



Utilice Cloud Data Sense

Cloud Data Sense

NetApp
March 08, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-data-sense/task-controlling-governance-data.html> on March 08, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

- Utilice Cloud Data Sense 1
 - Ver los detalles de gobernanza sobre los datos almacenados en su organización. 1
 - Ver los detalles de cumplimiento de normativas sobre los datos almacenados en la empresa 6
 - Categorías de datos privados 13
 - Investigue los datos almacenados en su organización 20
 - Organizar sus datos privados 29
 - Asignación de políticas a sus datos 38
 - Gestione sus datos privados 49
 - Ver informes de cumplimiento 59

Utilice Cloud Data Sense

Ver los detalles de gobernanza sobre los datos almacenados en su organización

Controle los costes relacionados con los datos que residen en los recursos de almacenamiento de su organización. Cloud Data Sense identifica la cantidad de datos desfasados, datos no empresariales, archivos duplicados y archivos de gran tamaño de sus sistemas para poder decidir si desea quitar o organizar algunos archivos en niveles en un almacenamiento de objetos menos costoso.

Además, si tiene pensado migrar datos desde ubicaciones locales al cloud, puede visualizar el tamaño de los datos y si alguno de ellos contiene información confidencial antes de moverlos.

El panel de control de gobierno

La consola de gobernanza proporciona información para que pueda aumentar la eficiencia y controlar los costes relacionados con los datos almacenados en sus recursos de almacenamiento.

Savings Opportunities

Stale Data 1

120K Items | 102.9 GB

Optimize Storage

Non-Business Data 1

9.3K Items | 16.7 GB

Optimize Storage

Duplicate Files 1

200K Items | 90.6 GB

Optimize Storage

Policies [View All](#)

Find Duplicate 290K Items

Paul Sensitive 280K Items

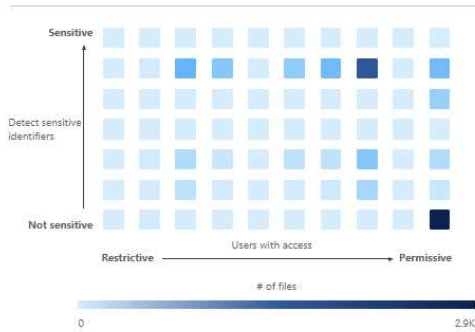
Data Overview

Scanned [Full Data Mapping Overview Report](#) 506.2 GB | 491K Files | 68 Tables

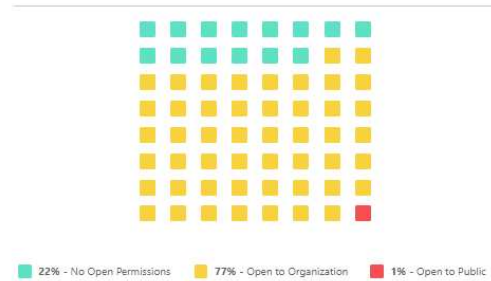
Top Data Repositories by Sensitivity Level



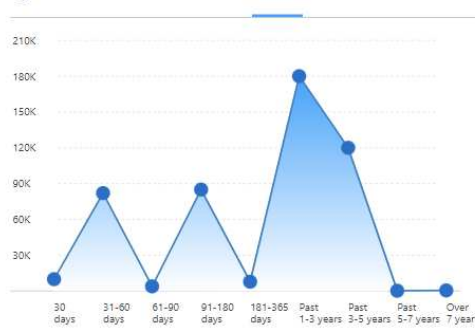
Sensitive Data and Wide Permissions



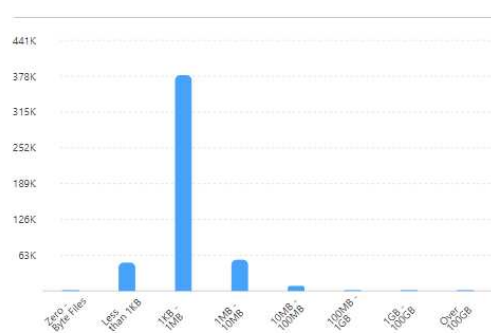
Open Permissions



Age of Data



Size of Data



Classification

41 Categories [View All](#)

Legal - Vendor-Customer Co... 12K Items

HR - Employee Contracts 7.5K Items

HR - Resumes 6.8K Items

Miscellaneous Documents 420K Items

108 File Types [View All](#)

PDF 200K Items

TXT 190K Items

DOCX 68K Items

DOC 9.6K Items

6 Labels [View All](#)

Highly Confidential 64K Items

Classified 10 Items

General 9 Items

aditest 2 Items

Guardando oportunidades

Puede que desee investigar los elementos del área *Saving Opportunities* para ver si hay datos que debe eliminar o organizar en niveles un almacenamiento de objetos menos costoso. Haga clic en cada elemento para ver los resultados filtrados en la página Investigación.

- * Datos obsoletos* - datos que se modificaron por última vez hace 3 años.
- **Datos no profesionales** - datos que se consideran no relacionados con el negocio, en función de su categoría o tipo de archivo. Estos recursos incluyen:
 - Datos de aplicaciones
 - Audio
 - Ejecutables
 - Imágenes
 - Registros
 - Vídeos
 - Varios (categoría general "otros")
- **Duplicar archivos:** Archivos duplicados en otras ubicaciones de los orígenes de datos que está analizando. ["Consulte qué tipos de archivos duplicados se muestran"](#).

Políticas con el mayor número de resultados

En el área *Policies*, las políticas con mayor número de resultados aparecen en la parte superior de la lista. Haga clic en el nombre de una directiva para mostrar los resultados en la página Investigación. Haga clic en **Ver todo** para ver la lista de todas las directivas disponibles.

Haga clic en ["aquí"](#) Para obtener más información acerca de las políticas.

Descripción general de los datos

La sección *Data Overview* proporciona una rápida descripción general de todos los datos que se están analizando. Haga clic en el botón para descargar un informe completo de asignación de datos que incluya capacidad de uso, antigüedad de los datos, tamaño de los datos y tipos de archivo para todos los entornos de trabajo y orígenes de datos. Consulte [Informe de asignación de datos](#) para obtener todos los detalles de este informe.

Principales repositorios de datos listados por sensibilidad de datos

El área *Top Data Repository by Sensitivity Level* enumera los cuatro principales repositorios de datos (entornos de trabajo y orígenes de datos) que contienen los elementos más sensibles. El gráfico de barras de cada entorno de trabajo se divide en:

- Datos no confidenciales
- Datos personales
- Datos personales confidenciales

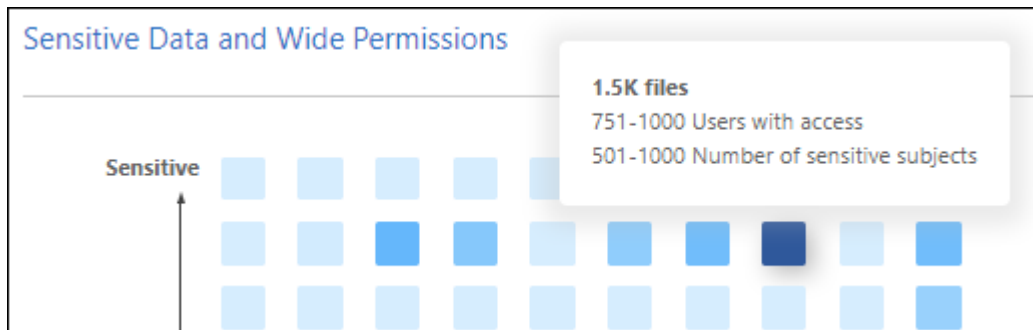
Puede pasar el ratón sobre cada sección para ver el número total de elementos de cada categoría.

Haga clic en cada área para ver los resultados filtrados en la página Investigación para que pueda seguir investigando.

Datos listados por sensibilidad y permisos amplios

El área *Sensitive Data y Wide Permissions* proporciona un mapa térmico de los archivos que contienen datos confidenciales (incluidos datos personales confidenciales y confidenciales) y que son demasiado permisivos. Esto puede ayudarle a ver dónde puede tener algunos riesgos con datos confidenciales.

Los archivos se clasifican en función del número de usuarios con permiso para acceder a los archivos del eje X (del más bajo al más alto) y del número de identificadores confidenciales dentro de los archivos del eje Y (del más bajo al más alto). Los bloques representan el número de archivos que coinciden con los elementos de los ejes X e Y. El bloque de color más claro es bueno; con menos usuarios capaces de acceder a los archivos y con menos identificadores confidenciales por archivo. Los bloques más oscuros son los elementos que tal vez desee investigar. Por ejemplo, la siguiente pantalla muestra el texto de desplazamiento del bloque azul oscuro. Muestra que tiene 1,500 archivos en los que 751-1000 usuarios tienen acceso y donde hay 501-1000 identificadores confidenciales por archivo.



Puede hacer clic en el bloque en el que está interesado para ver los resultados filtrados de los archivos afectados en la página Investigación para poder seguir investigando.

No se muestra ningún dato en este panel si no ha integrado un servicio de identidad con detección de datos. ["Descubra cómo integrar su servicio Active Directory con Data Sense"](#).



Este panel admite archivos en recursos compartidos de CIFS, OneDrive y orígenes de datos de SharePoint. Actualmente no existe compatibilidad con bases de datos, Google Drive, Amazon S3 y el almacenamiento de objetos genérico.

Datos listados por tipos de permisos abiertos

El área *Open Permissions* muestra el porcentaje de cada tipo de permisos que existen para todos los archivos que se están analizando. El gráfico muestra los siguientes tipos de permisos:

- Sin permisos abiertos
- Abierto a la organización
- Abierto al público
- Acceso desconocido

Puede pasar el ratón sobre cada sección para ver el número total de archivos de cada categoría. Haga clic en cada área para ver los resultados filtrados en la página Investigación para que pueda seguir investigando.

Antigüedad de los datos y tamaño de los gráficos de datos

Puede que desee investigar los elementos de los gráficos *Age* y *Size* para ver si hay datos que debe eliminar o organizar en niveles un almacenamiento de objetos menos costoso.

Puede pasar el ratón sobre un punto de los gráficos para ver detalles sobre la antigüedad o el tamaño de los datos de esa categoría. Haga clic para ver todos los archivos filtrados por esa edad o rango de tamaño.

- * Edad del Gráfico de datos* - categoriza los datos en función de la hora en que se creó, la última vez que se accedió o la última vez que se modificó.
- * Tamaño del gráfico de datos* - categoriza los datos en función del tamaño.

La mayoría de las clasificaciones de datos identificadas

El área *Classification* proporciona una lista de los más identificados "[Categorías](#)", "[Tipos de archivo](#)", y "[Etiquetas AIP](#)" en los datos escaneados.

Categorías

Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como "currículos" o "contratos de empleados" puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.

Consulte "[Ver archivos por categorías](#)" si quiere más información.

Tipos de archivo

La revisión de los tipos de archivo puede ayudarle a controlar los datos confidenciales porque puede encontrar que determinados tipos de archivo no se almacenan correctamente.

Consulte "[Visualización de tipos de archivo](#)" si quiere más información.

Etiquetas AIP

Si se ha suscrito a la protección de información de Azure (AIP), puede clasificar y proteger documentos y archivos aplicando etiquetas al contenido. La revisión de las etiquetas AIP más utilizadas que se asignan a los archivos le permite ver qué etiquetas se utilizan más en sus archivos.

Consulte "[Etiquetas AIP](#)" si quiere más información.

Informe de asignación de datos

El informe de asignación de datos proporciona una descripción general de los datos que se almacenan en sus fuentes de datos empresariales para ayudarle en la toma de decisiones de migración, copia de seguridad, seguridad y procesos de cumplimiento de normativas. En el informe se incluye, en primer lugar, un informe general en el que se resumen todos sus entornos de trabajo y fuentes de datos y, a continuación, se presenta un desglose de cada entorno de trabajo.

El informe incluye la siguiente información:

Capacidad de uso

Para todos los entornos de trabajo: Enumera el número de archivos y la capacidad utilizada para cada entorno de trabajo. Para entornos de trabajo individuales: Enumera los archivos que utilizan la mayor capacidad.

Antigüedad de los datos

Proporciona tres gráficos para cuándo se crearon los archivos, la última modificación o el último acceso. Enumera el número de archivos y su capacidad utilizada, en función de determinados rangos de fechas.

Tamaño de los datos

Enumera el número de archivos que existen dentro de determinados rangos de tamaño en los entornos de trabajo.

Tipos de archivo

Enumera el número total de archivos y la capacidad utilizada para cada tipo de archivo que se almacena en sus entornos de trabajo.

Generación del Informe de asignación de datos

Vaya a la ficha detección de datos para generar el informe.


Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Gobierno** y, a continuación, haga clic en el botón **Informe de visión general de mapas de datos completos** del Panel de gobierno.



Resultado

Cloud Data Sense genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Tenga en cuenta que puede personalizar el nombre de la empresa que aparece en la primera página del informe desde la parte superior de la página de detección de datos haciendo clic en  Y, a continuación, haga clic en **Cambiar nombre de compañía**. La próxima vez que genere el informe, incluirá el nuevo nombre.

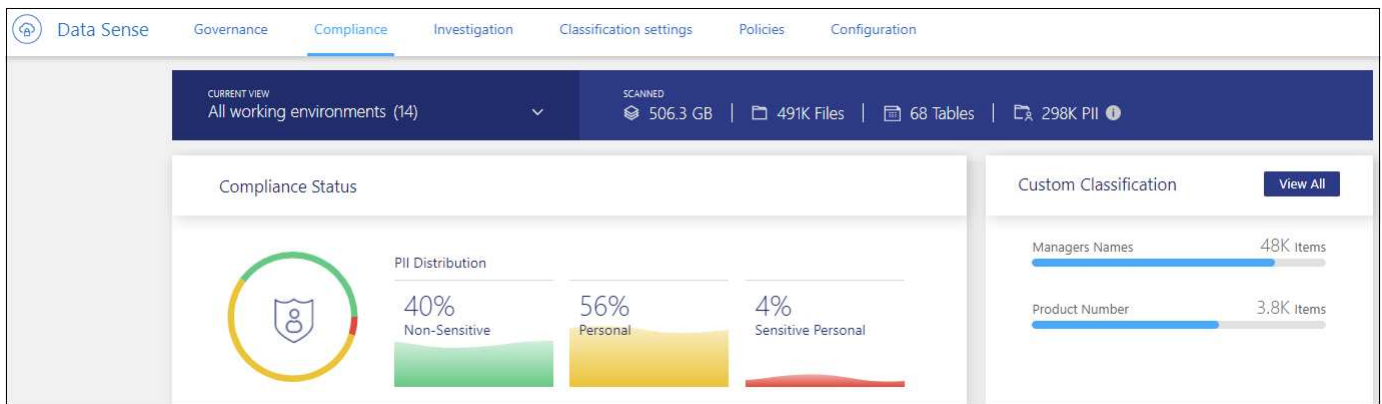
Ver los detalles de cumplimiento de normativas sobre los datos almacenados en la empresa

Controle sus datos privados al ver los detalles sobre los datos personales y los datos personales confidenciales de su empresa. También puede obtener visibilidad revisando las categorías y los tipos de archivo que se encuentran en Cloud Data en sus datos.



Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

De forma predeterminada, el panel Cloud Data Sense muestra los datos de cumplimiento de normativas de todas las bases de datos y entornos de trabajo.



Si sólo desea ver datos para algunos de los entornos de trabajo, [seleccione esos entornos de trabajo](#).

También puede filtrar los resultados desde la página Investigación de datos y descargar un informe de los resultados como un archivo CSV. Consulte ["Filtrar datos en la página Investigación de datos"](#) para obtener más detalles.

Visualización de archivos que contienen datos personales

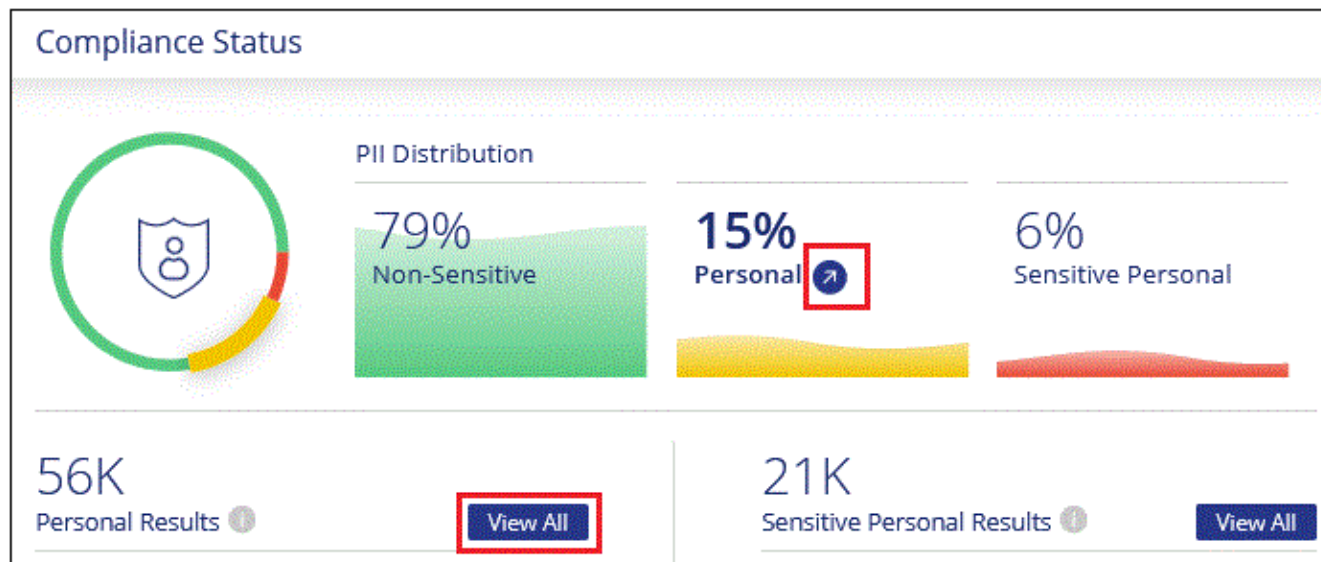
Cloud Data Sense identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. Por ejemplo, Información de identificación personal (PII), números de tarjeta de crédito, números de seguridad social, números de cuenta bancaria, contraseñas, y sigue. ["Consulte la lista completa"](#). Data Sense identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de base de datos.

