Supervise la exposición de datos confidenciales en AWS S3 y Azure Storage con DLP

Contenido

Introducción

Este documento describe cómo supervisar la exposición de datos confidenciales en AWS S3 y Azure Storage mediante la prevención de pérdida de datos (DLP).

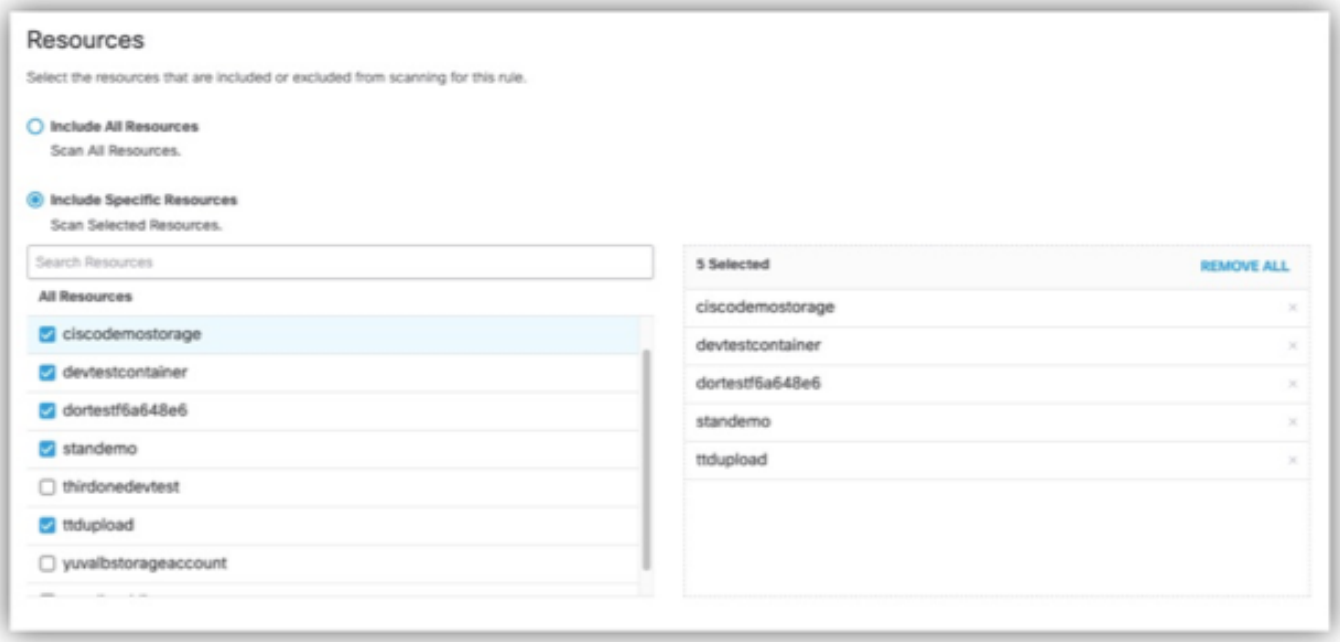
Overview

Con los nuevos conectores para AWS S3 y Azure Storage, ahora puede analizar la exposición de datos confidenciales en sus entornos de nube. Estas funciones le ayudan a descubrir y supervisar las credenciales expuestas (como claves API, secretos y tokens), así como datos confidenciales, incluida la información de identificación personal (PII), registros financieros e información sanitaria que puede estar expuesta a la Web pública.

¿Qué se escanea en AWS S3 y Azure File Storage?

- AWS S3:
  DLP realiza un análisis de detección inicial de datos confidenciales preexistentes y una supervisión continua de archivos nuevos o actualizados. Puede especificar los depósitos S3 que desea analizar seleccionándolos en la regla DLP.
- Azure File Storage:
  DLP admite la detección inicial y la supervisión continua de archivos nuevos o actualizados. Puede elegir los contenedores de Azure específicos que desea analizar dentro de su regla DLP.

Puede adaptar el escaneo de DLP seleccionando los depósitos exactos de AWS S3 o los contenedores de Azure para que se ajusten a sus necesidades y prioridades.



Acciones de respuesta admitidas para AWS y Azure

Actualmente, solo se admite la supervisión como acción de respuesta para AWS S3 y Azure Storage. Las acciones de remediación automáticas, como la eliminación de archivos o la cuarentena, no están disponibles. Este enfoque evita el riesgo de alterar los entornos de IaaS críticos al tiempo que le permite supervisar la exposición de datos confidenciales de forma eficaz.

Localizar depósitos AWS S3 y blobs de almacenamiento de Azure para remediación manual

Para facilitar la remediación manual, el informe de DLP incluye información detallada:

- El informe muestra el nombre real del bloque o depósito S3, lo que facilita la búsqueda en las consolas de AWS o Azure.
- Cada evento de violación de DLP proporciona el nombre del recurso, la URL de destino y, cuando está disponible, la ID del recurso.
- Utilice esta información para localizar y abordar las infracciones de DLP de forma eficaz dentro de los depósitos de AWS S3 y los blobs de almacenamiento de Azure.

Recursos relacionados

Consulte la documentación de Umbrella para obtener orientación detallada:

- Habilitar la protección contra pérdida de datos API SaaS para arrendatarios AWS
- Habilitar la protección contra pérdida de datos de API SaaS para arrendatarios de Azure
- Agregar una regla de API SaaS a la política de prevención de pérdida de datos

- Informe de prevención de pérdida de datos

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).