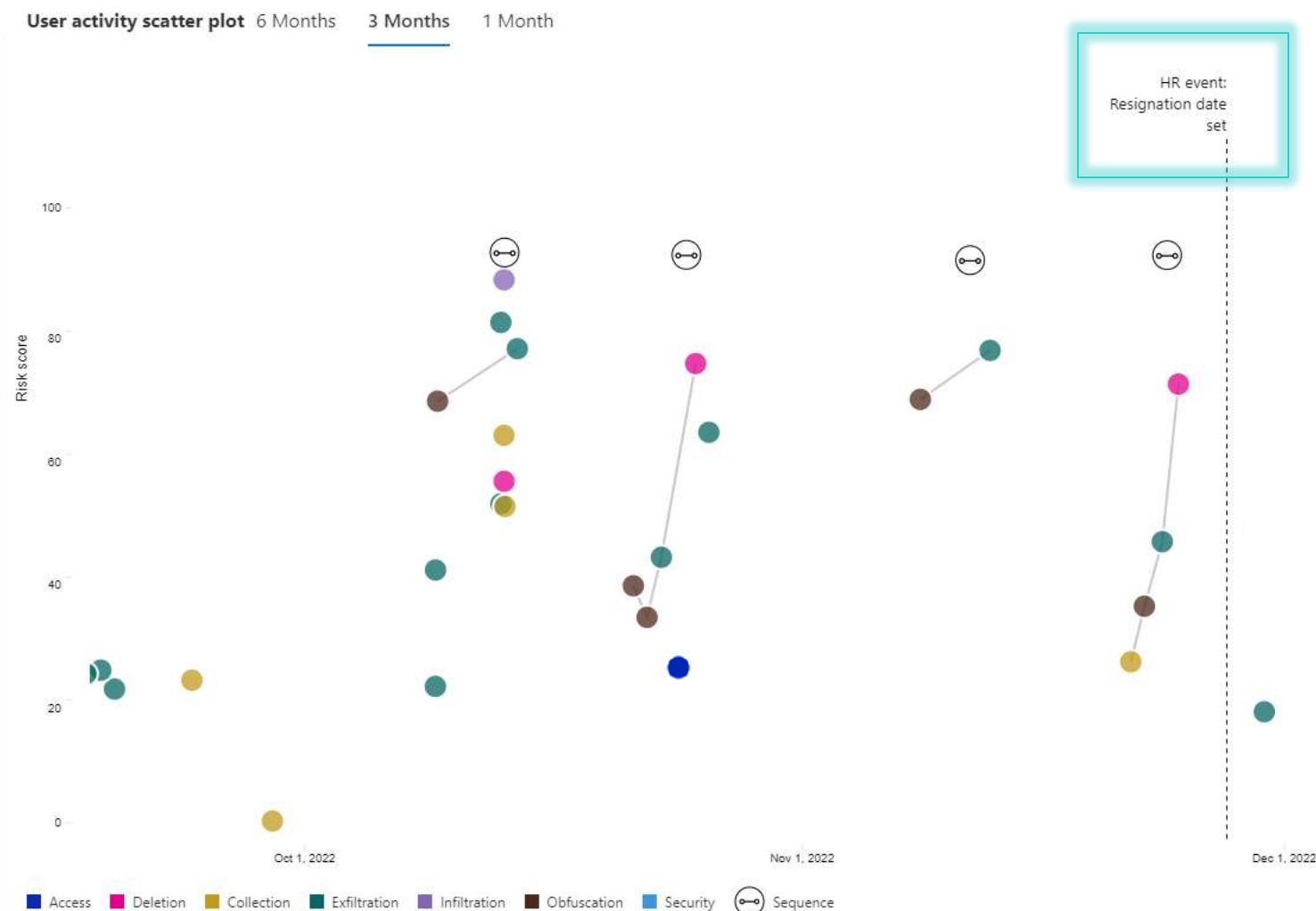
- 19 events: Files renamed
- 2 events: Files containing sensitive info, including: Credit Cards
- 12 events: Files with priority file extensions, including: pdf, ppt, docx, txt
- 12 events: Files with priority file extensions modified, including: docx, txt, pdf

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

- Exfiltration: Files copied to USB device

Nov 12, 2022 (UTC) | Risk score: 75/100
197 events: Files copied to USB devices



Comience con la seguridad integral de los datos

Paso 1

Información en un solo paso e implementación sin agentes



Descubre tus datos confidenciales



Visite la **clasificación de datos** y aproveche los tipos de información confidencial (SIT) integrados y personalizados, los clasificadores que se pueden entrenar y el contenido etiquetado.



Comprender los riesgos internos críticos



Active el **análisis de riesgos internos** y cree una directiva de fuga de datos recomendada.



Recibe Alertas de fidelidad



Cree directivas DLP y **active la protección adaptable** en modo de prueba o auditoría.

Intégrese sin problemas en una plataforma unificada y sin dependencias

Información procesable sin impacto en los usuarios finales

Comience con la seguridad integral de los datos

Paso 2

Avanza como un profesional con inteligencia integrada



Etiquete y proteja los datos

Defina la **taxonomía y el contenido de las etiquetas** habilitando las etiquetas predeterminadas, configurando el etiquetado manual o escalando con el etiquetado automático.



Investigue los riesgos críticos

Revise e **investigue las alertas de riesgo interno de alta gravedad** y ajuste las directivas.



Evite la pérdida de datos confidenciales

Ajuste las directivas DLP y **active la directiva DLP adaptable en el modo de bloqueo** o bloqueo con invalidación.

FAQ'S





¡Gracias!

ευχαριστώ Salamat Po متشكراً شكراً Grazie

благодаря ありがとうございます Kiitos Teşekkürler 谢谢

ໝາຍຄຸນຄວັ້ນ Obrigado شكریه Terima Kasih Dziękuję

Hvala Köszönöm Tak Dank u Wel ДЯКУЮ Tack

Mulțumesc спасибо Danke Cám ơn Gracias

多謝晒 Ďakujem תודה நன்றி Dėkuji 감사합니다