Además, si ha agregado un servidor de bases de datos para analizar, la función *Data Fusion* permite analizar los archivos para identificar si se encuentran identificadores únicos de las bases de datos en esos archivos u otras bases de datos. Consulte ["Adición de identificadores de datos personales mediante Data Fusion"](#) para obtener más detalles.

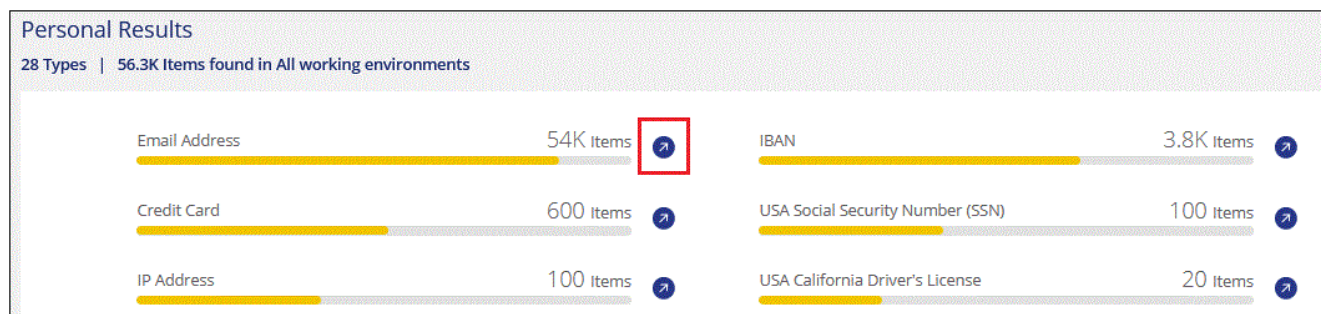
Para algunos tipos de datos personales, Data Sense utiliza *proximity validation* para validar sus hallazgos. La validación se produce buscando una o más palabras clave predefinidas cerca de los datos personales encontrados. Por ejemplo, Data Sense identifica a un EE. UU Número de seguridad social (SSN) como un SSN si ve una palabra de proximidad junto a ella (por ejemplo, *SSN* o *seguridad social*). ["La tabla de datos personales"](#) Muestra cuándo la detección de datos utiliza la validación de proximidad.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Para investigar los detalles de todos los datos personales, haga clic en el icono situado junto al porcentaje de datos personales.



3. Para investigar los detalles de un tipo específico de datos personales, haga clic en **Ver todos** y, a continuación, en el icono **investigar resultados** para un tipo específico de datos personales; por ejemplo, direcciones de correo electrónico.



4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Las 2 capturas de pantalla siguientes muestran datos personales encontrados en archivos individuales y encontrados en archivos dentro de directorios (recursos compartidos y carpetas). También puede seleccionar la ficha **estructurado** para ver los datos personales encontrados en las bases de datos.

Unstructured (54.6K Files) | Directories (6 Folders) | Structured (3 Tables) | Search by File Table or location

54.6K items

Tags | Assign to | Label | Move | Copy | Delete

File Name | Personal | Sensitive Personal | Data Subjects | File Type

customer-data.xls | S3 | 688 | 0 | 63 | XLS

Tags: Credit Cards | gidi | tartanpion

Working Environment (Account): S3 - 759995470648

Storage Repository (Bucket): compliancedemofiles

File Path: /Patterns/NEW SSN/customer-data.xls

Category: Miscellaneous Spreadsheets

File Size: 142.35 KB

Discovered Time: 2020-11-16 12:40

Created Time: 2019-12-16 12:18 | Last Modified: 2019-12-16 12:18

Open Permissions: NOT PUBLIC

Duplicates: 2 | View Details

Tags: 3 tags

Assigned to: Alona Tyupa

Assign a Label to this file

Copy File

Move File

Delete File

Give feedback on this result

Unstructured (491.4K Files) | Directories (60.7K Folders) | Structured (45 Tables) | Search by File, Table or location

60.7K items

Tags | Assign to | Label | Move | Copy | Delete

Directory Name | Storage Repository | Personal | Sensitive Personal | Type

cifs_labs_share | CVO | cifs_labs | 4 | 1 | Share

/datasensecopy/C\$/... | ANF | datasensecopy | 2 | 10 | Folder

Working Environment: Azure NetApp Files

Storage Repository (Volume): datasensecopy

Directory Path: /datasensecopy/copy_63/contextual_data/C\$/Users/shraga.WESTEROS/Desktop/...

Discovered Time: 2022-07-10 22:58

Last Modified: 2020-02-06 09:57

Visualización de archivos que contienen datos personales confidenciales

Cloud Data Sense identifica automáticamente tipos especiales de información personal confidencial, tal y como se define en normativas de privacidad como "Artículos 9 y 10 del RGPD". Por ejemplo, información sobre la salud, origen étnico o orientación sexual de una persona. "Consulte la lista completa". Data Sense identifica este tipo de información en archivos individuales, en archivos dentro de directorios (recursos compartidos y carpetas) y en tablas de base de datos.

Cloud Data Sense utiliza la inteligencia artificial (IA), el procesamiento de lenguaje natural (NLP), el aprendizaje automático (ML) y la computación cognitiva (CC) para comprender el significado del contenido que analiza con el fin de extraer entidades y categorizar según corresponda.

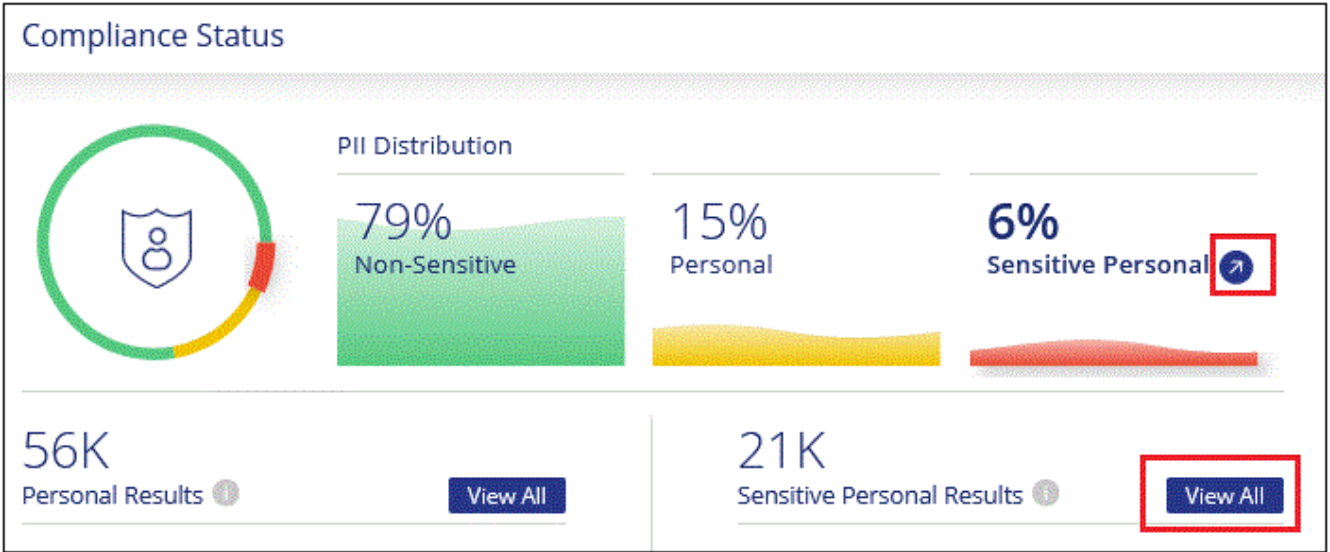
Por ejemplo, una categoría de datos confidenciales sobre el GDPR es su origen étnico. Debido a sus capacidades NLP, Data Sense puede distinguir la diferencia entre una frase que dice "George es mexicano" (que indica datos confidenciales como se especifica en el artículo 9 del RGPD), frente a "George está comiendo comida mexicana".



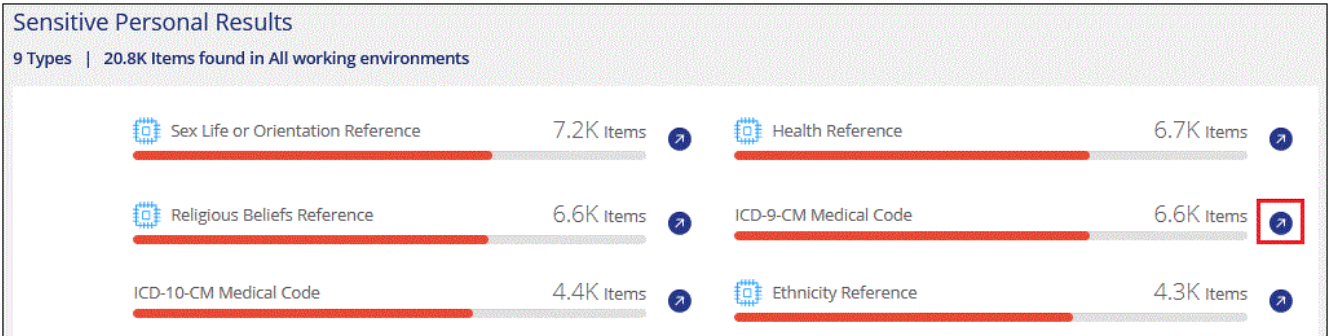
Sólo se admite inglés cuando se escanea datos personales confidenciales. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Para investigar los detalles de todos los datos personales confidenciales, haga clic en el icono situado junto al porcentaje de datos personales confidenciales.



3. Para investigar los detalles de un tipo específico de datos personales confidenciales, haga clic en **Ver todo** y, a continuación, haga clic en el icono **investigar resultados** para obtener un tipo específico de datos personales confidenciales.



4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Ver archivos por categorías

Cloud Data Sense toma los datos que ha analizado y los divide en diferentes tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. ["Vea la lista de categorías"](#).

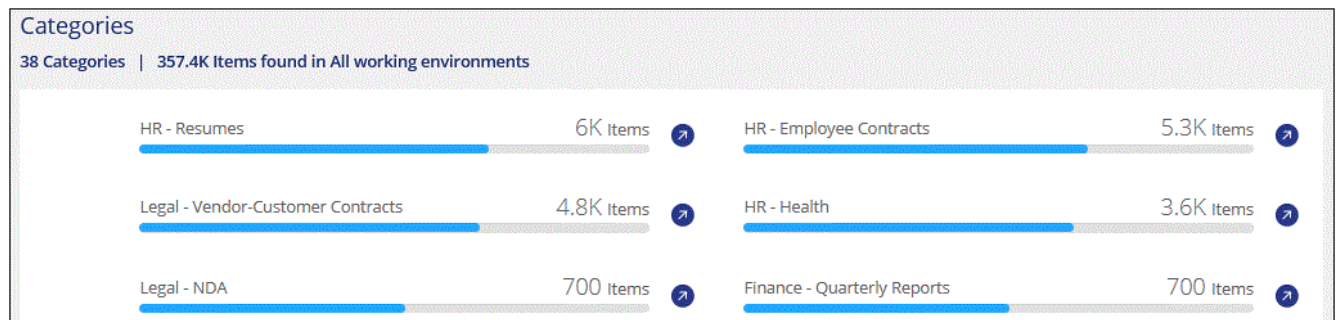
Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como currículos o contratos de empleados puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.



Las categorías son: Inglés, alemán y español. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Haga clic en el icono **investigar resultados** de una de las 4 categorías principales directamente desde la pantalla principal, o haga clic en **Ver todos** y luego haga clic en el icono de cualquiera de las categorías.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

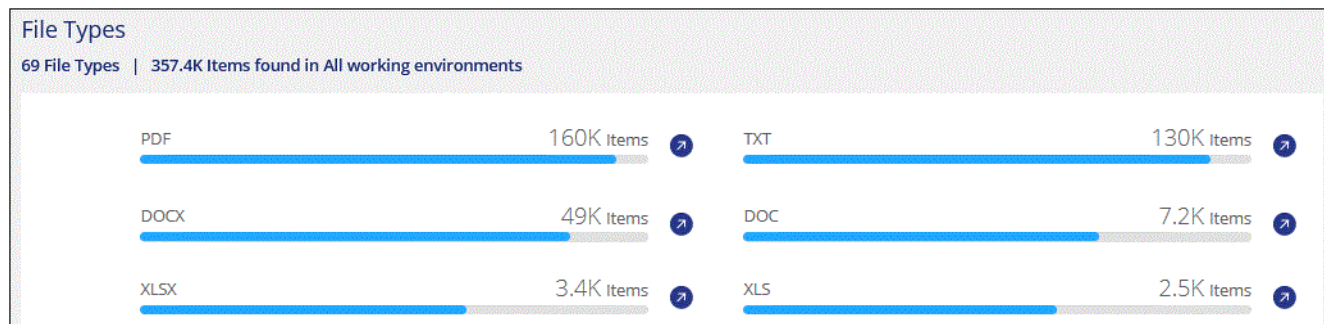
Ver archivos por tipos de archivos

Cloud Data Sense toma los datos que ha analizado y los divide por tipo de archivo. La revisión de los tipos de archivo puede ayudarle a controlar los datos confidenciales porque puede encontrar que determinados tipos de archivo no se almacenan correctamente. ["Consulte la lista de tipos de archivo"](#).

Por ejemplo, puede almacenar archivos CAD que incluyan información muy confidencial sobre su organización. Si no está seguro, puede tomar el control de los datos confidenciales restringiendo permisos o moviendo los archivos a otra ubicación.

Pasos

1. En el menú de navegación izquierdo de BlueXP, haga clic en **Gobierno > Clasificación** y, a continuación, haga clic en la ficha **cumplimiento**.
2. Haga clic en el icono **investigar resultados** de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todos** y, a continuación, haga clic en el icono de cualquiera de los tipos de archivo.



- Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

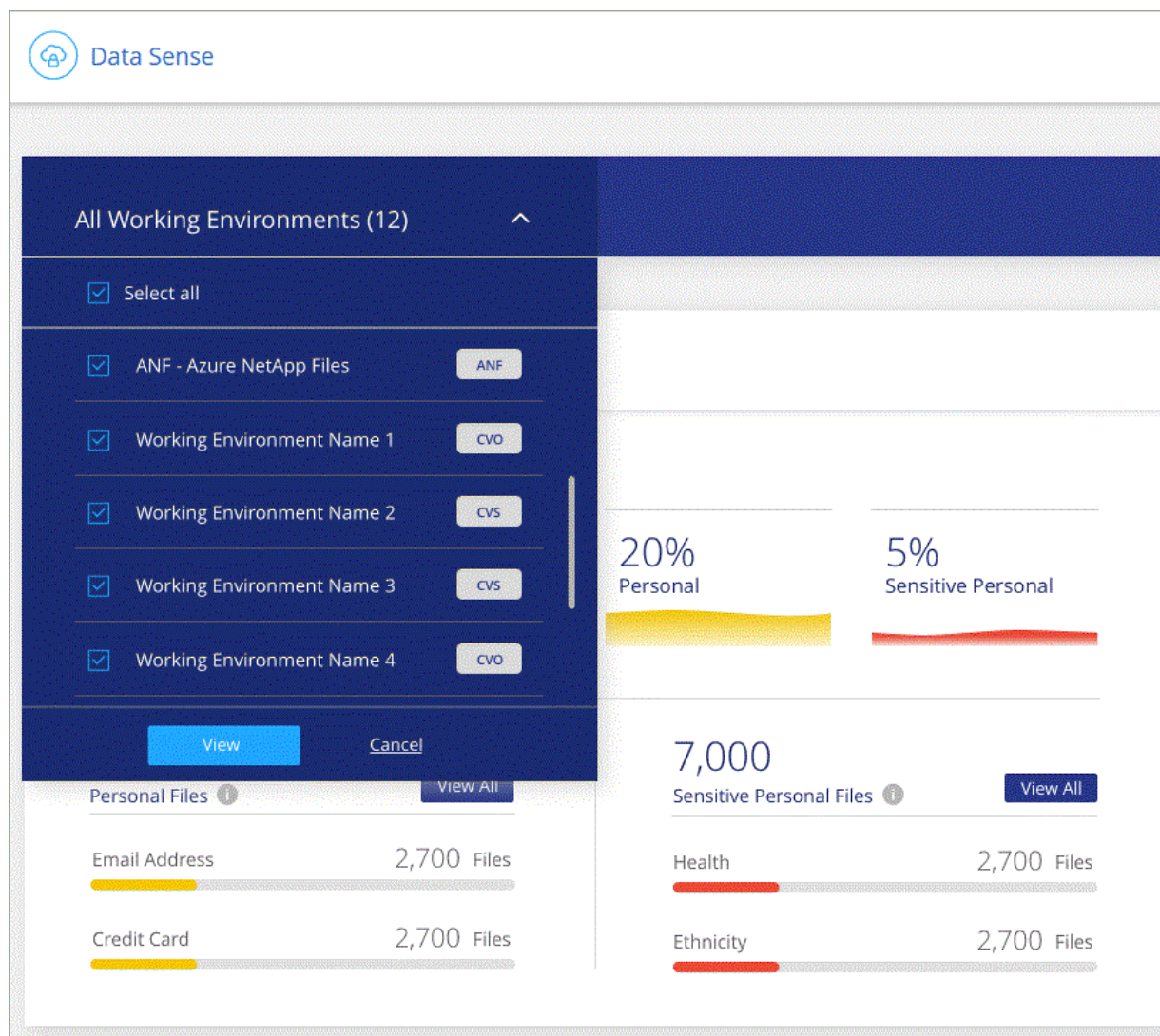
Visualización de datos de Dashboard para entornos de trabajo específicos

Puede filtrar el contenido del panel Cloud Data Sense para ver los datos de cumplimiento de normativas de todos los entornos y bases de datos de trabajo, o bien solo para entornos de trabajo específicos.

Cuando se filtra el panel, detección de datos define los datos de cumplimiento e informa únicamente a los entornos de trabajo seleccionados.

Pasos

- Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.



Categorías de datos privados

Hay muchos tipos de datos privados que Cloud Data Sense puede identificar en sus volúmenes, bloques de Amazon S3, bases de datos, carpetas de OneDrive, cuentas de SharePoint, Y cuentas de Google Drive. Vea las categorías a continuación.



Si necesita Cloud Data Sense para identificar otros tipos de datos privados, como números de identificación nacionales adicionales o identificadores sanitarios, envíe un correo electrónico a ng-contact-data-sense@netapp.com con su solicitud.

