



#GlobalAzure

#GABMUGPeru

#GABMUGPeru

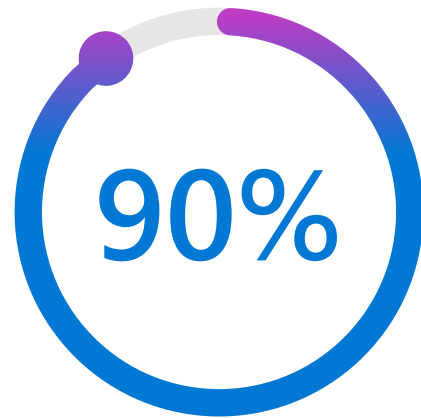
Despliegue en Azure: Static Web Apps

Valentina Milagros Chambilla Perca



#GlobalAzure

Data has moved beyond the traditional borders of business



Las organizaciones están adoptando múltiples infraestructuras, plataformas y servicios en la nube para administrar sus negocios

Source: Microsoft Data Security Index report

La necesidad de
proteger y gobernar
los datos en la IA
nunca ha sido mayor



“Menos de la mitad (47%) de los CIO y líderes tecnológicos dicen que confían en que su organización podrá mitigar los riesgos de la IA.”

– Gartner, We Shape AI, AI Shapes Us: 2023 ITSymposium/Xpo™ Keynote Insights, Mary Mesaglio, Don Scheibenreif, Hung LeHong, et al., October 2023

