Utilizzare la classificazione BlueXP

BlueXP classification

NetApp
April 03, 2024

This PDF was generated from https://docs.netapp.com/it-it/bluexp-classification/task-controlling-governance-data.html on April 03, 2024. Always check docs.netapp.com for the latest.

Sommario

Utilizzare la classificazione BlueXP

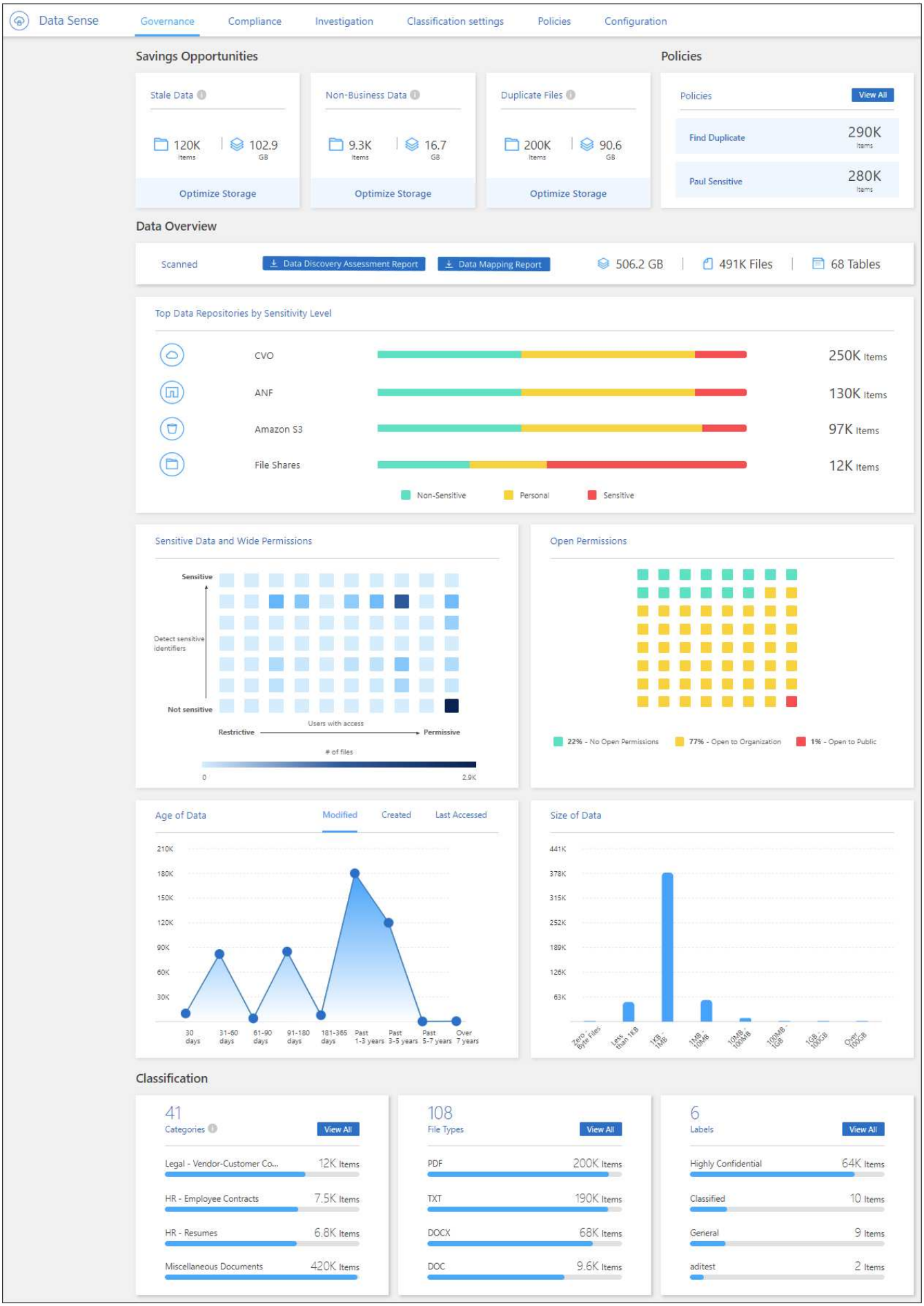
Visualizzare i dettagli di governance sui dati archiviati nell’organizzazione