Tipos de datos personales

Los datos personales encontrados en los archivos pueden ser datos personales generales o identificadores nacionales. La tercera columna de la tabla siguiente identifica si utiliza Cloud Data Sense "validación de proximidad" validar los resultados del identificador.

Los idiomas en los que se pueden reconocer estos elementos se identifican en la tabla.

Tenga en cuenta que puede agregar a la lista de datos personales que se encuentran en sus archivos. Si va a

analizar un servidor de bases de datos, la función *Data Fusion* permite elegir identificadores adicionales que el sentido de los datos en la nube buscará en sus análisis' seleccionando columnas en una tabla de base de datos. También puede agregar palabras clave personalizadas desde un archivo de texto o patrones personalizados utilizando una expresión regular. Consulte "[Adición de identificadores de datos personales a los análisis de detección de datos](#)" para obtener más detalles.

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés
Generales	Número de tarjeta de crédito	No	✓	✓	✓		✓
	Datos sujetos	No	✓	✓	✓		
	Dirección de correo electrónico	No	✓	✓	✓		✓
	Número de iban (número de cuenta bancaria internacional)	No	✓	✓	✓		✓
	Dirección IP	No	✓	✓	✓		✓
	Contraseña	Sí	✓	✓	✓		✓

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés
Identificadores nacionales							

Tipo	Identificador	¿validación de proximidad?	Inglés	Alemán	Español	Francés	Japonés
------	---------------	----------------------------	--------	--------	---------	---------	---------

	REINO UNIDO ID (NINO)	Sí	✓	✓	✓		
Tipo	Licencia de conducir de Estados Unidos California	Sí	✓	✓	✓		
	Licencia de conducir de Estados Unidos Indiana	¿validación de proximidad?	✓	✓	✓		
	Licencia de conducir de los Estados Unidos de Nueva York	Sí	✓	✓	✓		
	Número de Seguro Social de Estados Unidos (SSN)	Sí	✓	✓	✓		

Tipos de datos personales confidenciales

Los datos personales confidenciales que Cloud Data Sense puede encontrar en los archivos incluyen la siguiente lista.

Los elementos de esta categoría sólo se pueden reconocer en inglés en este momento.

Procedimientos penales referencia

Datos relativos a las condenas y delitos penales de una persona natural.

Referencia étnica

Datos relativos al origen racial o étnico de una persona natural.

Referencia de Salud

Datos relativos a la salud de una persona física.

Códigos médicos ICD-9-cm

Códigos utilizados en la industria médica y de la salud.

Códigos médicos ICD-10-cm

Códigos utilizados en la industria médica y de la salud.

Creencias filosóficas referencia

Datos relativos a las creencias filosóficas de una persona natural.

Opiniones políticas referencia

Datos relativos a las opiniones políticas de una persona natural.

Referencia de creencias religiosas

Datos relativos a las creencias religiosas de una persona natural.

Referencia de vida sexual o orientación

Datos relativos a la vida sexual o la orientación sexual de una persona natural.

Tipos de categorías

El sentido de los datos en el cloud categoriza sus datos de la siguiente forma.

La mayoría de estas categorías pueden ser reconocidas en inglés, alemán y español.

Categoría	Tipo	Inglés	Alemán	Español
Finanzas	Hojas de balance	✓	✓	✓
	Órdenes de compra	✓	✓	✓
	Facturas	✓	✓	✓
	Informes trimestrales	✓	✓	✓
RR. HH	Comprobaciones de fondo	✓		✓
	Planes de compensación	✓	✓	✓
	Contratos de empleados	✓		✓
	Revisiones de empleados	✓		✓
	Salud	✓		✓
	Se reanudará	✓	✓	✓
Legal	NDAS	✓	✓	✓
	Contratos con el proveedor y el cliente	✓	✓	✓
Marketing	Campañas	✓	✓	✓
	Conferencias	✓	✓	✓
Operaciones	Informes de auditoría	✓	✓	✓
Ventas	Pedidos de ventas	✓	✓	
Servicios	RFI	✓		✓
	RFP	✓		✓
	CERDA	✓	✓	✓
	Entrenamiento	✓	✓	✓
Soporte técnico	Quejas y boletos	✓	✓	✓

Los siguientes metadatos también se categorizan y se identifican en los mismos idiomas compatibles:

- Datos de aplicaciones
- Archivos de archivo
- Audio
- Datos de aplicaciones de negocio
- Archivos CAD
- Codificación
- Dañado
- Archivos de base de datos e índice
- Estadísticas de detección de datos
- Archivos de diseño
- Datos de aplicación de correo electrónico

- Cifrado (archivos con una puntuación de entropía alta)
- Ejecutables
- Datos de aplicaciones financieras
- Datos de aplicación de salud
- Imágenes
- Registros
- Documentos varios
- Presentaciones diversas
- Hojas de cálculo varias
- Varios "desconocidos"
- Archivos protegidos con contraseña
- Datos estructurados
- Vídeos
- Archivos de byte cero

Tipos de archivos

Cloud Data SENSE analiza todos los archivos en busca de información de categorías y metadatos y muestra todos los tipos de archivos en la sección tipos de archivos de la consola.

Sin embargo, cuando Data Sense detecta la Información personal identificable (PII) o cuando realiza una búsqueda DSAR, sólo se admiten los siguientes formatos de archivo:

.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides

Precisión de la información encontrada

NetApp no puede garantizar una precisión del 100 % de los datos personales y los datos personales confidenciales que identifique Cloud Data. Siempre debe validar la información revisando los datos.

Según nuestras pruebas, la siguiente tabla muestra la exactitud de la información que encuentra Data Sense. La dividiremos por *precision* y *RECALL*:

Precisión

La probabilidad de que lo que el sentido de datos encuentra se ha identificado correctamente. Por ejemplo, una tasa de precisión del 90% para los datos personales significa que 9 de cada 10 archivos identificados como que contienen información personal contienen realmente información personal. 1 de cada 10 archivos sería un falso positivo.

Recuperar

La probabilidad de que el sentido de los datos encuentre lo que debería. Por ejemplo, una tasa de recuperación del 70% para los datos personales significa que Data Sense puede identificar 7 de cada 10 archivos que contienen realmente información personal en su organización. El sentido de los datos provocaría un 30 % de los datos; estos no aparecerán en la consola.

Constantemente estamos mejorando la precisión de nuestros resultados. Dichas mejoras estarán disponibles automáticamente en versiones futuras de Data Sense.

Tipo	Precisión	Recuperar
Datos personales - General	90%-95%	60%-80%
Datos personales: Identificadores de país	30%-60%	40%-60%
Datos personales confidenciales	80%-95%	20%-30%
Categorías	90%-97%	60%-80%

Investigue los datos almacenados en su organización

Puede investigar los datos de su organización visualizando los detalles en la página Investigación de datos. Puede desplazarse a esta página desde muchas áreas de la interfaz de usuario de Data Sense, incluidos los paneles de control de gobierno y cumplimiento de normativas.



Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

Filtrar datos en la página Investigación de datos

Puede filtrar el contenido de la página de investigación para que muestre solo los resultados que desea ver. Esta es una característica muy eficaz porque después de afinar los datos, puede utilizar la barra de botones en la parte superior de la página para realizar una variedad de acciones, incluyendo copiar archivos, mover archivos, agregar una etiqueta o etiqueta AIP a los archivos, y mucho más.

Si desea descargar el contenido de la página como un informe después de haberlo afinado, haga clic en [botón](#). [Vaya aquí para obtener detalles sobre el informe de investigación de datos.](#)

The screenshot shows the 'Data Investigation' interface. At the top, there are tabs for 'Unstructured (364K Files)', 'Directories (64 Folders)', and 'Structured (45 Tables)'. A search bar is on the right. Below the tabs, there's a 'FILTERS' section on the left with expandable categories: Policies, Open Permissions, File Owner, Label, Working Environment Type (2), Working Environment, and Storage Repository (2). The main area displays a table of 364K items. The table has columns: File Name, Personal, Sensitive Personal, Data Subjects, and File Type. Each row represents a file, with checkboxes for selection and a dropdown arrow for file type. The files listed include 'cgdpr_yes_adam.txt' and 'true positive.txt'.

- Las pestañas de nivel superior le permiten ver datos de archivos (datos no estructurados), directorios (carpetas y archivos compartidos) o de bases de datos (datos estructurados).

- Los controles de la parte superior de cada columna permiten ordenar los resultados en orden numérico o alfabético.
- Los filtros del panel izquierdo permiten afinar los resultados seleccionando los atributos descritos en las secciones siguientes.

Filtrar datos por sensibilidad y contenido

Utilice los siguientes filtros para ver cuánta información confidencial contiene los datos.

Filtro	Detalles
Categoría	Seleccione la " tipos de categorías ".
Nivel de sensibilidad	Seleccione el nivel de sensibilidad: Personal, personal sensible o no confidencial.
Número de identificadores	Seleccione el rango de identificadores confidenciales detectados por archivo. Incluye datos personales y datos personales confidenciales. Al filtrar en directorios, Data Sense suma las coincidencias de todos los archivos de cada carpeta (y subcarpetas).
Datos personales	Seleccione la " tipos de datos personales ".
Datos personales confidenciales	Seleccione la " tipos de datos personales confidenciales ".
Asunto de los datos	Introduzca el nombre completo o el identificador conocido de un sujeto de datos.

Filtrar los datos por propietario y permisos de usuario

Utilice los siguientes filtros para ver los propietarios de archivos y los permisos para acceder a los datos.

Filtro	Detalles
Abra permisos	Seleccione el tipo de permisos dentro de los datos y dentro de carpetas o recursos compartidos.
Permisos de usuario/grupo	Seleccione uno o varios nombres de usuario y/o grupos, o introduzca un nombre parcial.
Propietario del archivo	Introduzca el nombre del propietario del archivo.
Número de usuarios con acceso	Seleccione uno o varios rangos de categorías para mostrar qué archivos y carpetas están abiertos a un determinado número de usuarios.

Filtrar los datos por tiempo

Utilice los siguientes filtros para ver datos según criterios de tiempo.

Filtro	Detalles
Hora de creación	Seleccione un intervalo de tiempo cuando se creó el archivo. También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda.

Filtro	Detalles
Hora de detección	Seleccione un intervalo de tiempo cuando Data Sense detectó el archivo. También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda.
Última modificación	Seleccione un intervalo de tiempo en el que se modificó por última vez el archivo. También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda.
Último acceso	Seleccione un intervalo de tiempo cuando se accedió por última vez al archivo o directorio (solo CIFS o NFS). También puede especificar un intervalo de tiempo personalizado para restringir aún más los resultados de la búsqueda. En el caso de los tipos de archivos que analiza Data Sense, es la última vez que Data Sense analizó el archivo.

Filtrar datos por metadatos

Utilice los siguientes filtros para ver los datos según la ubicación, el tamaño y el directorio o el tipo de archivo.

Filtro	Detalles
Ruta del archivo	Introduzca hasta 20 rutas parciales o completas que desee incluir o excluir de la consulta. Si introduce ambas rutas de acceso de inclusión y rutas de exclusión, Data Sense busca primero todos los archivos de las rutas de acceso incluidas, quita los archivos de las rutas de acceso excluidas y, a continuación, muestra los resultados. Tenga en cuenta que incluir "*" en este filtro no tiene ningún efecto; deberá buscar archivos y subcarpetas específicos utilizando rutas completas.
Tipo de directorio	Seleccione el tipo de directorio; "Compartir" o "carpeta".
Tipo de archivo	Seleccione la "tipos de archivos" .
Tamaño de archivo	Seleccione el rango de tamaño del archivo.
Hash de archivo	Introduzca el hash del archivo para buscar un archivo específico, aunque el nombre sea diferente.

Filtre los datos por tipo de almacenamiento

Utilice los siguientes filtros para ver datos por tipo de almacenamiento.

Filtro	Detalles
Tipo de entorno de trabajo	Seleccione el tipo de entorno de trabajo. OneDrive, SharePoint y Google Drive están clasificados en "aplicaciones".
Nombre del entorno de trabajo	Seleccione entornos de trabajo específicos.
Repositorio de almacenamiento	Seleccione el repositorio de almacenamiento, por ejemplo, un volumen o un esquema.

Filtre los datos por etiquetas, usuarios asignados y políticas

Utilice los siguientes filtros para ver los datos por etiquetas o etiquetas AIP.

Filtro	Detalles
Normativas	Seleccione una política o políticas. Vaya "aquí" para ver la lista de directivas existentes y crear sus propias directivas personalizadas.
Etiqueta	Seleccione "Etiquetas AIP" que se asignan a sus archivos.
Etiquetas	Seleccione "la etiqueta o las etiquetas" que se asignan a sus archivos.
Asignado a.	Seleccione el nombre de la persona a la que se asigna el archivo.

Filtrar datos por estado de análisis

Utilice el siguiente filtro para ver datos por el estado de análisis de detección de datos.

Filtro	Detalles
Estado del análisis	Seleccione una opción para mostrar la lista de archivos que están pendientes de primer análisis, que se han finalizado el análisis, que se han reescaneado pendiente o que no se han podido analizar.
Evento Análisis de exploración	Seleccione si desea ver los archivos que no estaban clasificados porque la detección de datos no pudo revertir la última hora a la que se accedió, o los archivos que se clasificaron aunque la detección de datos no pudo revertir la última hora a la que se accedió.

["Consulte los detalles acerca de la Marca de hora "última en la que se accedió""](#) Para obtener más información acerca de los elementos que aparecen en la página Investigación al filtrar mediante el filtrado del evento Análisis de Análisis.

Filtrar datos por duplicados

Utilice el siguiente filtro para ver los archivos duplicados en su almacenamiento.

Filtro	Detalles
Duplicados	Seleccione si el archivo está duplicado en los repositorios.

Visualización de metadatos de archivo

En el panel resultados de la investigación de datos puede hacer clic en  para cualquier archivo individual para ver los metadatos del archivo.

The screenshot shows a file management interface with a top bar indicating 364.9K items. Below the bar is a table of files. The first file is 'ground truth.xlsx' (1K, 0 tags, 0 data subjects, XLSX type). The second file is 'GM_PD 12-1-09 SP.xls.pdf' (930 tags, 0 data subjects, 901 data subjects, PDF type). A red box highlights the left arrow icon in the second file's row. Below the table, a detailed view of the selected file is shown. It includes metadata such as Working Environment (OneDrive daylabs.onmicrosoft.com), Storage Repository (User: ruh@daylabs.onmicrosoft.com), File Path (/scattered/26/GM_PD 12-1-09 SP.xls.pdf), Category (Miscellaneous Documents), File Size (427.46 KB), Discovered Time (2021-01-12 10:37), Created Time (2018-05-22 12:38), Last Modified (2018-10-22 13:28), and Duplicates (None). On the right side of the detailed view, there are buttons for 'Copy File', 'Move File', and 'Delete File', along with a section for 'Tags: 9 tags' and 'Assigned to: Amit Ashbel'.

Además de mostrarle el entorno de trabajo y el volumen en el que reside el archivo, los metadatos muestran mucha más información, incluidos los permisos de archivo, el propietario del archivo, si hay duplicados de este archivo y la etiqueta AIP asignada (si lo tiene ["AIP integrado en Cloud Data Sense"](#)). Esta información es útil si tiene previsto hacerlo ["Crear políticas"](#) porque puede ver toda la información que puede utilizar para filtrar sus datos.

Tenga en cuenta que no toda la información está disponible para todas las fuentes de datos - sólo lo que es apropiado para ese origen de datos. Por ejemplo, el nombre de volumen, los permisos y las etiquetas AIP no son relevantes para los archivos de la base de datos.

Al ver los detalles de un único archivo, hay algunas acciones que puede realizar en el archivo:

- Puede mover o copiar el archivo a cualquier recurso compartido NFS. Consulte ["Mover archivos de origen a un recurso compartido NFS"](#) y.. ["Copiando archivos de origen a un recurso compartido NFS"](#) para obtener más detalles.
- Puede eliminar el archivo. Consulte ["Eliminando archivos de origen"](#) para obtener más detalles.
- Puede asignar un estado determinado al archivo. Consulte ["Aplicación de etiquetas"](#) para obtener más detalles.
- Puede asignar el archivo a un usuario de BlueXP para que sea responsable de las acciones de seguimiento que se deban realizar en el archivo. Consulte ["Asignar usuarios a un archivo"](#) para obtener más detalles.
- Si ha integrado etiquetas AIP con Cloud Data Sense, puede asignar una etiqueta a este archivo o cambiar a una etiqueta diferente si ya existe. Consulte ["Asignación manual de etiquetas AIP"](#) para obtener más detalles.

Ver permisos para archivos y directorios

Para ver una lista de todos los usuarios o grupos que tienen acceso a un archivo o directorio y los tipos de permisos que tienen, haga clic en **Ver todos los permisos**. Este botón solo está disponible para datos en recursos compartidos CIFS, SharePoint Online, SharePoint en las instalaciones y OneDrive.

Tenga en cuenta que si ve SID (identificadores de seguridad) en lugar de nombres de usuario y de grupo, debe integrar Active Directory en el sentido de datos. "[Descubra cómo hacerlo](#)".

The screenshot shows a file management interface. On the left, a sidebar lists file details for 'Expense Report TPO-1060.pdf': Working Environment: WorkingEnvironment1, Repository: Volume Name, File Path: /Prod/labs-base/Expense Report TPO-1060.pdf, Category: Legal, File Size: 22 MB, Last Modified: 2019-08-06 07:51, Open Permissions: NO OPEN PERMISSIONS, and File Owner: Avy. A red box highlights the 'View all Permissions' button. On the right, a pop-up window titled 'Permissions list for "Expense Report TPO-1060.pdf"' displays a table of permissions.

User / Group	Name	Read	Write
User Name		✓	✓
Group Name		✓	✓
Group Name		✓	✓
John L		✓	✓
George H		✓	✓
Paul M		✓	✓
Ringo S		✓	✓

Puede hacer clic en  para que cualquier grupo vea la lista de usuarios que forman parte del grupo.

Además, Puede hacer clic en el nombre de un usuario o un grupo y la página de investigación se muestra con el nombre de ese usuario o grupo rellenado en el filtro "permisos de usuario/grupo" para poder ver todos los archivos y directorios a los que tiene acceso el usuario o grupo.