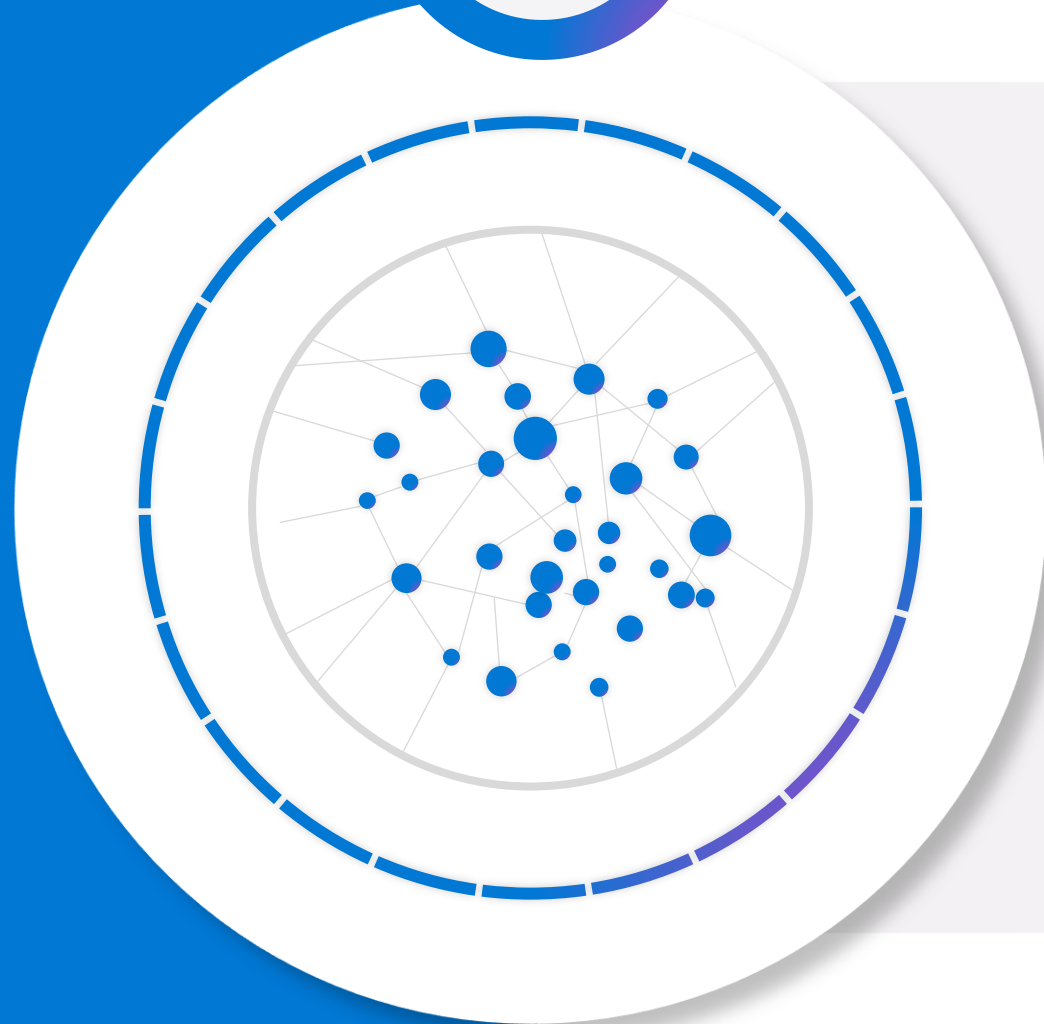
Las regulaciones siguen evolucionando



“Para 2027, al menos una empresa global verá su implementación de IA prohibida por un regulador por incumplimiento de la legislación de protección de datos o gobernanza de IA.”

– Gartner, Security Leader’s Guide to Data Security,
Andrew Bales, Sep 2023

Proteger y gobernar los datos y la IA es complejo y multifacético



Datos en todas partes y en crecimiento



La necesidad de proteger y gobernar la IA nunca ha sido mayor



Las regulaciones siguen evolucionando

Es un reto
para trabajar con
soluciones
dispare



10+

Las organizaciones utilizan
un promedio de 10
soluciones para proteger
su patrimonio de datos



Brechas de infraestructura
expuestas que son costosas
y complejas de administrar



Las soluciones fragmentadas conducen a

Copias duplicadas de datos

Transferencias de datos innecesarias

Clasificación de datos incoherente

Alertas redundantes

Investigaciones aisladas

Brechas de exposición



Aumento de la complejidad

Tiempos de implementación más largos

Mayor carga de gestión

Costos más altos

Peores resultados de seguridad

Microsoft Purview

Un enfoque más sencillo

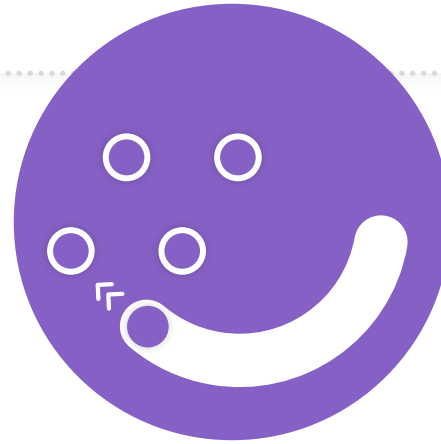
Microsoft Purview

Soluciones integradas para proteger y controlar todo su patrimonio de datos



Seguridad integral de los datos

Proteja los datos a lo largo de su ciclo de vida, dondequiera que se encuentren



Gobernanza de datos moderna

Gobierne los datos sin problemas para empoderar a su organización



Postura de riesgo y cumplimiento

Gestione los riesgos críticos y los requisitos normativos

Datos estructurados y no estructurados

Datos tradicionales y generados por IA

Microsoft 365 y multinube

Capacidades de plataforma compartida

Microsoft Purview

Soluciones integradas para proteger y controlar todo su patrimonio de datos

DATA SECURITY

Proteja los datos a lo largo de su ciclo de vida, dondequiera que se encuentren

Prevención de pérdida de datos
Gestión de riesgos internos
Protección de la información
Protección adaptativa

DATA GOVERNANCE

Gobierne los datos sin problemas para empoderar a su organización

Mapa de datos
Catálogo de datos
Insight sobre el patrimonio de datos

RISK & COMPLIANCE POSTURE

Gestione los riesgos críticos y los requisitos normativos

Administrador de cumplimiento
eDiscovery y auditoría
Cumplimiento de la comunicación
Gestión del ciclo de vida de los datos
Gestión de registros

Datos estructurados y no estructurados

Datos tradicionales y generados por IA

Microsoft 365 y multinube

Capacidades de plataforma compartida

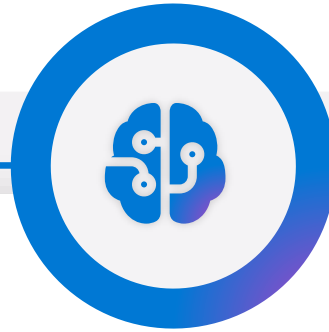
Data Map, Data Classification, Data Labels, Audit, Data Connectors