Ottieni il controllo dei costi relativi ai dati sulle risorse di storage della tua organizzazione. La classificazione BlueXP identifica la quantità di dati obsoleti, dati non aziendali, file duplicati e file molto grandi nei sistemi, in modo da poter decidere se rimuovere o tierare alcuni file in uno storage a oggetti meno costoso.

Inoltre, se si prevede di migrare i dati da posizioni on-premise al cloud, è possibile visualizzare le dimensioni dei dati e se alcuni di essi contengono informazioni sensibili prima di spostarli.

Dashboard di governance

La dashboard di governance fornisce informazioni che consentono di aumentare l’efficienza e controllare i costi relativi ai dati memorizzati nelle risorse di storage.


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
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

Risparmiare opportunità

È possibile esaminare gli elementi nell'area *Saving Opportunities* per verificare se sono presenti dati da eliminare o da assegnare allo storage a oggetti meno costoso. Fare clic su ciascun elemento per visualizzare i risultati filtrati nella pagina di analisi.

- **Dati obsoleti** - dati modificati più di 3 anni fa.
- **Dati non aziendali** - dati considerati non correlati al business, in base alla categoria o al tipo di file. Ciò include:
  - Dati dell'applicazione
  - Audio
  - Eseguibili
  - Immagini
  - Registri
  - Video
  - Varie (categoria generale "Altro")
- **File duplicati** - file duplicati in altre posizioni nelle origini dati che si stanno eseguendo la scansione. "Scopri quali tipi di file duplicati vengono visualizzati".

  NOTA

  Se una qualsiasi delle origini dati implementa il tiering dei dati, i dati vecchi che risiedono già nello storage a oggetti possono essere identificati nella categoria *dati obsoleti*.

Policy con il maggior numero di risultati

Nell'area *Policies*, i criteri con il maggior numero di risultati vengono visualizzati in cima all'elenco. Fare clic sul nome di una policy per visualizzare i risultati nella pagina delle analisi. Fare clic su **View All** (Visualizza tutto) per visualizzare l'elenco di tutte le policy disponibili.

Fare clic su "qui" Per ulteriori informazioni sulle policy.

Panoramica dei dati

La sezione *Data Overview* fornisce una rapida panoramica di tutti i dati sottoposti a scansione. Fare clic sul pulsante per scaricare un report di mappatura dei dati completo che include capacità di utilizzo, età dei dati, dimensione dei dati e tipi di file per tutti gli ambienti di lavoro e le origini dati. Vedere Report di mappatura dei dati per informazioni dettagliate su questo report.

Principali repository di dati elencati in base alla sensibilità dei dati

L'area *Top Data Repository per livello di sensibilità* elenca i primi quattro repository di dati (ambienti di lavoro e origini dati) che contengono gli elementi più sensibili. Il grafico a barre per ciascun ambiente di lavoro è suddiviso in:

- Dati non sensibili
- Dati personali
- Dati personali sensibili

È possibile passare il mouse su ciascuna sezione per visualizzare il numero totale di elementi in ciascuna