Buscando archivos duplicados en los sistemas de almacenamiento

Puede ver si se están almacenando ficheros duplicados en los sistemas de almacenamiento. Esto resulta útil para identificar áreas en las que puede ahorrar espacio de almacenamiento. También puede ser útil asegurarse de que determinados archivos que tienen permisos específicos o información confidencial no se dupliquen innecesariamente en sus sistemas de almacenamiento.

La detección de datos utiliza la tecnología de hashing para determinar los archivos duplicados. Si algún archivo tiene el mismo código hash que otro archivo, podemos estar 100% seguros de que los archivos son duplicados exactos, incluso si los nombres de archivo son diferentes.


Puede descargar la lista de archivos duplicados y enviarlos al administrador de almacenamiento para que puedan decidir qué archivos se pueden eliminar, si los hay. O usted puede "[eliminar el archivo](#)" usted mismo si está seguro de que una versión específica del archivo no es necesaria.

Ver todos los archivos duplicados


Si desea obtener una lista de todos los archivos duplicados en los entornos de trabajo y los orígenes de datos que está analizando, puede utilizar el filtro llamado **duplicados > tiene duplicados** en la página Investigación de datos.


Todos los archivos con duplicados de todos los tipos de archivo (sin incluir bases de datos), con un tamaño mínimo de 50 MB y/o que contengan información personal personal o confidencial, se mostrarán en la página de resultados.


Ver si se duplica un archivo específico


Si desea ver si un único archivo tiene duplicados, en el panel resultados de investigación de datos puede hacer clic en  para cualquier archivo individual para ver los metadatos del archivo. Si hay duplicados de un archivo determinado, esta información aparece junto al campo *Duplicates*.

Para ver la lista de archivos duplicados y su ubicación, haga clic en **Ver detalles**. En la página siguiente, haga clic en **Ver duplicados** para ver los archivos en la página Investigación.


 Last Modified: 2019-08-06 07:51


 Open Permissions: NO OPEN PERMISSIONS [View all Permissions](#)


 File Owner: Asaf Ley

 Duplicates: 3 [View Details](#)

Duplicates of File 'Name 1'




 Duplicates: 3


 Total Size of all Duplicates: 1GB

 File Hash: xxxxxx

[View Duplicates](#) [Close](#)

3 items

<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	



Puede usar el valor "hash de archivo" que se proporciona en esta página e introducirlo directamente en la página Investigación para buscar un archivo duplicado específico en cualquier momento, o puede usarlo en una directiva.

Informe de investigación de datos

El Informe de investigación de datos es una descarga del contenido filtrado de la página Investigación de datos.


Puede guardar el informe en la máquina local como un archivo .CSV (que puede incluir hasta 5,000 filas de

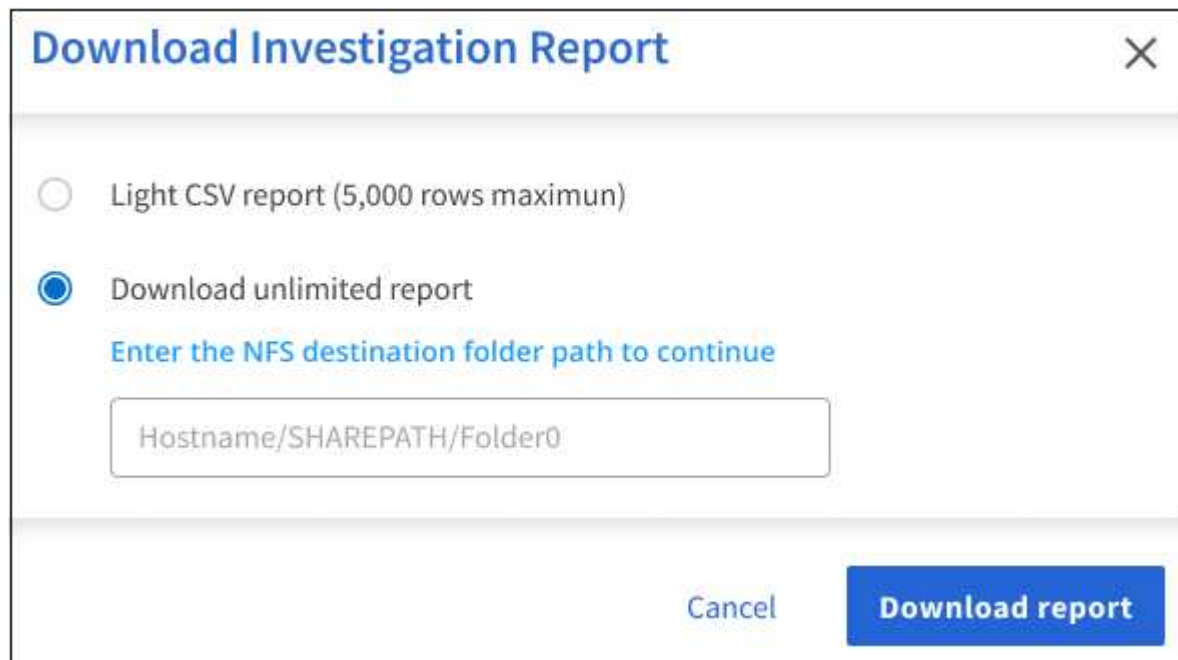
datos) o como un archivo .JSON que exporte a un recurso compartido NFS (que puede incluir un número ilimitado de filas). Si la detección de datos está analizando archivos (datos no estructurados), directorios (carpetas y recursos compartidos de archivos) o bases de datos (datos estructurados), puede descargar hasta tres archivos de informes.

Al exportar a un recurso compartido de archivos, asegúrese de que Data Sense tiene los permisos correctos para el acceso de exportación.

Generación del informe de investigación de datos

Pasos

1. En la página Data Investigation, haga clic en  en la parte superior derecha de la página.
2. Seleccione si desea descargar un informe .CSV o un informe .JSON de los datos y haga clic en **Descargar informe**.



The dialog box titled "Download Investigation Report" has a close button (X) in the top right corner. It contains two radio button options: "Light CSV report (5,000 rows maximum)" and "Download unlimited report". The "Download unlimited report" option is selected. Below these options is a text prompt "Enter the NFS destination folder path to continue" in blue. Underneath is a text input field with the placeholder text "Hostname/SHAREPATH/Folder0". At the bottom right, there are two buttons: "Cancel" and "Download report".

Al seleccionar un informe .JSON, introduzca el nombre del recurso compartido NFS al que se descargará el informe con el formato `<host_name>:/<share_path>`.

Resultado

Un cuadro de diálogo muestra un mensaje que indica que los informes se están descargando.

Puede ver el progreso de la generación de informes JSON en la ["Panel Estado de acciones"](#).

Lo que se incluye en cada informe de investigación de datos

El **Informe de datos de archivos no estructurados** incluye la siguiente información sobre sus archivos:

- Nombre de archivo
- Tipo de ubicación
- Nombre del entorno de trabajo
- Repositorio de almacenamiento (por ejemplo, un volumen, un bloque, recursos compartidos)

- Tipo de entorno de trabajo
- Ruta del archivo
- Tipo de archivo
- Tamaño de archivo
- Hora de creación
- Última modificación
- Último acceso
- Propietario del archivo
- Categoría
- Información personal
- Información personal confidencial
- Fecha de detección de eliminación

Una fecha de detección de eliminación identifica la fecha en la que se eliminó o movió el archivo. Esto le permite identificar cuándo se han movido los archivos confidenciales. Los archivos eliminados no forman parte del recuento de números de archivo que aparece en el panel o en la página Investigación. Los archivos solo aparecen en los informes CSV.

Informe de datos de directorios no estructurados incluye la siguiente información sobre sus carpetas y recursos compartidos de archivos:

- Nombre del entorno de trabajo
- Repositorio de almacenamiento (por ejemplo, una carpeta o archivos compartidos)
- Tipo de entorno de trabajo
- Ruta del archivo (nombre de directorio)
- Propietario del archivo
- Hora de creación
- Hora de detección
- Última modificación
- Último acceso
- Permisos abiertos
- Tipo de directorio

El **Informe de datos estructurados** incluye la siguiente información sobre las tablas de la base de datos:

- Nombre de tabla DE BASE de DATOS
- Tipo de ubicación
- Nombre del entorno de trabajo
- Repositorio de almacenamiento (por ejemplo, un esquema)
- Recuento de columnas
- Recuento de filas

- Información personal
- Información personal confidencial

Organizar sus datos privados

Cloud Data Sense ofrece muchas formas de gestionar y organizar sus datos privados. Esto le facilita ver los datos que más le importan.

- Si está suscrito a ["Protección de información de Azure \(AIP\)"](#) Para clasificar y proteger sus archivos, puede utilizar Cloud Data Sense para administrar esas etiquetas AIP.
- Puede agregar etiquetas a los archivos que desee marcar para la organización o para algún tipo de seguimiento.
- Puede asignar un usuario de BlueXP a un archivo específico, o a varios archivos, para que la persona pueda ser responsable de administrar el archivo.
- Con la funcionalidad "Directiva" puede crear sus propias consultas de búsqueda personalizadas para que pueda ver fácilmente los resultados haciendo clic en un botón.
- Puede enviar alertas por correo electrónico a los usuarios de BlueXP o a cualquier otra dirección de correo electrónico, cuando ciertas políticas críticas devuelvan resultados.



Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.

¿Debo usar etiquetas o etiquetas?

A continuación se ofrece una comparación del etiquetado de Data Sense y del etiquetado de la protección de la información de Azure.

Etiquetas	Etiquetas
Las etiquetas de archivo son una parte integrada de Data Sense.	Requiere que se haya suscrito a la protección de información de Azure (AIP).
La etiqueta sólo se guarda en la base de datos de detección de datos; no se escribe en el archivo. No cambia el archivo, ni los tiempos de acceso o modificación del archivo.	La etiqueta forma parte del archivo y cuando la etiqueta cambia, el archivo cambia. Este cambio también cambia los tiempos de acceso y modificación del archivo.
Puede tener varias etiquetas en un único archivo.	Puede tener una etiqueta en un solo archivo.
La etiqueta se puede utilizar para la acción de detección de datos interna, como copiar, mover, eliminar, ejecutar una política, etc.	Otros sistemas que pueden leer el archivo pueden ver la etiqueta, que se puede utilizar para automatización adicional.
Sólo se utiliza una sola llamada API para ver si un archivo tiene una etiqueta.	

Categorizar sus datos mediante etiquetas AIP

Puede administrar etiquetas AIP en los archivos que detección de datos en la nube está analizando si se ha suscrito ["Protección de información de Azure \(AIP\)"](#). AIP le permite clasificar y proteger documentos y archivos aplicando etiquetas al contenido. Data Sense permite ver las etiquetas que ya están asignadas a los archivos,

agregar etiquetas a los archivos y cambiar etiquetas cuando ya existe una etiqueta.

Cloud Data Sense admite etiquetas AIP dentro de los siguientes tipos de archivo: .DOC, .DOCX, .PDF, .PPTX, .XLS, .XLSX.



- Actualmente no puede cambiar etiquetas en archivos de más de 30 MB. Para las cuentas de OneDrive, SharePoint y Google Drive, el tamaño máximo del archivo es 4 MB.
- Si un archivo tiene una etiqueta que ya no existe en AIP, Cloud Data Sense la considera un archivo sin etiqueta.
- Si ha implementado Data Sense en una región gubernamental o en una ubicación local que no tiene acceso a Internet (también conocida como sitio oscuro), la funcionalidad de etiqueta AIP no estará disponible.

Integración de etiquetas AIP en el espacio de trabajo

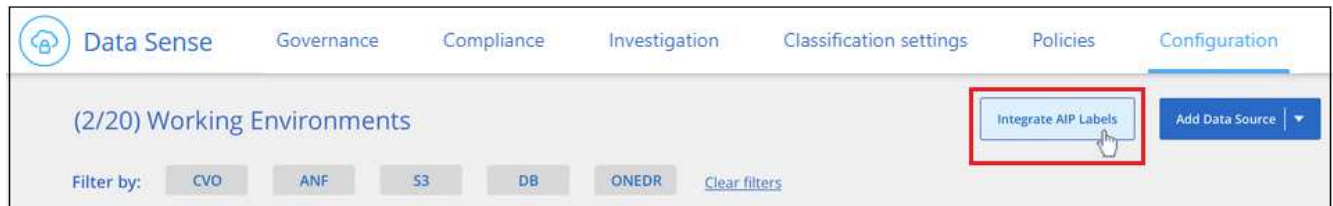
Antes de poder administrar etiquetas AIP, debe integrar la funcionalidad de etiquetas AIP en Cloud Data Sense iniciando sesión en su cuenta de Azure existente. Una vez activado, puede administrar etiquetas AIP dentro de los archivos para todos "fuentes de datos" En el espacio de trabajo de BlueXP.

Requisitos

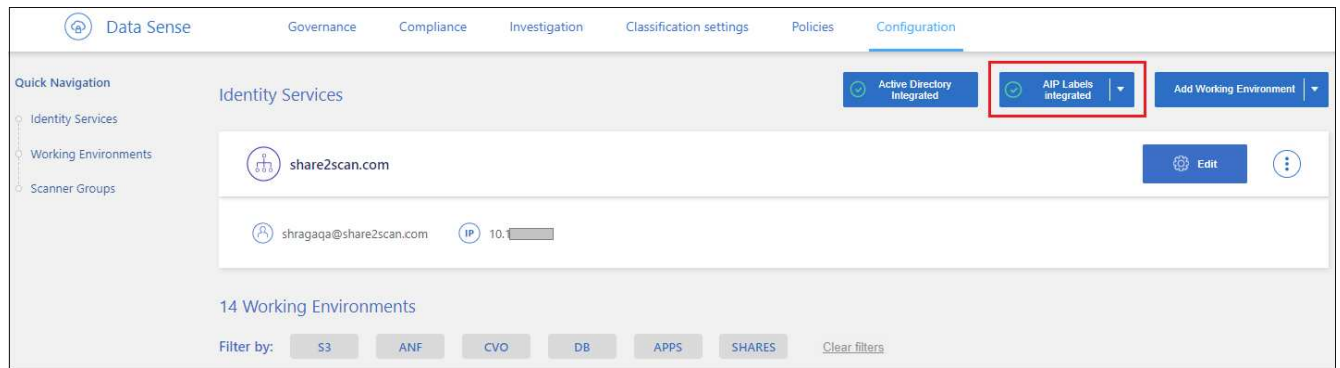
- Debe tener una cuenta y una licencia de Azure Information Protection.
- Debe tener las credenciales de inicio de sesión de la cuenta de Azure.
- Si planea cambiar las etiquetas de los archivos que residen en bloques de Amazon S3, asegúrese de que el permiso `s3:PutObject` se incluye en el rol IAM. Consulte "Configuración del rol IAM".

Pasos

1. En la página Configuración de detección de datos en la nube, haga clic en **integrar etiquetas AIP**.



2. En el cuadro de diálogo integrar etiquetas AIP, haga clic en **Iniciar sesión en Azure**.
3. En la página de Microsoft que aparece, seleccione la cuenta e introduzca las credenciales necesarias.
4. Vuelva a la ficha sentido de datos en la nube y verá el mensaje "AIP Labels se han integrado correctamente con la cuenta <account_name>".
5. Haga clic en **Cerrar** y verá el texto *AIP Labels integrated* en la parte superior de la página.




Resultado

Puede ver y asignar etiquetas AIP desde el panel de resultados de la página Investigación. También puede asignar etiquetas AIP a archivos mediante directivas.

Ver etiquetas AIP en los archivos

Puede ver la etiqueta AIP actual que está asignada a un archivo.

En el panel resultados de la investigación de datos, haga clic en  para que el archivo expanda los detalles de metadatos del archivo.




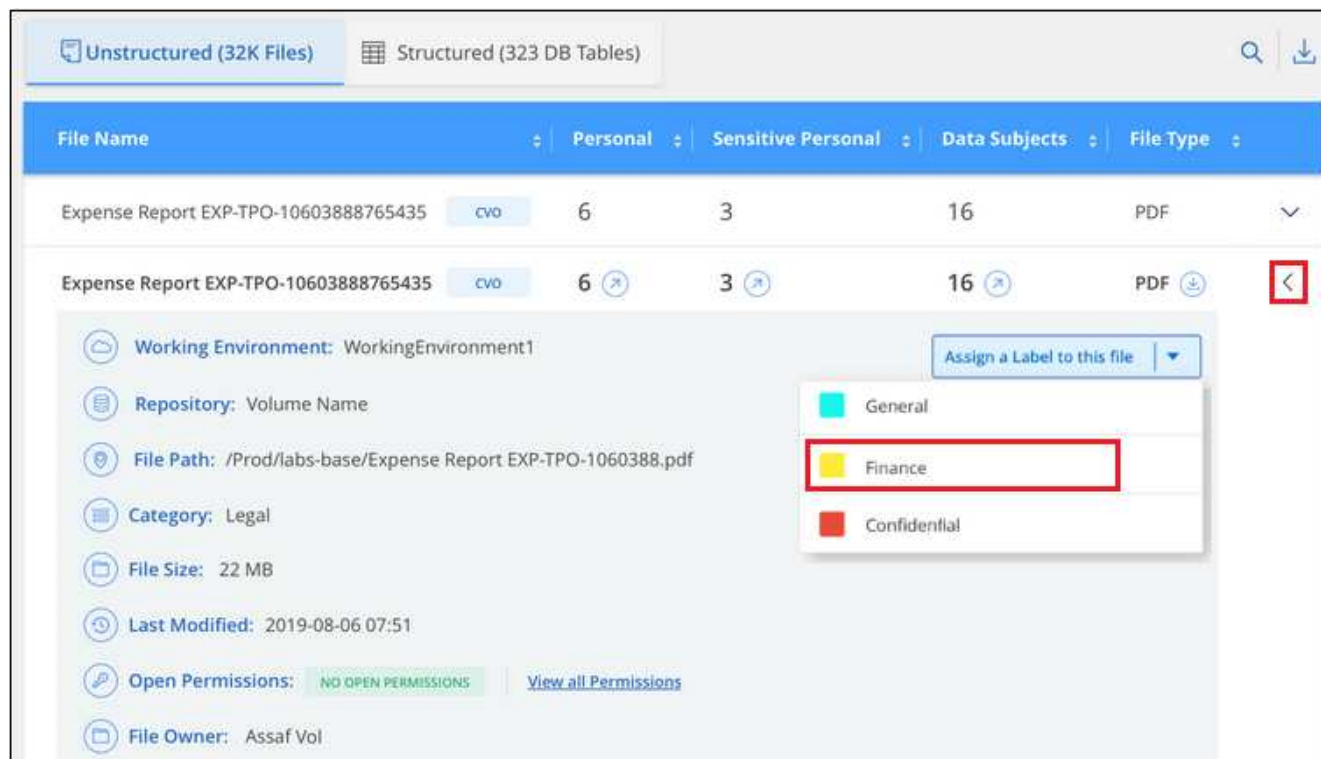
Asignación manual de etiquetas AIP

Puede agregar, cambiar y eliminar etiquetas AIP de sus archivos con Cloud Data Sense.