Innovaciones de Microsoft Purview

Proteger y gobernar los datos en la era de la IA



**Proteja y controle
todo su
patrimonio de
datos**



**Amplíe la
seguridad de los
datos y el
cumplimiento
normativo a la IA**



**Seguridad
impulsada por IA
con Microsoft
Security Copilot**

Innovaciones de Microsoft Purview

Proteger y gobernar los datos en la era de la IA



**Proteja y controle
todo su
patrimonio de
datos**



Extend data
security and
compliance
to AI



AI-powered
security with
Microsoft
Security Copilot

Es un reto proteger el patrimonio de datos



Múltiples soluciones

+10 soluciones utilizadas para asegurar el patrimonio



Protecciones inconsistentes

para tipos de datos estructurados y no estructurados



Puntos ciegos

de los usuarios a través de un patrimonio de datos más complejo



Plataforma unificada

en todo su patrimonio de datos con escaneo de datos integrado. Etiquetado y clasificación



Etiquetado y protecciones

para tipos de datos estructurados como Azure SQL, Azure Data Lake Storage y Amazon S3



Detecciones ampliadas

en la gestión de riesgos internos en nubes de infraestructura como AWS y aplicaciones como Google Drive y Box.

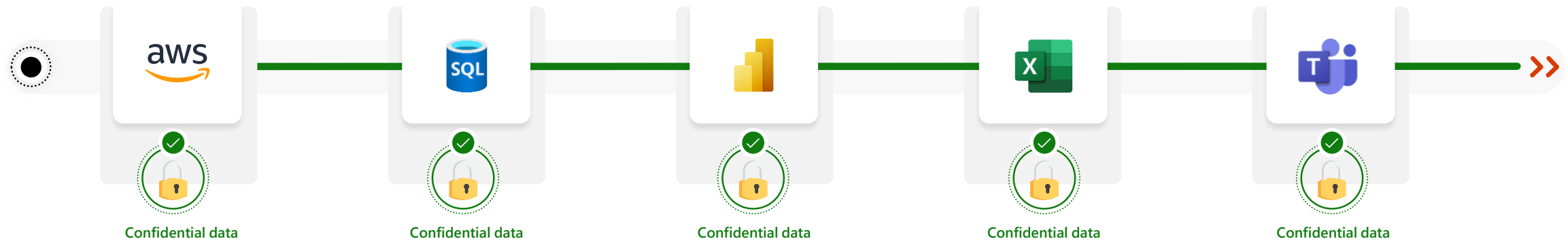
**Anuncio de nuevas
funciones para
proteger el
patrimonio de
datos**



Cerrar la brecha entre datos estructurados y no estructurados



Cerrar la brecha entre datos estructurados y no estructurados



#GABMUGPeru

Protecting structured and unstructured data demo



#GlobalAzure

Proteja todo su patrimonio de datos con Microsoft Purview

Visibilidad completa

PUBLIC PREVIEW

Portal unificado para
Comprenda, etiquete y
clasifique datos
confidenciales desde un
plano de control común

Protecciones ampliadas

PRIVATE PREVIEW

Etiquetado y clasificación
across SQL, Azure Data Lake
Storage y Amazon S3

Marco normativo unificado
para aplicación de políticas de
protección en SQL, Azure Data
Lake Storage y Amazon S3

Detecciones de riesgos

PRIVATE PREVIEW

Expanded Señales de gestión
de riesgos internos en AWS,
Box, DropBox, Goodle Drive y
GitHub