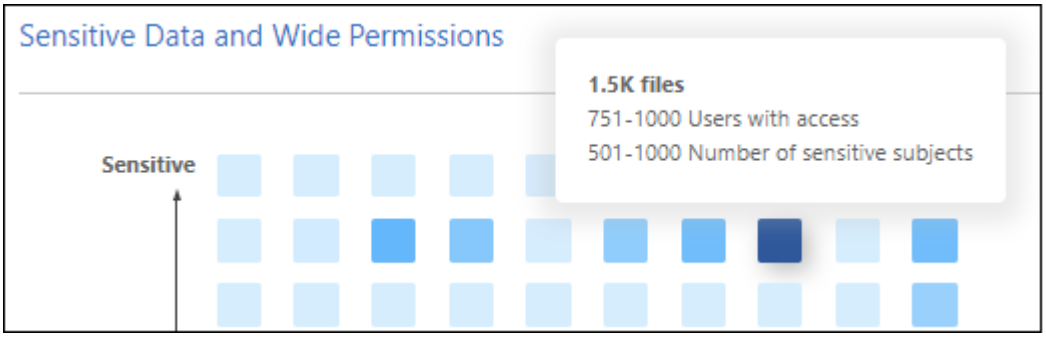
categoria.

Fare clic su ciascuna area per visualizzare i risultati filtrati nella pagina di analisi in modo da poter analizzare ulteriormente.

Dati elencati in base alla sensibilità e alle autorizzazioni estese

L'area *dati sensibili e permessi estesi* fornisce una mappa termica dei file che contengono dati sensibili (inclusi dati personali sensibili e sensibili) e che sono eccessivamente permissivi. In questo modo è possibile individuare i rischi associati ai dati sensibili.

La classificazione dei file dipende dal numero di utenti autorizzati ad accedere ai file sull'asse X (dal più basso al più alto) e dal numero di identificatori sensibili all'interno dei file sull'asse Y (dal più basso al più alto). I blocchi rappresentano il numero di file che corrispondono agli elementi degli assi X e Y. I blocchi di colore più chiaro sono buoni, con meno utenti in grado di accedere ai file e con meno identificatori sensibili per file. I blocchi più scuri sono gli elementi che potresti voler esaminare. Ad esempio, la schermata seguente mostra il testo del passaggio del mouse per il blocco blu scuro. Indica che sono disponibili 1,500 file a cui hanno accesso 751-100 utenti e 501-100 identificatori sensibili per file.



È possibile fare clic sul blocco desiderato per visualizzare i risultati filtrati dei file interessati nella pagina di analisi, in modo da poter analizzare ulteriormente.

Se non si è integrato un servizio di identità con la classificazione BlueXP, in questo pannello non viene visualizzato alcun dato. "Scopri come integrare il servizio Active Directory con la classificazione BlueXP".

> Questo pannello supporta i file in condivisioni CIFS, OneDrive e origini dati SharePoint. Attualmente non è disponibile alcun supporto per database, Google Drive, Amazon S3 e storage a oggetti generici.

Dati elencati in base ai tipi di autorizzazioni aperte

L'area *Open Permissions* mostra la percentuale per ciascun tipo di permessi esistenti per tutti i file sottoposti a scansione. Il grafico mostra i seguenti tipi di autorizzazioni:

- Nessuna autorizzazione aperta
- Aperto all'organizzazione
- Aperto al pubblico
- Accesso sconosciuto

È possibile passare il mouse su ciascuna sezione per visualizzare il numero totale di file in ciascuna categoria. Fare clic su ciascuna area per visualizzare i risultati filtrati nella pagina di analisi in modo da poter analizzare ulteriormente.

Età dei dati e dimensioni dei grafici dei dati

È possibile esaminare gli elementi nei grafici *Age* e *Size* per verificare se sono presenti dati da eliminare o da assegnare allo storage a oggetti meno costoso.

È possibile passare il mouse su un punto dei grafici per visualizzare i dettagli relativi all'età o alle dimensioni dei dati in tale categoria. Fare clic per visualizzare tutti i file filtrati in base all'età o all'intervallo di dimensioni.

- **Age of Data graph** - classifica i dati in base all'ora in cui sono stati creati, all'ultima volta in cui sono stati utilizzati o all'ultima volta in cui sono stati modificati.
- **Dimensione del grafico dei dati** - classifica i dati in base alle dimensioni.