Siga estos pasos para asignar una etiqueta AIP a un único archivo.

Pasos

1. En el panel resultados de la investigación de datos, haga clic en  para que el archivo expanda los detalles de metadatos del archivo.



2. Haga clic en **asignar una etiqueta a este archivo** y, a continuación, seleccione la etiqueta.

La etiqueta aparece en los metadatos del archivo.

Para asignar una etiqueta AIP a varios archivos:

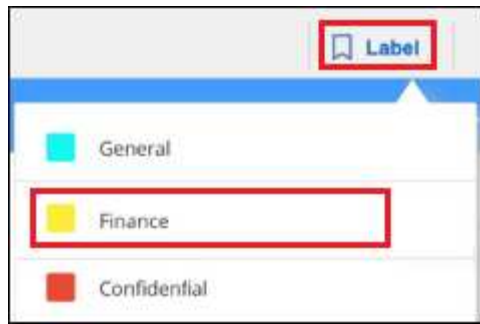
Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea etiquetar.



- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).

2. En la barra de botones, haga clic en **etiqueta** y seleccione la etiqueta AIP:



La etiqueta AIP se agrega a los metadatos de todos los archivos seleccionados.

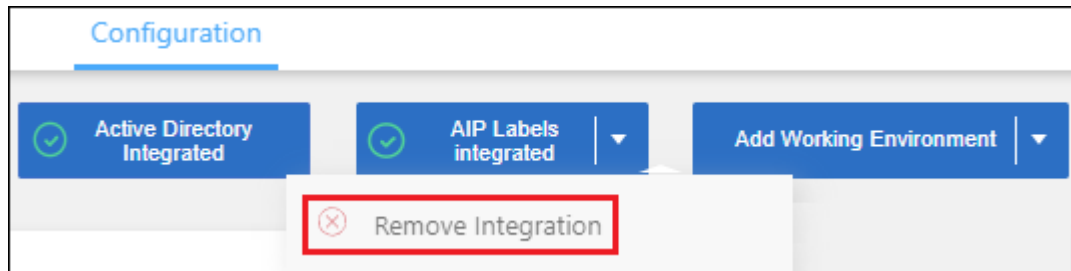
Eliminación de la integración AIP

Si ya no desea gestionar etiquetas AIP en archivos, puede eliminar la cuenta AIP de la interfaz de Cloud Data Sense.

Tenga en cuenta que no se realiza ningún cambio en las etiquetas que ha agregado con Data Sense. Las etiquetas que existen en los archivos permanecerán tal como existen actualmente.

Pasos

1. En la página *Configuration*, haga clic en **Etiquetas AIP integradas > Eliminar integración**.



2. Haga clic en **Eliminar integración** en el cuadro de diálogo de confirmación.

Aplicación de etiquetas para administrar los archivos capturados

Puede agregar una etiqueta a los archivos que desee marcar para algún tipo de seguimiento. Por ejemplo, es posible que haya encontrado algunos archivos duplicados y desee eliminar uno de ellos, pero debe comprobar qué se debe eliminar. Puede agregar una etiqueta de "comprobar para eliminar" al archivo para que sepa que este archivo requiere algún tipo de investigación y acción futura.

Data Sense permite ver las etiquetas asignadas a los archivos, agregar o quitar etiquetas de los archivos y cambiar el nombre o eliminar una etiqueta existente.

Tenga en cuenta que la etiqueta no se agrega al archivo de la misma manera que las etiquetas AIP forman parte de los metadatos del archivo. Los usuarios de BlueXP acaban de ver la etiqueta con Cloud Data Sense, por lo que puede ver si es necesario eliminar o comprobar un archivo para algún tipo de seguimiento.

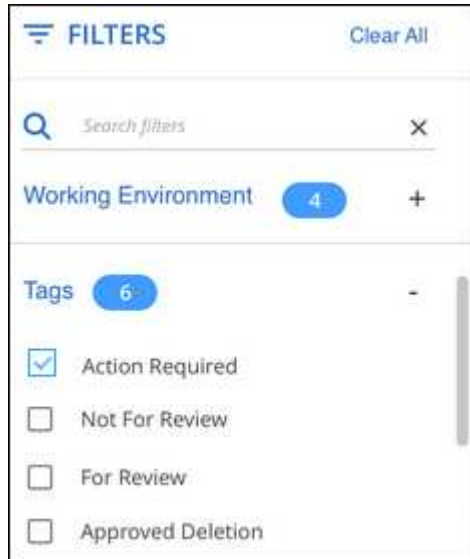


Las etiquetas asignadas a los archivos en Cloud Data Sense no están relacionadas con las etiquetas que puede agregar a los recursos, como volúmenes o instancias de máquinas virtuales. Las etiquetas de detección de datos se aplican en el nivel de archivo.

Ver archivos que tienen ciertas etiquetas aplicadas

Puede ver todos los archivos que tienen asignadas etiquetas específicas.

1. Haga clic en la ficha **Investigación** de Cloud Data Sense.
2. En la página Investigación de datos, haga clic en **Etiquetas** en el panel Filtros y, a continuación, seleccione las etiquetas necesarias.




El panel resultados de la investigación muestra todos los archivos que tienen asignadas esas etiquetas.

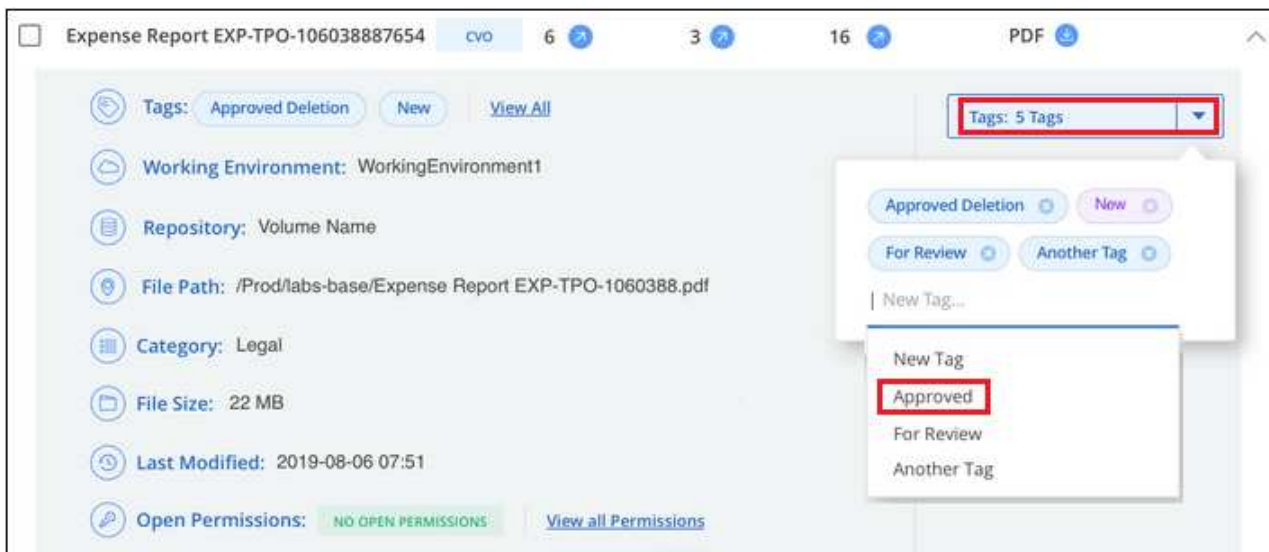
Asignar etiquetas a archivos

Puede agregar etiquetas a un único archivo o a un grupo de archivos.

Para agregar una etiqueta a un único archivo:

Pasos

1. En el panel resultados de la investigación de datos, haga clic en  para que el archivo expanda los detalles de metadatos del archivo.
2. Haga clic en el campo **Etiquetas** y se mostrarán las etiquetas asignadas actualmente.
3. Agregue la etiqueta o las etiquetas:
 - Para asignar una etiqueta existente, haga clic en el campo **Nueva etiqueta...** y empiece a escribir el nombre de la etiqueta. Cuando aparezca la etiqueta que está buscando, selecciónela y pulse **Intro**.
 - Para crear una nueva etiqueta y asignarla al archivo, haga clic en el campo **Nueva etiqueta...**, escriba el nombre de la nueva etiqueta y pulse **Intro**.



La etiqueta aparece en los metadatos del archivo.

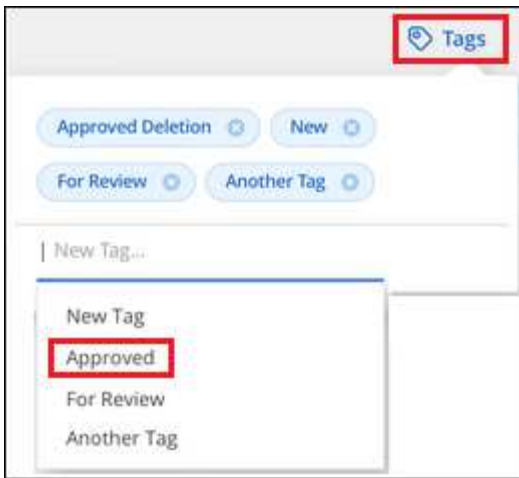
Para agregar una etiqueta a varios archivos:

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desee etiquetar.

2345 items						
<input type="checkbox"/>	File Name	Personal	Sensitive Personal	Data Subjects	File Type	
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF

- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
 - Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).
2. En la barra de botones, haga clic en **Etiquetas** y aparecerán las etiquetas asignadas actualmente.
 3. Agregue la etiqueta o las etiquetas:
 - Para asignar una etiqueta existente, haga clic en el campo **Nueva etiqueta...** y empiece a escribir el nombre de la etiqueta. Cuando aparezca la etiqueta que está buscando, selecciónela y pulse **Intro**.
 - Para crear una nueva etiqueta y asignarla al archivo, haga clic en el campo **Nueva etiqueta...**, escriba el nombre de la nueva etiqueta y pulse **Intro**.



4. Apruebe la adición de etiquetas en el cuadro de diálogo de confirmación y las etiquetas se agregarán a los metadatos de todos los archivos seleccionados.

Eliminar etiquetas de los archivos

Puede eliminar una etiqueta si ya no necesita utilizarla.

Sólo tiene que hacer clic en **x** para ver una etiqueta existente.



Si ha seleccionado varios archivos, la etiqueta se elimina de todos los archivos.

Asignar usuarios para administrar determinados archivos

Puede asignar un usuario de BlueXP a un archivo específico, o a varios archivos, para que pueda ser responsable de cualquier acción de seguimiento que necesite realizar en el archivo. Esta funcionalidad se suele utilizar con la función para agregar etiquetas de estado personalizadas a un archivo.

Por ejemplo, puede tener un archivo que contiene ciertos datos personales que permiten a demasiados usuarios acceso de lectura y escritura (permisos abiertos). Así que podría asignar la etiqueta de estado "Cambiar permisos" y asignar este archivo al usuario "Joan Smith" para que puedan decidir cómo solucionar el problema. Cuando hayan solucionado el problema, podrían cambiar la etiqueta de estado a "completado".

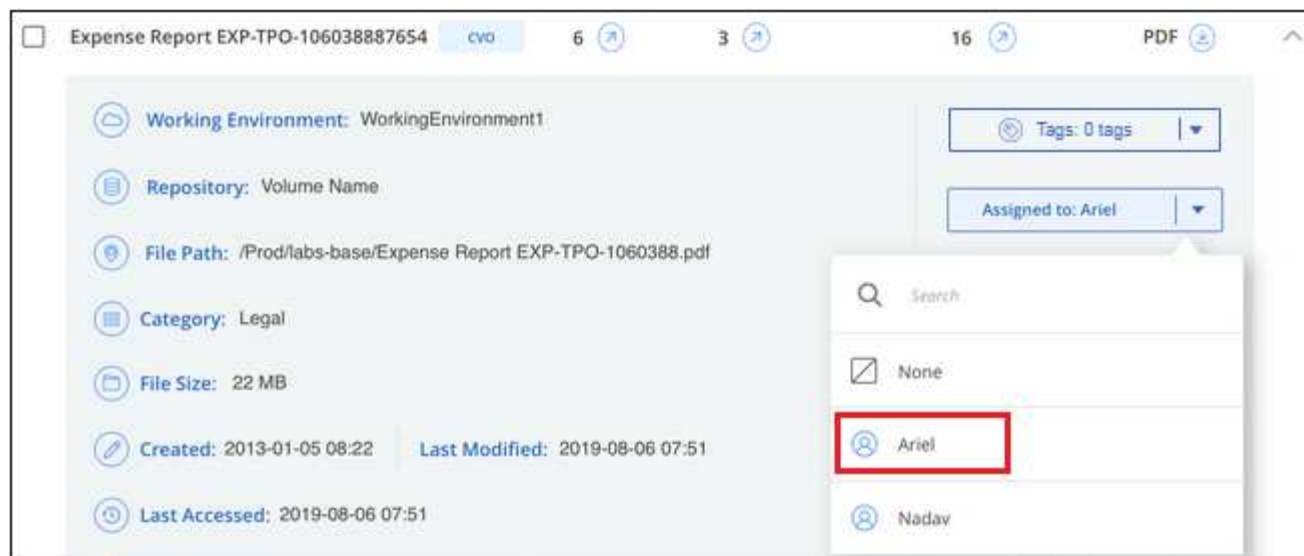
Tenga en cuenta que el nombre de usuario no se agrega al archivo como parte de los metadatos de los archivos; los usuarios de BlueXP acaban de ver al utilizar Cloud Data Sense.

Un filtro nuevo en la página Investigación le permite ver fácilmente todos los archivos que tienen la misma persona en el campo "asignado a".

Para asignar un usuario a un único archivo:

Pasos

1. En el panel resultados de la investigación de datos, haga clic en **▼** para que el archivo expanda los detalles de metadatos del archivo.
2. Haga clic en el campo **asignado a** y seleccione el nombre de usuario.



El nombre de usuario aparece en los metadatos del archivo.

Para asignar un usuario a varios archivos:

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea asignar a un usuario.

2345 items

 Tags

 Assign to

 Label

 Copy

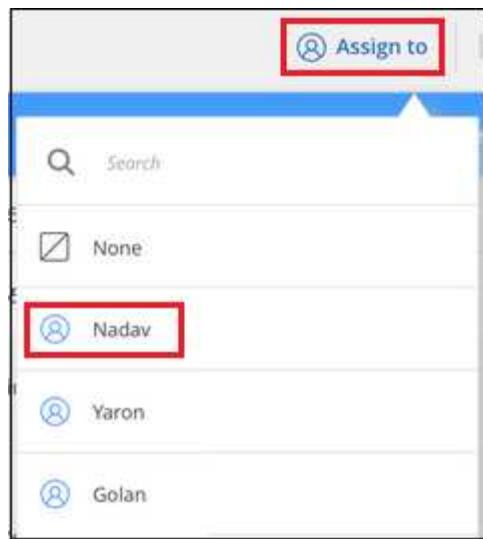
 Move

 Delete

<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼

- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).

2. En la barra de botones, haga clic en **asignar a** y seleccione el nombre de usuario:



El usuario se agrega a los metadatos de todos los archivos seleccionados.

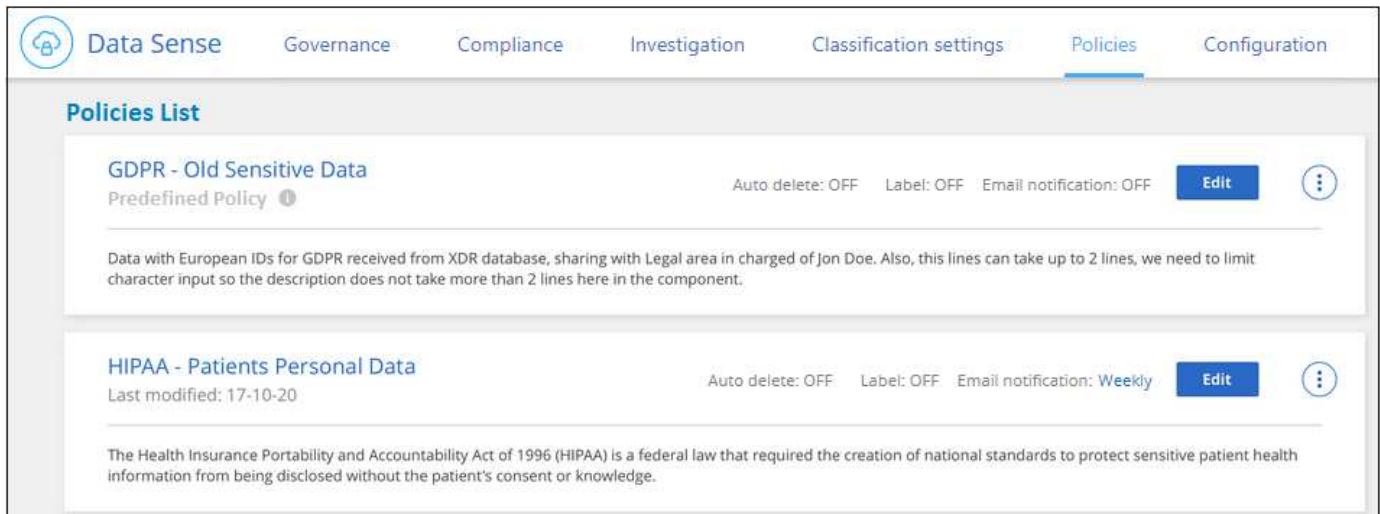
Asignación de políticas a sus datos

Las directivas son como una lista de favoritos de filtros personalizados que proporcionan resultados de búsqueda en la página de investigación para consultas de cumplimiento solicitadas con frecuencia. Cloud Data Sense proporciona un conjunto de políticas predefinidas basadas en las solicitudes comunes del cliente. Puede crear directivas personalizadas que proporcionen resultados para búsquedas específicas de su organización.