Innovaciones de Microsoft Purview

Proteger y gobernar los datos en la era de la IA



Secure and
govern your
entire data
estate

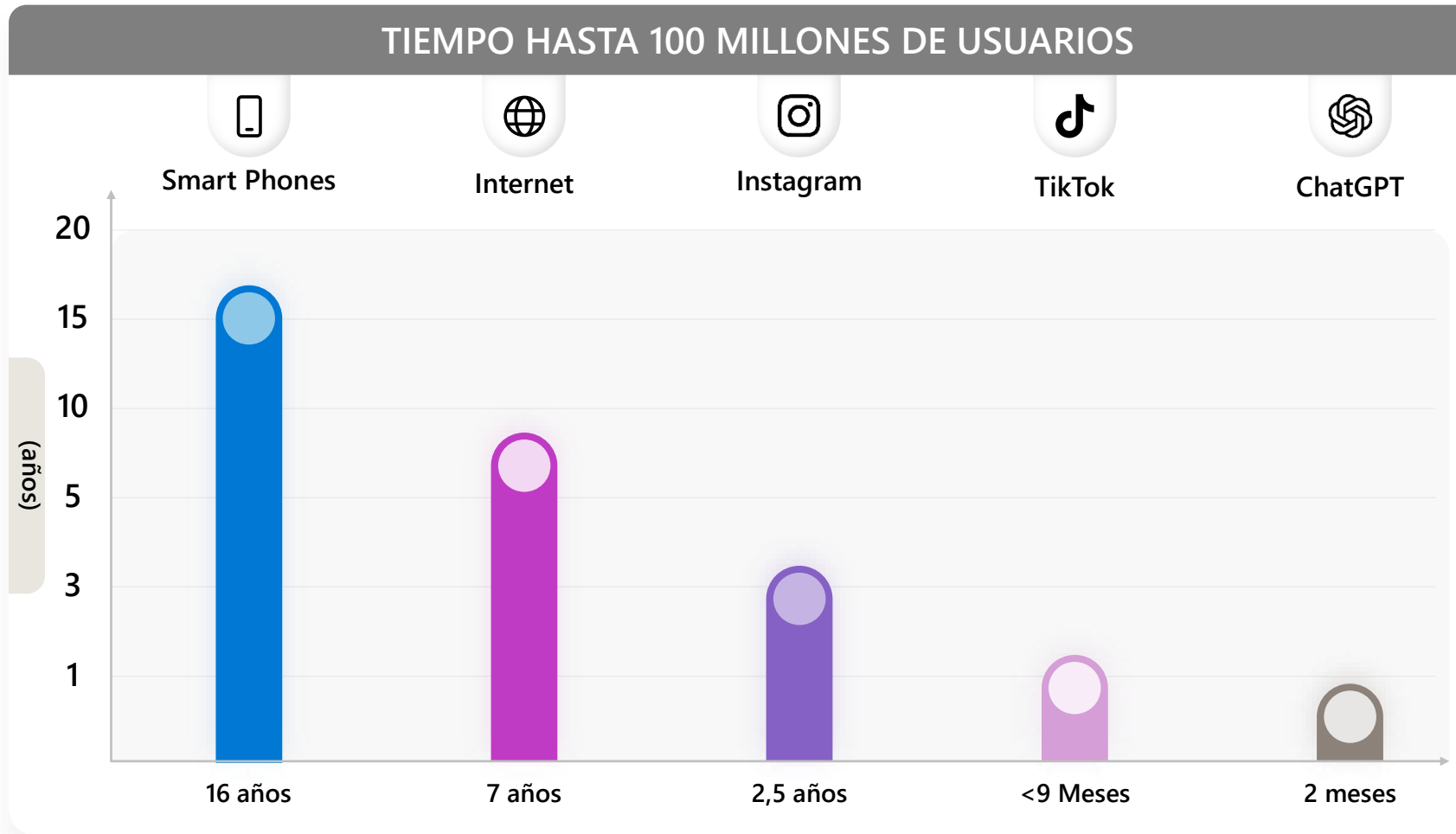


Amplíe la
seguridad de los
datos y el
cumplimiento
normativo a la IA



AI-powered
security with
Microsoft
Security Copilot

¡La tecnología de IA generativa ya está aquí!



Y puede ayudar...



Da rienda suelta a la creatividad



Desbloquear la productividad



Habilidades de nivel superior

Veamos un ejemplo



Contoso usa la IA generativa para predecir reacciones dañinas y no deseadas a los medicamentos. Sin programas de seguridad y gobernanza de datos, Contoso podría estar expuesto a riesgos:



Sobreexposición de datos

Los datos utilizados por la IA podrían ser confidenciales, incluidas la PII y la PHI, y podrían violar los derechos de privacidad del paciente



Pérdida de confianza de los clientes



Pérdida de datos

Los datos producidos por la IA pueden ser vulnerables al acceso no autorizado o a la divulgación por parte de actores malintencionados



Disminución de la ventaja competitiva



Incumplimiento de datos

Es posible que los datos utilizados y producidos por la IA no cumplan con las regulaciones pertinentes y los principios éticos de la IA