NOTA

Se una qualsiasi delle origini dati implementa il tiering dei dati, i dati vecchi che risiedono già nello storage a oggetti possono essere identificati nel grafico *Age of Data*.

Classificazioni dei dati più identificate

L'area *Classification* fornisce un elenco dei più identificati "Categorie", "Tipi di file", e. "Etichette AIP" nei dati sottoposti a scansione.

Categorie

Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come "curriculum" o "contratti dipendenti" può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

Vedere "Visualizzazione dei file in base alle categorie" per ulteriori informazioni.

Tipi di file

La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere memorizzati correttamente.

Vedere "Visualizzazione dei tipi di file" per ulteriori informazioni.

Etichette AIP

Se si è abbonati ad Azure Information Protection (AIP), è possibile classificare e proteggere documenti e file applicando etichette ai contenuti. La revisione delle etichette AIP più utilizzate assegnate ai file consente di visualizzare le etichette più utilizzate nei file.

Vedere "Etichette AIP" per ulteriori informazioni.

Report di mappatura dei dati

Il Data Mapping Report fornisce una panoramica dei dati memorizzati nelle origini dati aziendali per assisterti nelle decisioni relative a migrazione, backup, sicurezza e processi di conformità. Il report elenca prima una panoramica che riepiloga tutti gli ambienti di lavoro e le origini dati, quindi fornisce un'analisi dettagliata per ciascun ambiente di lavoro.

Il report contiene le seguenti informazioni:

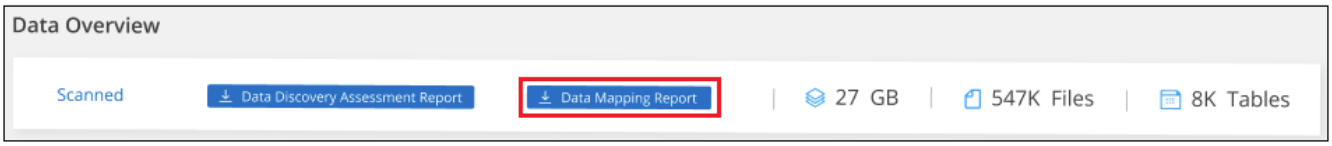
Categoria	Descrizione
Capacità di utilizzo	Per tutti gli ambienti di lavoro: Elenca il numero di file e la capacità utilizzata per ciascun ambiente di lavoro. Per ambienti di lavoro singoli: Elenca i file che utilizzano la capacità maggiore.
Età dei dati	Fornisce tre grafici e grafici per la data di creazione, l'ultima modifica o l'ultimo accesso ai file. Elenca il numero di file e la relativa capacità utilizzata, in base a determinati intervalli di date.
Dimensione dei dati	Elenca il numero di file presenti in determinati intervalli di dimensioni negli ambienti di lavoro.
Tipi di file	Elenca il numero totale di file e la capacità utilizzata per ciascun tipo di file memorizzato negli ambienti di lavoro.

Generare il rapporto di mappatura dati

Questo report viene generato dalla scheda Governance della classificazione BlueXP.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Governance**, quindi sul pulsante **Data Mapping Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

Se il report è più grande di 1 MB, il file PDF viene conservato nell'istanza di classificazione di BlueXP e viene visualizzato un messaggio a comparsa relativo alla posizione esatta. Quando la classificazione BlueXP viene installata su una macchina Linux in sede o su una macchina Linux implementata nel cloud, è possibile accedere direttamente al file PDF. Quando la classificazione BlueXP viene implementata nel cloud, è necessario eseguire l'SSH nell'istanza di classificazione BlueXP per scaricare il file PDF. "Scopri come accedere ai dati sull'istanza di Classification".

Nota: È possibile personalizzare il nome della società visualizzato nella prima pagina del report dalla parte superiore della pagina di classificazione di BlueXP facendo clic su ⋮ Quindi fare clic su **Cambia nome azienda**. La volta successiva che si genera il report, questo includerà il nuovo nome.