Las políticas ofrecen la siguiente funcionalidad:


- [Directivas predefinidas](#) Desde NetApp según solicitudes de usuarios
- Capacidad de crear sus propias políticas personalizadas
- Inicie la página de investigación con los resultados de las políticas con un solo clic
- Envíe alertas por correo electrónico a los usuarios de BlueXP o a cualquier otra dirección de correo electrónico cuando determinadas políticas críticas devuelvan resultados para que pueda obtener notificaciones que protejan sus datos
- Asigne etiquetas AIP (Protección de información de Azure) automáticamente a todos los archivos que coincidan con los criterios definidos en una directiva
- Elimine archivos automáticamente (una vez al día) cuando determinadas directivas devuelvan resultados para que pueda proteger sus datos automáticamente

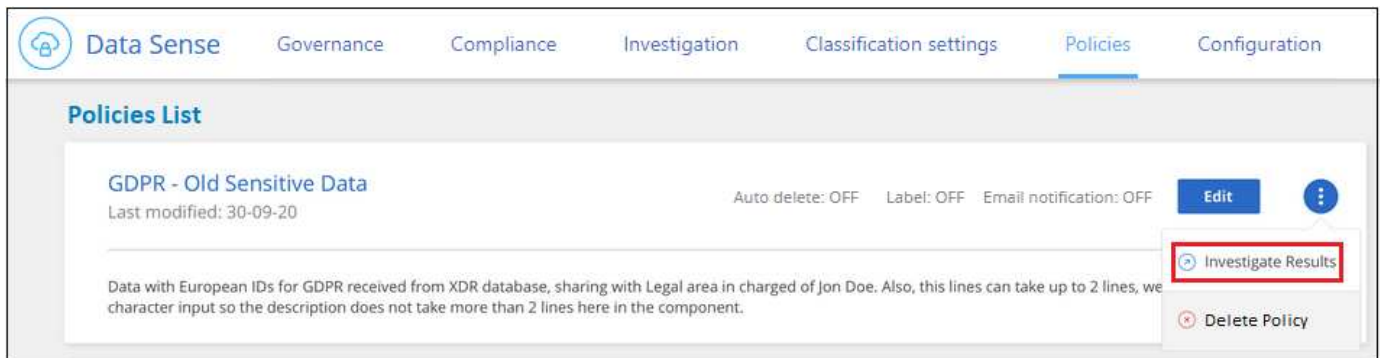
En la ficha **Directivas** del Panel de cumplimiento se enumeran todas las directivas predefinidas y personalizadas disponibles en esta instancia de Cloud Data Sense.



Además, las políticas aparecen en la lista de filtros de la página Investigación.

Ver los resultados de la directiva en la página Investigación

Para mostrar los resultados de una directiva en la página Investigación, haga clic en  Para una política específica y, a continuación, seleccione **investigar resultados**.



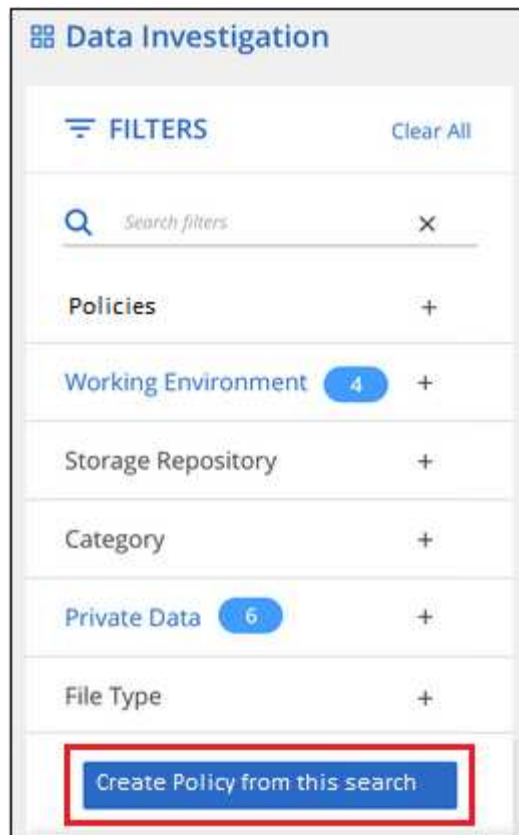
Creación de directivas personalizadas

Puede crear sus propias directivas personalizadas que proporcionen resultados para búsquedas específicas de su organización. Los resultados se devuelven para todos los archivos y directorios (recursos compartidos y carpetas) que coincidan con los criterios de búsqueda.

Tenga en cuenta que las acciones para eliminar datos y asignar etiquetas AIP basadas en los resultados de la directiva sólo son válidas para archivos. Los directorios que coinciden con los criterios de búsqueda no se pueden eliminar automáticamente ni asignar etiquetas AIP.

Pasos

1. En la página Investigación de datos, defina la búsqueda seleccionando todos los filtros que desee utilizar. Consulte ["Filtrar datos en la página Investigación de datos"](#) para obtener más detalles.
2. Una vez que tenga todas las características de filtro de la forma que desee, haga clic en **Crear directiva de esta búsqueda**.



3. Asigne un nombre a la directiva y seleccione otras acciones que ésta pueda realizar:
 - a. Introduzca un nombre y una descripción únicos.
 - b. Opcionalmente, marque la casilla para eliminar automáticamente los archivos que coincidan con los parámetros de directiva. Más información acerca de [eliminación de archivos de origen mediante una directiva](#).
 - c. Opcionalmente, marque la casilla si desea que se envíen correos electrónicos de notificación a usuarios de BlueXP en su cuenta y elija el intervalo en el que se envía el correo electrónico. Más información acerca de [envío de alertas por correo electrónico basadas en los resultados de la política](#).
 - d. Opcionalmente, marque la casilla si desea enviar correos electrónicos de notificación a otros usuarios, introduzca hasta 20 direcciones de correo electrónico y elija el intervalo en el que se envía el correo electrónico.
 - e. Opcionalmente, active la casilla para asignar automáticamente etiquetas AIP a archivos que coincidan con los parámetros de directiva y seleccione la etiqueta. (Sólo si ya tiene etiquetas AIP integradas. Más información acerca de ["Etiquetas AIP"](#).)
 - f. Haga clic en **Crear directiva**.

Create Policy

This will create a new Policy according to the current selected filters and search term. You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

Files with personal data created over 60 days ago

Give it a detailed description that explains what it searches for

See if any old files with personal data should be moved or deleted

☐ Automatically delete files that match this policy (Every Day)

Email updates about this Policy:

☒ Email all the users in this account Every Day

☐ Send Email Every Day to:

Label:

☐ Automatically label this Policy's matches with: New Personal

[Cancel](#) [Create Policy](#)

Resultado

La nueva directiva aparece en la ficha Directivas.

Envío de alertas por correo electrónico cuando se encuentran datos no conformes

Cloud Data Sense puede enviar alertas por correo electrónico a los usuarios de BlueXP en su cuenta cuando ciertas políticas críticas devuelven resultados para que pueda obtener notificaciones para proteger sus datos. Puede optar por enviar las notificaciones por correo electrónico diariamente, semanalmente o mensualmente. También puede optar por enviar alertas de correo electrónico a cualquier otra dirección de correo electrónico - hasta 20 direcciones de correo electrónico - no en su cuenta de BlueXP.

Puede configurar esta configuración al crear la directiva o al editar cualquier directiva.

Siga estos pasos para agregar actualizaciones de correo electrónico a una directiva existente.

Pasos

1. En la página Lista de directivas, haga clic en **Editar** para la directiva en la que desea agregar (o cambiar) la configuración de correo electrónico.

Data Sense Governance Compliance Investigation Classification settings **Policies** Configuration

Policies List

GDPR - Old Sensitive Data
Predefined Policy ⓘ

Label: General | E-mail notifications: Monthly Edit ⓘ

Data with European IDs for GDPR received from XDR database, sharing with Legal area in charged of Jon Doe. Also, this lines can take up to 2 lines, we need to limit character input so the description does not take more than 2 lines here in the component.

HIPAA - Patients Personal Data
Last modified: 17-10-20

Label: OFF | E-mail notifications: OFF Edit ⓘ

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

2. En la página Edit Policy:

- Marque la casilla "Enviar por correo electrónico a todos los usuarios de esta cuenta" si desea enviar correos electrónicos de notificación a los usuarios de su cuenta de BlueXP y elija el intervalo en el que se envía el correo electrónico (por ejemplo, **todos los días**).
- Marque la casilla "Enviar correo electrónico" si desea enviar correos electrónicos de notificación a usuarios adicionales, seleccione el intervalo en el que se envía el correo electrónico e introduzca hasta 20 direcciones de correo electrónico.

Edit Policy

Saving this filtered view will create a new Policy, you can view/edit it in the "Policy" tab

Name this Policy

HIPAA - Patient Personal Data

Give it a description to quickly identify it

Files containing patient health information that is more than 30 days old

☐ Automatically delete files that match this policy (Every Day)

Email updates about this Policy:

☒ Email all the users in this account Every Day ▾

☒ Send Email Every Day ▾ to: email@gmail.com ✕ +2 ✕

Label:

☐ Automatically label this Policy's matches with: New Personal ▾

Cancel Save Policy

- Haga clic en **Guardar directiva** y el intervalo en el que se envía el correo electrónico aparecerá en la

descripción de la directiva.

Resultado

El primer correo electrónico se envía ahora si hay algún resultado de la Política, pero sólo si alguno de los archivos cumple los criterios de la Política. No se envía información personal en los correos electrónicos de notificación. El correo electrónico indica que hay archivos que coinciden con los criterios de directiva y proporciona un vínculo a los resultados de la directiva.

Eliminación automática de archivos de origen mediante directivas

Puede crear una directiva personalizada para eliminar los archivos que coincidan con la directiva. Por ejemplo, puede que desee eliminar archivos que contengan información confidencial y que fueron detectados por Data Sense en los últimos 30 días.

Sólo los administradores de cuentas pueden crear una directiva para eliminar archivos automáticamente.



Todos los archivos que coincidan con la directiva se eliminarán de forma permanente una vez al día.

Pasos

1. En la página Investigación de datos, defina la búsqueda seleccionando todos los filtros que desee utilizar. Consulte ["Filtrar datos en la página Investigación de datos"](#) para obtener más detalles.
2. Una vez que tenga todas las características de filtro de la forma que desee, haga clic en **Crear directiva de esta búsqueda**.
3. Asigne un nombre a la directiva y seleccione otras acciones que ésta pueda realizar:
 - a. Introduzca un nombre y una descripción únicos.
 - b. Active la casilla para "eliminar automáticamente los archivos que coinciden con esta directiva" y escriba **eliminar permanentemente** para confirmar que desea que los archivos se eliminen de forma permanente mediante esta directiva.
 - c. Haga clic en **Crear directiva**.

Create Policy

This will create a new Policy according to the current selected filters and search term. You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

Delete files with sensitive data

Give it a detailed description that explains what it searches for

Delete files that contain sensitive information and that were discovered in the past 30 days

☒ Automatically delete files that match this policy (Every Day)

Type *"permanently delete"* to continue with the deletion.

permanently delete

☐ Send email updates about this Policy to Cloud Manager users on this account every Day

☐ Automatically label this Policy's matches with: Select a label

Create Policy

Cancel

Resultado

La nueva directiva aparece en la ficha Directivas. Los archivos que coinciden con la directiva se eliminan una vez al día cuando se ejecuta la directiva.

Puede ver la lista de archivos que se han eliminado en ["Panel Estado de acciones"](#).

Asignación automática de etiquetas AIP con directivas

Puede asignar una etiqueta AIP a todos los archivos que cumplan los criterios de la directiva. Puede especificar la etiqueta AIP al crear la directiva, o puede agregar la etiqueta al editar cualquier directiva.

Las etiquetas se agregan o actualizan continuamente en archivos a medida que Cloud Data Sense analiza los archivos.

En función de si una etiqueta ya se ha aplicado a un archivo y del nivel de clasificación de la etiqueta, se realizan las siguientes acciones al cambiar una etiqueta:

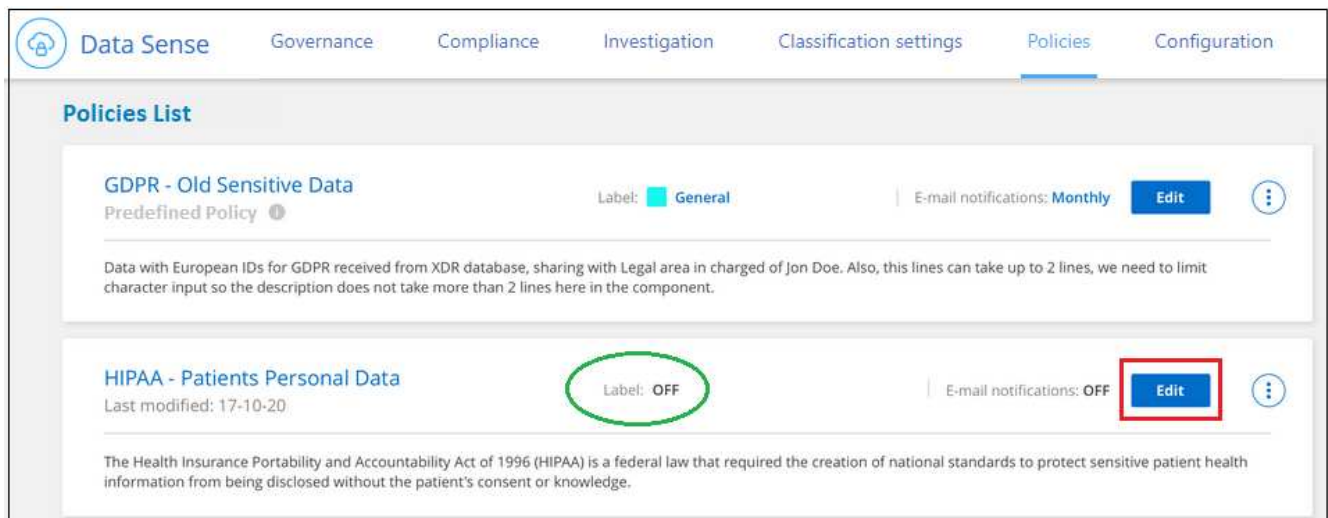
Si el archivo...	Realice lo siguiente...
No tiene etiqueta	Se agrega la etiqueta
Tiene una etiqueta de un nivel inferior de clasificación	Se agrega la etiqueta de nivel superior

Si el archivo...	Realice lo siguiente...
Tiene una etiqueta existente de un nivel superior de clasificación	Se mantiene la etiqueta de nivel superior
Se asigna una etiqueta tanto manualmente como por una directiva	Se agrega la etiqueta de nivel superior
Se asignan dos etiquetas diferentes mediante dos directivas	Se agrega la etiqueta de nivel superior

Siga estos pasos para agregar una etiqueta AIP a una directiva existente.

Pasos

1. En la página Lista de directivas, haga clic en **Editar** para la directiva en la que desea agregar (o cambiar) la etiqueta AIP.



2. En la página Editar directiva, active la casilla para habilitar etiquetas automáticas para los archivos que coincidan con los parámetros de directiva y seleccione la etiqueta (por ejemplo, **General**).

3. Haga clic en **Guardar directiva** y la etiqueta aparecerá en la descripción de la directiva.



Si se ha configurado una directiva con una etiqueta, pero la etiqueta se ha eliminado de AIP, el nombre de la etiqueta se desactiva y la etiqueta ya no se asigna.

Edición de directivas

Puede modificar cualquier criterio para una política existente que haya creado previamente. Esto puede resultar especialmente útil si desea cambiar la consulta (los elementos definidos mediante Filtros) para agregar o quitar determinados parámetros.

Tenga en cuenta que para directivas predefinidas, sólo puede modificar si se envían notificaciones de correo electrónico y si se agregan etiquetas AIP. No se pueden cambiar otros valores.

Pasos

1. En la página Lista de directivas, haga clic en **Editar** para la directiva que desea cambiar.

2. Si sólo desea cambiar los elementos de esta página (Nombre, Descripción, si se envían notificaciones de correo electrónico y si se agregan etiquetas AIP), realice el cambio y haga clic en **Guardar directiva**.

Si desea cambiar los filtros de la consulta guardada, haga clic en **Editar consulta**.

Edit Policy

Edit Query

Name this Policy

Personal from SMB share (DB)

Give it a detailed description that explains what it searches for

Find any files containing personal data on our SMB share

☐ Automatically delete files that match this policy (Every Day)

Email updates about this Policy:

☐ Email all the users in this account

Every Day

☐ Send Email

Every Day

 to:

Label:

☐ Automatically label this Policy's matches with:

Cancel

Save Policy

- En la página Investigación que define esa consulta, edite la consulta agregando, quitando o personalizando los filtros y haga clic en **Guardar cambios**.

Data Investigation

Unstructured (16 Files)

Directories (0 Folders)

Structured (0 Tables)

Search by File, Table or loca

FILTERS:

Clear All

Policies 1

Open Permissions

User / Group Permissions

File Owner

Label

Working Environment Type

Working Environment

Save Changes

Cancel Edit Query

16 items

Tags

Assign to

Label

Move

Copy

Delete

<div><div></div></div> File Name	Personal	Sensitive Personal	Data Subjects	File Type	
<div><div></div></div> cifs2.json	SHARES	1	0	0	JSON
<div><div></div></div> cifs12.json	SHARES	1	0	0	JSON
<div><div></div></div> TableTextServiceYi.txt	SHARES	1	0	0	TXT
<div><div></div></div> testpass.json	SHARES	1	0	0	JSON
<div><div></div></div> urlp.txt	SHARES	1	0	0	TXT
<div><div></div></div> License.sharpen.txt	SHARES	1	0	1	TXT
<div><div></div></div> TableTextServiceYi.txt	SHARES	1	0	0	TXT
<div><div></div></div> Notice.txt	SHARES	1	0	0	TXT
<div><div></div></div> urlp.txt	SHARES	1	0	0	TXT
<div><div></div></div> Notice.txt	SHARES	1	0	0	TXT


1-16 of 16

Resultado

La directiva cambia inmediatamente. Cualquier acción definida para que esa directiva envíe un correo electrónico, agregue etiquetas AIP o elimine archivos tendrá lugar en el siguiente interno.

Eliminar directivas

Puede eliminar cualquier directiva personalizada que haya creado si ya no la necesita. No se puede eliminar ninguna de las directivas predefinidas.