Fuertes penalidades o multas

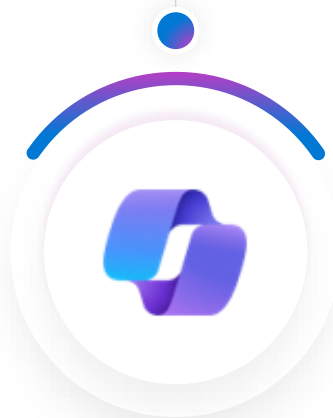
Microsoft Purview

Soluciones integrales para proteger y gobernar los datos en IA

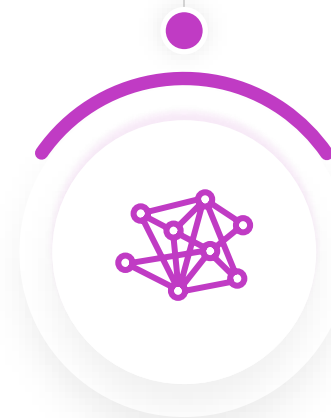
En todas las aplicaciones de IA



IA creada por la empresa



Microsoft Copilot



Non-Microsoft AI

Datos seguros en la era de la IA con Microsoft Purview

Visibilidad completa

Obtenga información procesable sobre la actividad de la IA generativa

Extenso protección

Evite la pérdida de datos en los avisos de IA y proteja los datos en las respuestas de IA

Conformidad mandos

Cumpla fácilmente con los requisitos empresariales, normativos y de cumplimiento

#GABMUGPeru

Demo: Securing AI with Microsoft Purview



#GlobalAzure

Innovaciones de Microsoft Purview

Proteger y gobernar los datos en la era de la IA



Secure and
govern your
entire data
estate



Extend data
security and
compliance
to AI



**Seguridad
impulsada por IA
con Microsoft
Security Copilot**

Habilidades de Purview impulsadas por IA para múltiples personas



Herramientas de solución fragmentadas

Los clientes que emplean más herramientas de seguridad (16+) experimentan 2,8 veces más incidentes de seguridad de datos.



SOC admin



Alto volumen de alertas complejas

Los administradores de seguridad de datos reciben 50+ alertas por día y solo pueden llegar a ~60-70% de ellas como máximo.



Data security admin



Revisión prolongada, que requiere experiencia

El 60 % del tiempo de administración de exhibición de documentos electrónicos se dedica a revisar las pruebas recopiladas en los conjuntos de revisión.



Compliance admin

Se ofrecen dos tipos de experiencias

STANDALONE

Tell me more about the user involved in this alert?

> 3 steps completed 1 min

12:34 PM

The user in this DLP alert is a Sales Manager and is considered high risk because of following reasons:

1. They are considered a potential high impact user as they accessed more content containing sensitive information than other users and have a GlobalAdmin role assigned in Azure AD.
2. The user is also identified as a departing user with resignation date confirmed as October 18th, 2023.
3. The user is also involved in sequential events that occurred from Sept. 9 to Sept.12, 2023. The sequence contained 50 events that included sensitive files being downloaded from SharePoint, renamed, printed and subsequently deleted. There were 5 events of this sequence that involved files with Project Obsidian label. There were 2 events that involved files containing credit card info. The user was involved in 39 events of print file activity which was more events than 80% of users with the same job title. There were 3 print events which involved documents containing SSN information.

The user also has 2 active alerts and 1 open case in Insider Risk Management. The activities indicate potential data security concerns that merit further investigation or mitigation measures.

📄 ⬇️ 😊 How's this response?

EMBEDDED

Contoso | Microsoft Purview

(7bbc3040) Data theft by departing users

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

Assign Needs review Summarize Dismiss alert Confirm alert

Activity that generated this alert
Data exfiltration: Files downloaded from unallowed site
10/100 High severity 1 Sept 28, 2023 6/10
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)

Triggering event
Sept 28, 10:15 AM
An HR connector imported a resignation date for this user.

User details
jdoe@contoso.com
View all details

User alert history
See where
Data theft for departing employees 3 alerts
Sensitive data leaks 1 alert
Security violations 2 alerts

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

Risk factors

Top exfiltration activities
▲ 1.9K exfiltration activities
Files uploaded to cloud storage 1,181
Files copied to USB 342
Files shared externally 181

Cumulative exfiltration activities
▲ High severity cumulative exfiltration activities detected from 9/24-9/28
File downloads from SharePoint Online: More events than 95% of other users. User: 5,240
Files copied to USB: More events than 95% of other users. User: 1,272
Documents printed: More than 92% of other users. User: 342