Report sulla valutazione del rilevamento dei dati

Il Data Discovery Assessment Report fornisce un'analisi di alto livello dell'ambiente sottoposto a scansione per evidenziare i risultati del sistema e mostrare le aree di interesse e le potenziali fasi di correzione. I risultati si basano sia sulla mappatura che sulla classificazione dei dati. L'obiettivo di questo report è quello di sensibilizzare l'utente su tre aspetti significativi del set di dati:

Funzione	Descrizione
Problemi di governance dei dati	Un'immagine dettagliata di tutti i dati in tuo possesso e delle aree in cui puoi ridurre la quantità di dati per risparmiare sui costi.
Esposizioni alla sicurezza dei dati	Aree in cui i dati sono accessibili ad attacchi interni o esterni a causa di ampie autorizzazioni di accesso.
Lacune nella compliance dei dati	Dove si trovano le informazioni personali o sensibili per motivi di sicurezza e DSAR (richieste di accesso dei soggetti).

Dopo la valutazione, questo report identifica le aree in cui è possibile:

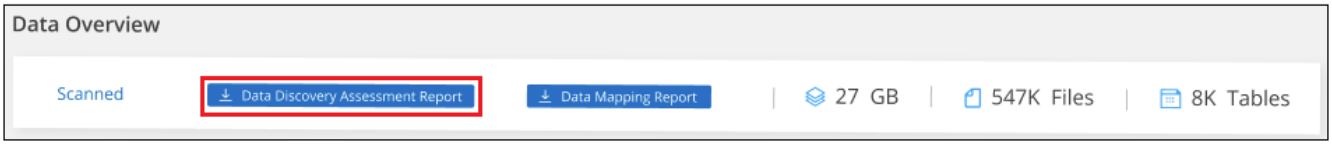
- Riduci i costi di storage modificando la policy di conservazione o spostando o eliminando determinati dati (dati obsoleti, duplicati o non aziendali)
- Proteggi i tuoi dati che dispongono di ampie autorizzazioni rivedendo le policy di gestione dei gruppi globali
- Proteggi i tuoi dati personali o sensibili trasferendo le informazioni personali in archivi di dati più sicuri

Generare il report di valutazione per il rilevamento dei dati

Questo report viene generato dalla scheda Governance della classificazione BlueXP.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Governance**, quindi sul pulsante **Data Discovery Assessment Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

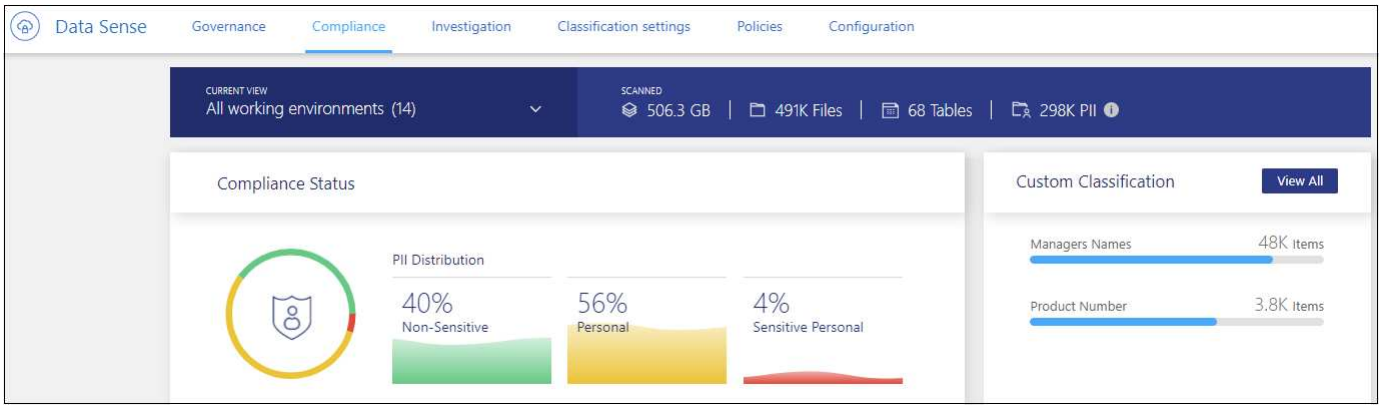
Nota: È possibile personalizzare il nome della società visualizzato nella prima pagina del report dalla parte superiore della pagina di classificazione di BlueXP facendo clic su ⋮ Quindi fare clic su **Cambia nome azienda**. La volta successiva che si genera il report, questo includerà il nuovo nome.