Para eliminar una directiva, haga clic en  Para una directiva específica, haga clic en **Eliminar directiva** y, a continuación, vuelva a hacer clic en **Eliminar directiva** en el cuadro de diálogo de confirmación.

Lista de directivas predefinidas

Cloud Data Sense proporciona las siguientes políticas definidas por el sistema:

Nombre	Descripción	Lógica
S3: Datos privados expuestos públicamente	S3 objetos que contienen información personal o confidencial, con acceso público de lectura abierto.	S3 Public y contiene información personal o confidencial
PCI DSS: Datos obsoletos durante 30 días	Archivos con información de tarjeta de crédito, modificado por última vez hace 30 días.	Contiene tarjeta de crédito y última modificación durante 30 días
HIPAA: Datos desfasados a lo largo de 30 días	Archivos que contienen información médica, modificada por última vez hace 30 días.	Contiene datos de salud (definidos de la misma forma que en el informe HIPAA) Y última modificación durante 30 días
Datos privados: Obsoletos a lo largo de 7 años	Archivos que contengan información personal o confidencial, modificado por última vez hace más de 7 años.	Archivos que contengan información personal o confidencial, modificado por última vez hace más de 7 años
RGPD: Ciudadanos europeos	Archivos que contienen más de 5 identificadores de ciudadanos de un país de la UE o tablas de DB que contienen identificadores de ciudadanos de un país de la UE.	Archivos que contienen más de 5 identificadores de una (una) tablas de ciudadanos o bases de datos de la UE que contienen filas con más del 15% de columnas con identificadores de la UE de un país. (Cualquiera de los identificadores nacionales de los países europeos. No incluye Brasil, California, Estados Unidos SSN, Israel, Sudáfrica)
CCPA - residentes de California	Archivos que contienen más de 10 identificadores de licencia de controlador de California o tablas de base de datos con este identificador.	Archivos que contienen más de 10 identificadores de Licencia de controlador de California O tablas de base de datos que contienen la licencia de controlador de California
Nombres de sujetos de datos: Alto riesgo	Archivos con más de 50 nombres de asunto de datos.	Archivos con más de 50 nombres de asunto de datos

Nombre	Descripción	Lógica
Direcciones de correo electrónico: Alto riesgo	Archivos con más de 50 direcciones de correo electrónico o columnas de base de datos con más del 50% de sus filas que contienen direcciones de correo electrónico	Archivos con más de 50 direcciones de correo electrónico o columnas de base de datos con más del 50% de sus filas que contienen direcciones de correo electrónico
Datos personales: Alto riesgo	Archivos con más de 20 identificadores de datos personales o columnas de base de datos con más del 50% de sus filas que contienen identificadores de datos personales.	Archivos con más de 20 columnas personales o de base de datos con más del 50% de sus filas que contienen personales
Datos personales confidenciales: Alto riesgo	Archivos con más de 20 identificadores de datos personales confidenciales, o columnas de base de datos con más del 50% de sus filas que contienen datos personales confidenciales.	Archivos con más de 20 columnas confidenciales personales o de base de datos con más del 50% de sus filas que contienen personal confidencial

Gestione sus datos privados

Cloud Data Sense ofrece varias formas de gestionar sus datos privados. Algunas funcionalidades facilitan la preparación para la migración de datos, mientras que otras permiten realizar cambios en los datos.

- Puede copiar archivos en un recurso compartido NFS de destino si desea realizar una copia de determinados datos y moverlos a una ubicación NFS diferente.
- Es posible clonar un volumen de ONTAP en un volumen nuevo, e incluir solo los archivos seleccionados del volumen de origen en el nuevo volumen clonado. Esto resulta útil en situaciones en las que se migran datos y se desean excluir determinados archivos del volumen original.
- Puede copiar y sincronizar archivos de un repositorio de origen a un directorio en una ubicación de destino específica. Esto resulta útil en situaciones en las que se migran datos de un sistema de origen a otro mientras todavía hay alguna actividad final en los archivos de origen.
- Puede mover los archivos de origen que Data Sense esté analizando a cualquier recurso compartido de NFS.
- Puede eliminar archivos que parecen poco seguros o demasiado arriesgados para dejar en el sistema de almacenamiento, o que ha identificado como duplicados.



- Las capacidades descritas en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación no muestran detalles de nivel de archivo.
- Los datos de cuentas de Google Drive no pueden usar ninguna de estas funcionalidades en este momento.

Copiando archivos de origen

Puede copiar cualquier archivo de origen que Data Sense esté analizando. Existen tres tipos de operaciones de copia en función de lo que intente lograr:

- **Copiar archivos** de los mismos volúmenes o orígenes de datos o diferentes a un recurso compartido NFS de destino.

Esto resulta útil si se desea realizar una copia de ciertos datos y moverlos a una ubicación NFS diferente.

- **Clonar un volumen ONTAP** en un volumen nuevo del mismo agregado, pero incluir sólo los archivos seleccionados del volumen de origen en el nuevo volumen clonado.

Esto resulta útil en situaciones en las que se migran datos y se desean excluir determinados archivos del volumen original. Esta acción utiliza ["FlexClone de NetApp"](#) funcionalidad para duplicar rápidamente el volumen y, a continuación, eliminar los archivos que **no** seleccionó.

- **Copiar y sincronizar archivos** desde un único repositorio de origen (volumen ONTAP, bloque S3, recurso compartido NFS, etc.) a un directorio en una ubicación de destino específica.

Esto resulta útil en situaciones en las que se migran datos de un sistema de origen a otro. Después de la copia inicial, el servicio sincroniza los datos modificados con la programación que se haya establecido. Esta acción utiliza ["Cloud Sync de NetApp"](#) funcionalidad para copiar y sincronizar datos de un origen en un destino.

Copiando archivos de origen a un recurso compartido NFS

Puede copiar archivos de origen que Data Sense esté analizando en cualquier recurso compartido de NFS. El recurso compartido NFS no necesita integrarse con Data Sense, simplemente necesita saber el nombre del recurso compartido NFS donde se copiarán todos los archivos seleccionados en el formato `<host_name>:/<share_path>`.



No se pueden copiar archivos que residen en bases de datos.

Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para copiar archivos.
- La copia de archivos requiere que el recurso compartido NFS de destino permita el acceso desde la instancia de Data Sense.
- Puede copiar un máximo de 100,000 archivos al mismo tiempo.

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea copiar y haga clic en **Copiar**.



- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).
- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (☒ File Name) y, a continuación, en el mensaje emergente **All 20 Items on this page selected Select all Items in list (63K Items)**, Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

2. En el cuadro de diálogo *Copy Files*, seleccione la ficha **copia normal**.

3. Introduzca el nombre del recurso compartido NFS donde se copiarán todos los archivos seleccionados en el formato `<host_name>:/<share_path>` y haga clic en **Copiar**.

Se muestra un cuadro de diálogo con el estado de la operación de copia.

Puede ver el progreso de la operación de copia en "[Panel Estado de acciones](#)".

Tenga en cuenta que también puede copiar un archivo individual al ver los detalles de metadatos de un archivo. Haga clic en **Copiar archivo**.

Clonar datos de volumen en un volumen nuevo

Puede clonar un volumen de ONTAP existente que detección de datos está analizando con la funcionalidad *FlexClone* de NetApp. Esto le permite duplicar rápidamente el volumen e incluir únicamente los archivos seleccionados. Esto resulta útil si va a migrar datos y desea excluir determinados archivos del volumen

original o si desea crear una copia de un volumen para realizar las pruebas.

El nuevo volumen se creará en el mismo agregado que el volumen de origen. Asegúrese de tener suficiente espacio para este nuevo volumen en el agregado antes de iniciar esta tarea. Si es necesario, póngase en contacto con el administrador de almacenamiento.

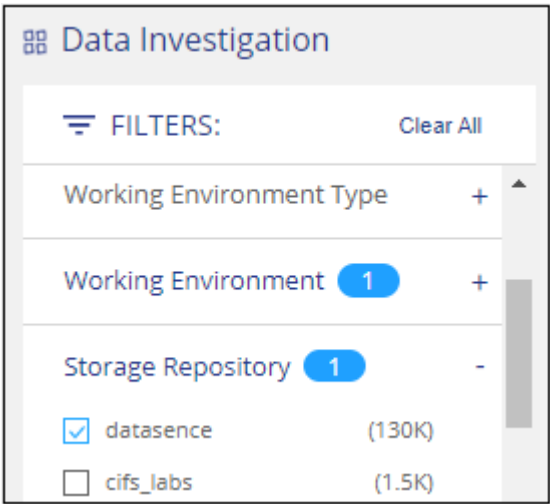
Nota: los volúmenes FlexGroup no se pueden clonar porque FlexClone no los admite.

Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para copiar archivos.
- Todos los archivos seleccionados deben ser del mismo volumen y el volumen debe estar en línea.
- El volumen debe ser de un sistema ONTAP Cloud Volumes ONTAP o en las instalaciones. Actualmente no se admiten otros orígenes de datos.
- Debe instalar la licencia de FlexClone en el clúster. Esta licencia se instala de manera predeterminada en sistemas Cloud Volumes ONTAP.

Pasos

1. En el panel Investigación de datos, cree un filtro seleccionando un solo **entorno de trabajo** y un único **repositorio de almacenamiento** para asegurarse de que todos los archivos pertenecen al mismo volumen ONTAP.



Aplique otros filtros para ver solo los archivos que desea clonar en el nuevo volumen.

2. En el panel resultados de la investigación, seleccione los archivos que desea clonar y haga clic en **Copiar**.



- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).
- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (☒ File Name) y, a continuación, en el mensaje emergente **All 20 Items on this page selected Select all Items in list (63K Items)**, Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

3. En el cuadro de diálogo *Copy Files*, seleccione la ficha **FlexClone**. Esta página muestra el número total de archivos que se clonarán desde el volumen (los archivos seleccionados) y el número de archivos que no se incluyen o eliminan (los archivos que no seleccionó) del volumen clonado.

4. Introduzca el nombre del nuevo volumen y haga clic en **FlexClone**.

Se muestra un cuadro de diálogo con el estado de la operación de clonado.

Resultado

El nuevo volumen clonado se crea en el mismo agregado que el volumen de origen.

Puede ver el progreso de la operación de clonado en el ["Panel Estado de acciones"](#).

Si seleccionó inicialmente **asignar todos los volúmenes** o **asignar y clasificar todos los volúmenes** cuando habilita detección de datos para el entorno de trabajo donde reside el volumen de origen, entonces detección de datos escaneará automáticamente el nuevo volumen clonado. Si inicialmente no ha utilizado ninguna de estas selecciones, si desea explorar este nuevo volumen, deberá hacerlo ["active la exploración en el volumen manualmente"](#).

Copiar y sincronizar archivos de origen en un sistema de destino

Puede copiar archivos de origen que Data Sense esté analizando desde cualquier origen de datos no estructurados admitido a un directorio en una ubicación de destino específica (["Ubicaciones de destino"](#)

compatibles con Cloud Sync"). Después de la copia inicial, los datos modificados en los archivos se sincronizan en función de la programación que configure.

Esto resulta útil en situaciones en las que se migran datos de un sistema de origen a otro. Esta acción utiliza "Cloud Sync de NetApp" funcionalidad para copiar y sincronizar datos de un origen en un destino.



No se pueden copiar y sincronizar archivos que residen en cuentas de SharePoint, cuentas de OneDrive o bases de datos.

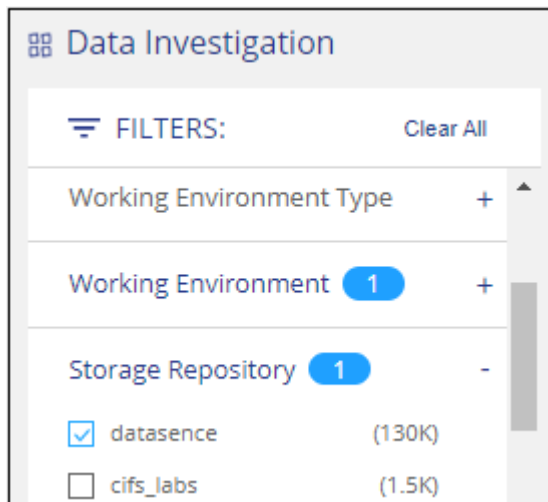
Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para copiar y sincronizar archivos.
- Todos los archivos seleccionados deben ser del mismo repositorio de origen (volumen ONTAP, bloque de S3, recurso compartido NFS o CIFS, etc.).
- Tendrá que activar el servicio Cloud Sync y configurar un mínimo de un agente de datos que se puede utilizar para transferir archivos entre los sistemas de origen y destino. Revise los requisitos de Cloud Sync que comienzan con "Descripción de Inicio rápido".

Tenga en cuenta que el servicio Cloud Sync tiene cargos por servicio independientes para sus relaciones de sincronización y incurrirá en cargos por recursos si implementa el agente de datos en el cloud.

Pasos

1. En el panel Investigación de datos, cree un filtro seleccionando un solo **entorno de trabajo** y un único **repositorio de almacenamiento** para asegurarse de que todos los archivos están del mismo repositorio.



Aplique cualquier otro filtro para que sólo vea los archivos que desea copiar y sincronizar con el sistema de destino.

2. En el panel resultados de la investigación, seleccione todos los archivos de todas las páginas marcando la casilla de la fila de título (☒ **File Name**), luego en el mensaje emergente **All 20 Items on this page selected** [Select all Items in list \(63K Items\)](#) Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)** y, a continuación, haga clic en **Copiar**.

126.3K items | 20 selected

Tags | Assign to | Label | Move | Copy | Delete

☒ File Name 1

Personal | Sensitive Personal | Data Subjects | File Type

All 20 Items on this page selected Select all Items in list (126.3K Items) 2

	File Name	CVO	652	0	1	TXT	
<input checked="" type="checkbox"/>	CRM_Customers.txt	CVO	652	0	1	TXT	▼
<input checked="" type="checkbox"/>	truepositive.txt	CVO	0	61	11	TXT	▼
<input checked="" type="checkbox"/>	test_file.txt	CVO	6	611	111	TXT	▼
<input checked="" type="checkbox"/>	test_positive.txt	CVO	0	65	51	TXT	▼

3. En el cuadro de diálogo *Copy Files*, seleccione la ficha **Sync**.

Regular Copy | FlexClone | **Sync**

An easy to use replication service for transferring data between any file or object store, on prem or in the cloud.

[Learn More](#)

32K items will be synced using Cloud Sync.

Source ↔ Target

Data Sense

Data Broker

OK Cancel

4. Si está seguro de que desea sincronizar los archivos seleccionados con una ubicación de destino, haga clic en **Aceptar**.

La interfaz de usuario de Cloud Sync se abre en BlueXP.

Se le solicitará que defina la relación de sincronización. El sistema de origen se rellena previamente en función del repositorio y los archivos que ya haya seleccionado en detección de datos.

5. Deberá seleccionar el sistema de destino y, a continuación, seleccionar (o crear) el agente de datos que desea utilizar. Revise los requisitos de Cloud Sync que comienzan con "[Descripción de Inicio rápido](#)".

Resultado

Los archivos se copian en el sistema de destino y se sincronizarán según la programación que defina. Si selecciona una sincronización única, los archivos se copiarán y sincronizarán una vez. Si elige una sincronización periódica, los archivos se sincronizan según la programación. Tenga en cuenta que si el sistema de origen agrega nuevos archivos que coinciden con la consulta creada mediante filtros, esos

archivos *new* se copiarán en el destino y se sincronizarán en el futuro.

Tenga en cuenta que algunas de las operaciones habituales de Cloud Sync están deshabilitadas cuando se invoca desde Data Sense:

- No puede utilizar los botones **Eliminar archivos en origen** o **Eliminar archivos en destino**.
- La ejecución de un informe está deshabilitada.

Mover archivos de origen a un recurso compartido NFS

Puede mover los archivos de origen que Data Sense esté analizando a cualquier recurso compartido de NFS. El recurso compartido de NFS no necesita estar integrado con Data Sense (consulte "[Analizando recursos compartidos de archivos](#)").

De manera opcional, puede dejar un archivo de rastro en la ubicación del archivo movido. Un archivo de rastro ayuda a los usuarios a comprender por qué se trasladó un archivo desde su ubicación original. Para cada archivo movido, el sistema crea un archivo de rastro en la ubicación de origen llamada <filename>-breadcrumb-<date>.txt. Puede añadir texto al cuadro de diálogo que se añadirá al archivo de rastro para indicar la ubicación donde se trasladó el archivo y el usuario que trasladó el archivo.

Si existe un archivo con el mismo nombre en la ubicación de destino, el archivo no se moverá.



No se pueden mover los archivos que residen en las bases de datos.

Requisitos

- Debe tener el rol Administrador de cuentas o Administrador de área de trabajo para mover archivos.
- Los archivos de origen se pueden ubicar en los siguientes orígenes de datos: ONTAP en las instalaciones, Cloud Volumes ONTAP, Azure NetApp Files, recursos compartidos de archivos y SharePoint Online.
- Mover archivos requiere que el recurso compartido NFS permita el acceso desde la dirección IP de la instancia de Data Sense.
- Puede mover un máximo de 15 millones de archivos al mismo tiempo.

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desee mover.


2345 items							Tags	Assign to	Label	Copy	Move	Delete
<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						

- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).

- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título

(☒ **File Name**) y, a continuación, en el mensaje emergente **All 20 Items on this page selected Select all Items in list (63K Items)**, Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

2. En la barra de botones, haga clic en **mover**.

 **Move Files (63)**

The files will be moved to the destination folder you provide and will no longer be available at their current location.


Moving files is supported only to destination folders in NFS Shares. Any NFS Share is supported, no matter where it is hosted, as long as the share's export policy allows access from the data connector instance IP address.

The status of this action will appear in the Action Status.

Enter the NFS destination folder path to continue

☒ **Leave breadcrumb**

A breadcrumb file helps your users understand why a file was moved from its original location. For each moved file, the system creates a breadcrumb file in the source location named **<filename>-breadcrumb-<date>.txt**.

 **Max length should be maximum 400 characters**

Move Files

Cancel

3. En el cuadro de diálogo *Move Files*, escriba el nombre del recurso compartido NFS donde se moverán todos los archivos seleccionados en el formato **<host_name>:/<share_path>**.
4. Si desea dejar un archivo de rastro, marque la casilla *Leave breadcrumb*. Puede escribir texto en el cuadro de diálogo para indicar la ubicación en la que se ha movido el archivo y el usuario que lo ha movido, así como cualquier otra información, como el motivo por el que se ha movido el archivo.
5. Haga clic en **mover archivos**.