Sequences of activity
No sequences detected

Unusual activity for this user
▲ 3 patterns of unusual activities

Priority content
No priority content detected

Unallowed domains
▲ 4 unallowed domains

#GABMUGPeru

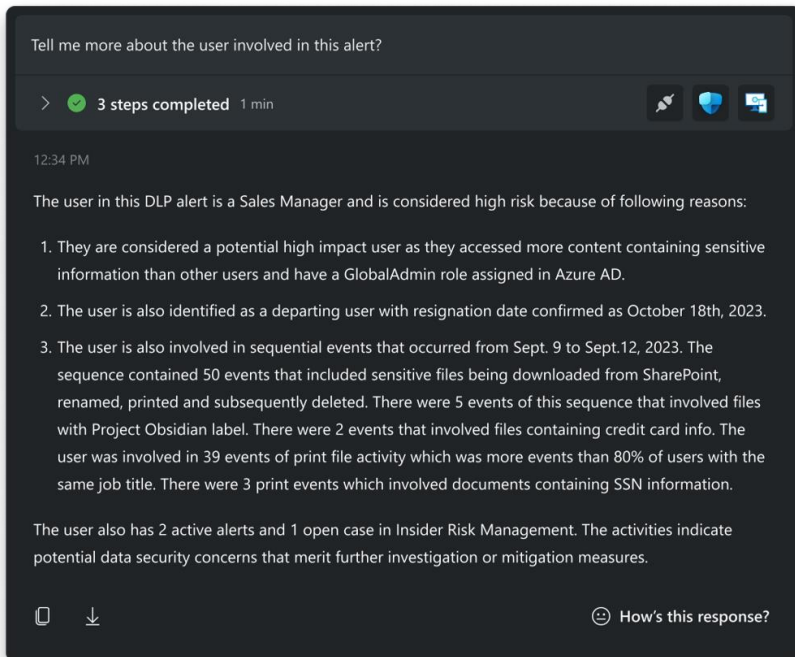
Demo: Purview capabilities in Security Copilot



#GlobalAzure

¡Pero eso no es todo!

STANDALONE



PROMPTS

- Which Purview Data Loss Prevention alerts should I prioritize today?
- Can you summarize the first purview alert?
- What was the data or action that triggered this alert?
- Who is the user involved in this alert
- What is the risk level of this user?
- What information does Purview have about the risk associated with this user?
- Show me all the activities for this user in the last 7 days.
- What type of unusual activities did the user engage in the last 7 days?
- What type of exfiltration activities did the user engage in the last 5 days?
- What type of sequential activities did the user engage in the last 10 days?
- What are the data risks related to this alert?
- For the files related to the alert, show me all activities done in last 7 days
- Can you get me the status of labeling on these files?
- What Suspicious Actions Have Been Performed On This Files?
- List all active Purview Policies covering the sensitive data in the file
- List all active purview policies applied to this user
- What other DLP alerts are present for this user?
- According to Purview, What is the implication of these DLP Alerts
- How many DLP policies have adaptive protection configured?

y más...

#GABMUGPeru

Demo: Security Copilot in Microsoft Purview



#GlobalAzure

Private Preview

STANDALONE

- Which Purview Data Loss Prevention alerts should I prioritize today?
- Can you summarize the first purview alert?
- What was the data or action that triggered this alert?
- Who is the user involved in this alert
- What is the risk level of this user?
- What is the Purview risk associated with this user?
- Show me all the activities for this user in the last 7 days.
- What type of unusual activities did the user engage in the last 7 days?
- What type of exfiltration activities did the user engage in the last 5 days?
- What type of sequential activities did the user engage in the last 10 days?
- What are the data risks related to this alert?
- For the files related to the alert, show me all activities done in last 7 days
- Can you get me the status of labeling on these files?
- What Suspicious Actions Have Been Performed On This Files?
- List all active Purview Policies covering the sensitive data in the file
- List all active purview policies applied to this user
- What other DLP alerts are present for this user?
- According to Purview, What is the implication of these DLP Alerts
- How many DLP policies have adaptive protection configured?

EMBEDDED

- Comprehensive summary of Data Loss Prevention alerts
- Comprehensive summary of Insider Risk Management alerts
- Contextual summary of Communication Compliance policy matches
- Contextual summary of evidence collected in eDiscovery review sets
- Natural language conditions for eDiscovery searches
- Keyword query language from natural language in eDiscovery

and more...

Patrocinadores



