# Monitoraggio dell'esposizione dei dati sensibili in AWS S3 e Archiviazione di Azure con DLP

## Sommario

## Introduzione

In questo documento viene descritto come monitorare l'esposizione dei dati sensibili in AWS S3 e nell'archiviazione di Azure utilizzando Data Loss Prevention (DLP).

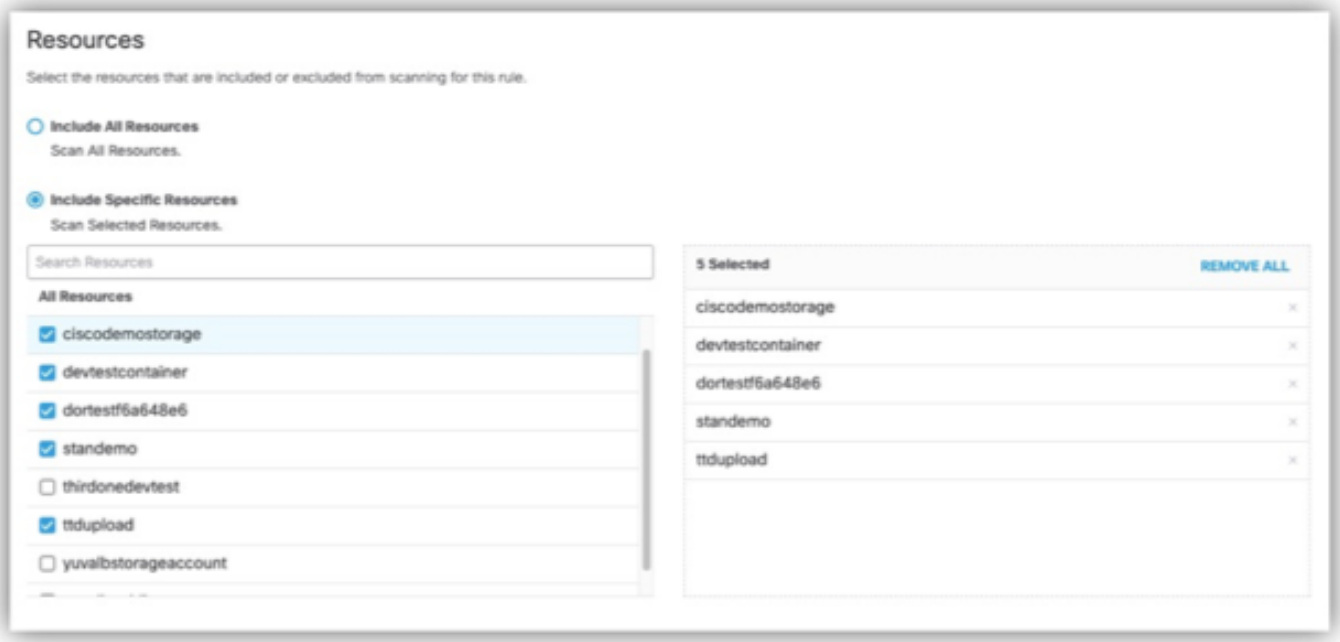
## Panoramica

Con i nuovi connettori per AWS S3 e Archiviazione di Azure, è ora possibile eseguire la scansione per rilevare l'esposizione dei dati sensibili negli ambienti cloud. Queste funzionalità consentono di individuare e monitorare le credenziali esposte, ad esempio chiavi API, segreti e token, nonché i dati sensibili, incluse le informazioni identificabili personalmente (PII, Personal Identifier), i record finanziari e le informazioni sanitarie che possono essere esposte al Web pubblico.

## Che cosa viene analizzato in AWS S3 e Archiviazione file di Azure?

- AWS-S3:
  DLP esegue sia una scansione iniziale di rilevamento per i dati sensibili preesistenti sia il monitoraggio continuo per i file nuovi o aggiornati. È possibile specificare i bucket S3 da analizzare selezionandoli nella regola di prevenzione della perdita dei dati.
- Archiviazione file di Azure:
  DLP supporta l'individuazione iniziale e il monitoraggio continuo per i file nuovi o aggiornati. È possibile scegliere i contenitori di Azure specifici da analizzare nella regola di prevenzione della perdita dei dati.

È possibile personalizzare l'analisi DLP selezionando i bucket AWS S3 esatti o i contenitori di Azure in base alle proprie esigenze e priorità.




## Azioni di risposta supportate per AWS e Azure

Attualmente, solo il monitoraggio è supportato come azione di risposta per AWS S3 e Archiviazione di Azure. Non sono disponibili azioni di monitoraggio e aggiornamento automatici, ad esempio l'eliminazione o la quarantena dei file. Questo approccio evita il rischio di interruzione delle attività negli ambienti IaaS mission-critical, consentendo al tempo stesso di monitorare in modo efficace l'esposizione dei dati sensibili.

## Individuare i bucket AWS-S3 e i BLOB di archiviazione di Azure per il monitoraggio e l'aggiornamento manuali

Per agevolare il risanamento manuale, il rapporto DLP include informazioni dettagliate:

- Il report visualizza il nome effettivo del bucket o del BLOB S3, semplificando la ricerca in AWS o nelle console di Azure.
- Ogni evento di violazione dei criteri di prevenzione della perdita dei dati fornisce il nome della risorsa, l'URL di destinazione e, se disponibile, l'ID della risorsa.
- Utilizzare queste informazioni per individuare e risolvere in modo efficiente le violazioni dei criteri di prevenzione della perdita dei dati all'interno dei bucket AWS S3 e dei BLOB di archiviazione di Azure.

## Risorse correlate

Per ulteriori informazioni, fare riferimento alla documentazione di Umbrella:

- Abilita protezione da perdita di dati dell'API SaaS per tenant AWS

- Abilita protezione da perdita di dati dell'API SaaS per tenant di Azure
- Aggiungere una regola API SaaS ai criteri di prevenzione della perdita di dati
- Rapporto sulla prevenzione della perdita dei dati

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).