Tenga en cuenta que también puede mover un archivo individual al ver los detalles de los metadatos de un archivo. Simplemente haga clic en **mover archivo**.



Eliminando archivos de origen

Puede eliminar de forma permanente los archivos de origen que parezcan poco seguros o demasiado arriesgados para dejar su sistema de almacenamiento, o que haya identificado como duplicados. Esta acción es permanente y no hay deshacer ni restaurar.

Puede eliminar archivos manualmente desde el panel Investigación, o. ["Uso automático de directivas"](#).



No se pueden eliminar los archivos que residen en las bases de datos.

Para eliminar archivos, es necesario contar con los siguientes permisos:

- Para datos NFS: La política de exportación debe definirse con permisos de escritura.
- Para datos CIFS: Las credenciales CIFS necesitan permisos de escritura.
- Para datos S3 - el rol IAM debe incluir el siguiente permiso: `s3:DeleteObject`.

Eliminación manual de archivos de origen

Requisitos

- Debe tener el rol de administrador de cuentas o administrador de área de trabajo para eliminar archivos.
- Puede eliminar un máximo de 100,000 archivos al mismo tiempo.

Pasos

1. En el panel resultados de la investigación de datos, seleccione el archivo o los archivos que desea eliminar.



- Para seleccionar archivos individuales, marque la casilla de cada archivo (☒ Volume_1).
- Para seleccionar todos los archivos de la página actual, active la casilla de la fila de título (☒ File Name).
- Para seleccionar todos los archivos de todas las páginas, active la casilla de la fila de título (☒ File Name) y, a continuación, en el mensaje emergente **All 20 items on this page selected Select all items in list (63K items)**, Haga clic en **Seleccionar todos los elementos de la lista (xxx elementos)**.

2. En la barra de botones, haga clic en **Eliminar**.

3. Debido a que la operación de eliminación es permanente, debe escribir "**permanentemente delete**" en el diálogo posterior *Delete File* y hacer clic en **Delete File**.

Puede ver el progreso de la operación de eliminación en la "[Panel Estado de acciones](#)".

Tenga en cuenta que también puede eliminar un archivo individual al ver los detalles de metadatos de un archivo. Simplemente haga clic en **Eliminar archivo**.



Ver informes de cumplimiento

Cloud Data Sense ofrece informes que puede usar para comprender mejor el estado del programa de privacidad de datos de su organización.

De forma predeterminada, los paneles Cloud Data Sense muestran datos de cumplimiento de normativas y gobierno de todos los entornos de trabajo, bases de datos y orígenes de datos. Si desea ver informes que contengan datos sólo para algunos de los entornos de trabajo, [seleccione esos entornos de trabajo](#).



- Los informes descritos en esta sección sólo están disponibles si ha elegido realizar un análisis de clasificación completo en sus orígenes de datos. Los orígenes de datos que han tenido un análisis de sólo asignación sólo pueden generar el informe de asignación de datos.
- NetApp no puede garantizar una precisión del 100 % de los datos personales y los datos personales confidenciales que identifique Cloud Data. Siempre debe validar la información revisando los datos.

Informe de evaluación del riesgo de privacidad

El informe de evaluación de riesgos de privacidad ofrece una descripción general del estado de riesgo de privacidad de su organización, tal y como lo exigen las normativas de privacidad como el RGPD y la CCPA. El informe incluye la siguiente información:

Estado de cumplimiento

A. [puntuación de gravedad](#) y la distribución de los datos, ya sean personales, confidenciales o no confidenciales.

Descripción general de la evaluación

Desglose de los tipos de datos personales encontrados, así como de las categorías de datos.

Datos sujetos en esta evaluación

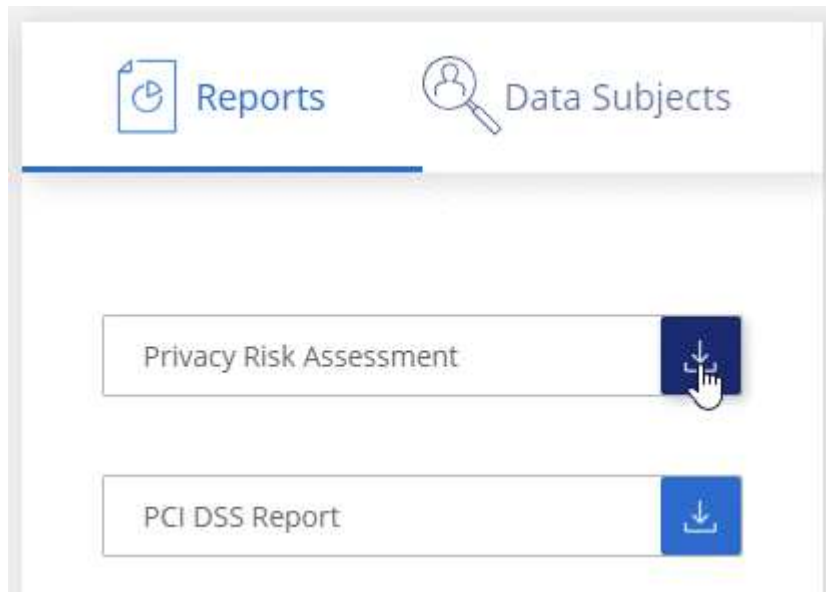
El número de personas, por ubicación, para las cuales se encontraron identificadores nacionales.

Generación del Informe de Evaluación de riesgo de Privacidad

Vaya a la ficha detección de datos para generar el informe.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **cumplimiento** y, a continuación, haga clic en el icono de descarga situado junto a **Evaluación de riesgo de privacidad** en **Informes**.



Resultado

Cloud Data Sense genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Puntuación de gravedad

Cloud Data Sense calcula la puntuación de gravedad del informe de evaluación del riesgo de privacidad basándose en tres variables:

- El porcentaje de datos personales de todos los datos.

- El porcentaje de datos personales confidenciales de todos los datos.
- El porcentaje de archivos que incluyen temas de datos, determinado por identificadores nacionales como ID nacionales, números de Seguro Social y números de identificación fiscal.

La lógica utilizada para determinar la puntuación es la siguiente:

Puntuación de gravedad	Lógica
0	Las tres variables son exactamente 0 %
1	Una de las variables es mayor que 0 %
2	Una de las variables es mayor que el 3 %
3	Dos de las variables son mayores que el 3%
4	Tres de las variables son mayores que el 3%
5	Una de las variables es mayor que el 6 %
6	Dos de las variables son mayores que el 6%
7	Tres de las variables son mayores que el 6%
8	Una de las variables es mayor que el 15 %
9	Dos de las variables son mayores que el 15%
10	Tres de las variables son mayores que el 15%

Informe PCI DSS

El Informe de estándares de seguridad de datos del sector de la tarjeta de pago (PCI DSS) puede ayudarle a identificar la distribución de información de la tarjeta de crédito a través de sus archivos. El informe incluye la siguiente información:

Descripción general

Cuántos archivos contienen información de tarjeta de crédito y en qué entornos de trabajo.

Cifrado

Porcentaje de archivos que contienen información de la tarjeta de crédito en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware

Porcentaje de archivos que contienen información de tarjetas de crédito en entornos de trabajo que tienen o no la protección contra ransomware habilitada. Esta información es específica de Cloud Volumes ONTAP.

Retención

El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de la tarjeta de crédito por más tiempo de lo que necesita para procesarla.

Distribución de la información de la tarjeta de crédito

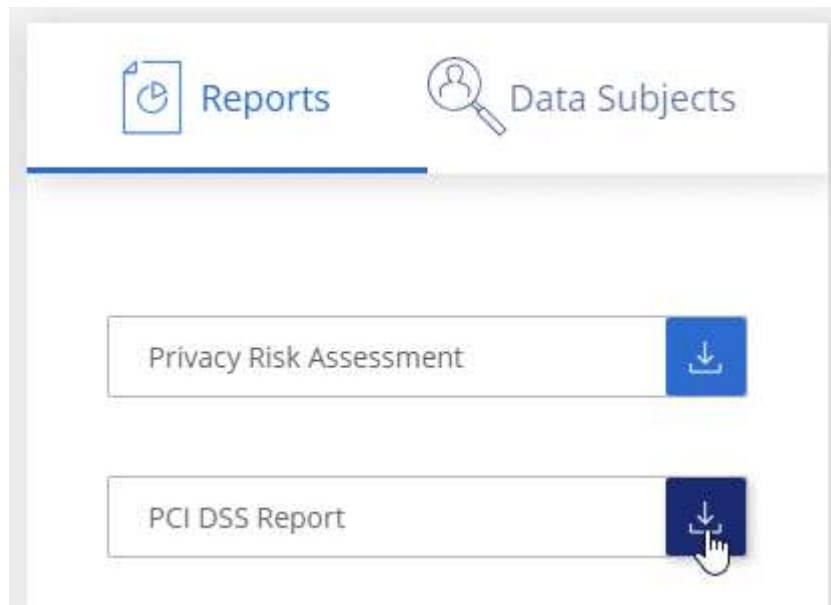
Entornos en los que se encontró la información de la tarjeta de crédito y si la protección mediante cifrado y ransomware están habilitadas.

Generación del informe PCI DSS

Vaya a la ficha detección de datos para generar el informe.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **conformidad** y, a continuación, haga clic en el icono de descarga situado junto a **Informe DSS de PCI** en **Informes**.



Resultado

Cloud Data Sense genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Informe HIPAA

El Informe de la Ley de Portabilidad y responsabilidad de los Seguros médicos (HIPAA) puede ayudarle a identificar archivos que contengan información médica. Se ha diseñado para ayudar en el requisito de su organización a cumplir las leyes de privacidad de datos HIPAA. El Cloud Data Sense de información incluye:

- Patrón de referencia de salud
- Código médico ICD-10-cm
- Código médico ICD-9-cm
- HR - Categoría de salud
- Datos de aplicación de Salud

El informe incluye la siguiente información:

Descripción general

Cuántos archivos contienen información médica y en qué entornos de trabajo.

Cifrado

Porcentaje de archivos que contienen información médica en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware

Porcentaje de archivos que contienen información médica en entornos de trabajo que tienen o no la protección contra ransomware activada. Esta información es específica de Cloud Volumes ONTAP.

Retención

El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de salud por más tiempo de lo que necesita para procesarla.

Distribución de la información de salud

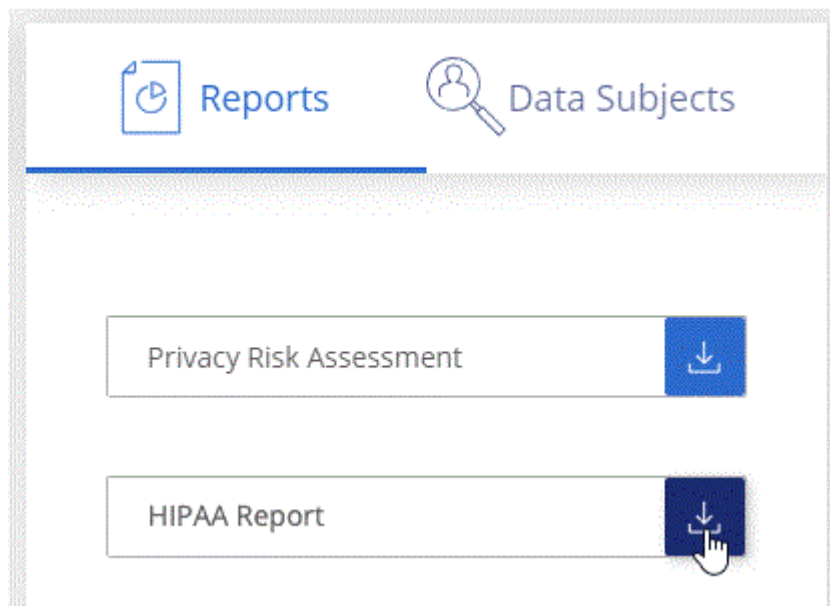
Entornos en los que se encontró la información médica y si está habilitada el cifrado y la protección contra ransomware.

Generación del informe HIPAA

Vaya a la ficha detección de datos para generar el informe.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **cumplimiento** y, a continuación, haga clic en el icono de descarga situado junto a **Informe HIPAA** en **Informes**.



Resultado

Cloud Data Sense genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

¿Qué es una solicitud de acceso de asunto de datos?

Las normas de privacidad, como el GDPR europeo, otorgan a sujetos de datos (como clientes o empleados) el derecho a acceder a sus datos personales. Cuando un sujeto de datos solicita esta información, se le conoce como DSAR (solicitud de acceso a sujetos de datos). Las organizaciones deben responder a estas solicitudes "sin demora indebida" y, a más tardar, en el plazo de un mes a partir de su recepción.

Puede responder a un DSAR buscando el nombre completo o el identificador conocido de un sujeto (como una dirección de correo electrónico) y, a continuación, descargando un informe. El informe está diseñado para ayudar en el requisito de su organización a cumplir con el RGPD o con leyes de privacidad de datos similares.

¿Cómo puede ayudarle Cloud Data Sense a responder a un DSAR?

Cuando se realiza una búsqueda de asunto de datos, Cloud Data Sense encuentra en ella todos los archivos, bloques, OneDrive y cuentas de SharePoint que tienen el nombre o el identificador de esa persona. Data Sense comprueba el nombre o identificador de los datos preindexados más recientes. No inicia una nueva exploración.

Una vez finalizada la búsqueda, puede descargar la lista de archivos para un informe de solicitud de acceso a un sujeto de datos. El informe agrega información procedente de los datos y los coloca en términos legales de los que se puede enviar a la persona.



La búsqueda de sujetos de datos no es compatible en las bases de datos en este momento.

Búsqueda de sujetos de datos y descarga de informes

Busque el nombre completo o el identificador conocido del sujeto de datos y, a continuación, descargue un informe de la lista de archivos o un informe DSAR. Puede buscar por "[cualquier tipo de información personal](#)".

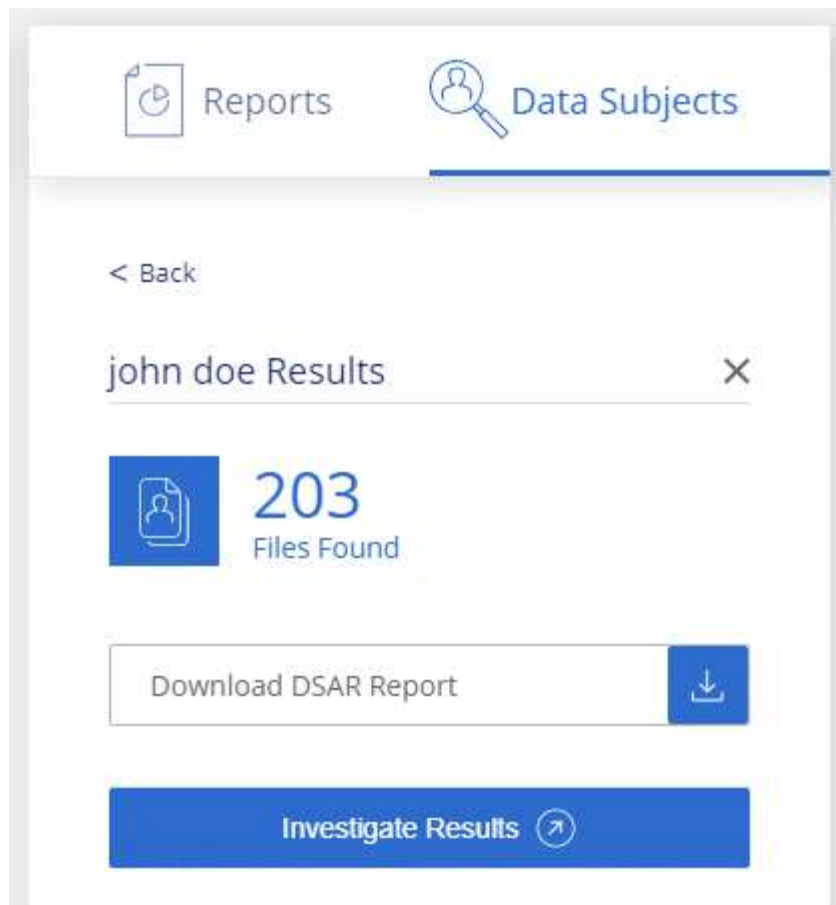


Se admiten el inglés, el alemán y el español cuando se buscan los nombres de los temas de datos. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En el menú BlueXP, haga clic en **Gobierno > Clasificación**.
2. Haga clic en **Temas de datos**.
3. Busque el nombre completo o el identificador conocido del sujeto de datos.

A continuación se muestra un ejemplo que muestra una búsqueda del nombre *john doe*:



4. Elija una de las opciones disponibles:

- **Descargar informe DSAR:** Respuesta formal a la solicitud de acceso que se puede enviar al sujeto de datos. Este informe contiene información generada automáticamente en función de los datos de que Cloud Data Sense se encuentra en el asunto de los datos y está diseñado para su uso como plantilla. Debe completar el formulario y revisarlo internamente antes de enviarlo al sujeto de datos.
- **investigar resultados:** Página que permite investigar los datos mediante la búsqueda, clasificación, ampliación de los detalles de un archivo específico y descarga de la lista de archivos.



Si hay más de 10,000 resultados, sólo los 10,000 primeros aparecen en la lista de archivos.

Selección de los entornos de trabajo para los informes

Puede filtrar el contenido de la consola Cloud Data Sense Compliance para ver los datos de cumplimiento de normativas de todos los entornos de trabajo y bases de datos, o solo en entornos de trabajo específicos.

Cuando se filtra el panel, detección de datos define los datos de cumplimiento e informa únicamente a los entornos de trabajo seleccionados.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.

All Working Environments (12) ^

☒ Select all

☒ ANF - Azure NetApp Files

ANF

☒ Working Environment Name 1

CVO

☒ Working Environment Name 2

CVS

☒ Working Environment Name 3

CVS

☒ Working Environment Name 4

CVO

View

Cancel

Personal Files ⓘ

View All

Email Address 2,700 Files



Credit Card 2,700 Files



20%
Personal



5%
Sensitive Personal



7,000

Sensitive Personal Files ⓘ

View All

Health 2,700 Files



Ethnicity 2,700 Files



Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.