Consente di visualizzare i dettagli di conformità relativi ai dati archiviati nell'organizzazione

Ottieni il controllo dei tuoi dati privati visualizzando i dettagli relativi ai dati personali e ai dati personali sensibili della tua organizzazione. È inoltre possibile ottenere visibilità esaminando le categorie e i tipi di file che BlueXP classifica trovato nei dati.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

Per impostazione predefinita, la dashboard di classificazione BlueXP visualizza i dati di conformità per tutti gli ambienti di lavoro e i database.



Se si desidera visualizzare i dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

È inoltre possibile filtrare i risultati dalla pagina Data Investigation (analisi dati) e scaricare un report dei risultati come file CSV. Vedere "Filtraggio dei dati nella pagina Data Investigation" per ulteriori informazioni.

Consente di visualizzare i file che contengono dati personali

La classificazione BlueXP identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario, password, e molto altro ancora. "Consulta l'elenco completo". La classificazione BlueXP identifica questo tipo di informazioni nei singoli file, nei file all'interno delle directory (condivisioni e cartelle) e nelle tabelle dei database.

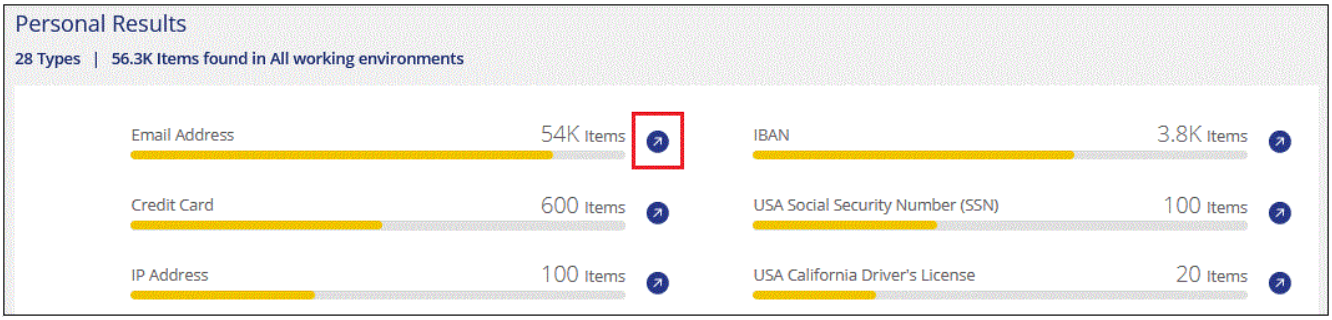
Inoltre, se è stato aggiunto un server di database da sottoporre a scansione, la funzione *Data Fusion* consente di eseguire la scansione dei file per identificare se gli identificatori univoci dei database sono presenti in tali file o in altri database. Vedere "Aggiunta di identificatori di dati personali mediante Data Fusion" per ulteriori informazioni.

Per alcuni tipi di dati personali, la classificazione BlueXP utilizza *Proximity Validation* per validarne i risultati. La convalida avviene cercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, la classificazione BlueXP identifica un Numero di previdenza sociale (SSN) come SSN se viene visualizzato un termine di prossimità, ad esempio *SSN* o *social Security*. "La tabella dei dati personali" Mostra quando la classificazione BlueXP utilizza la convalida di prossimità.

Fasi

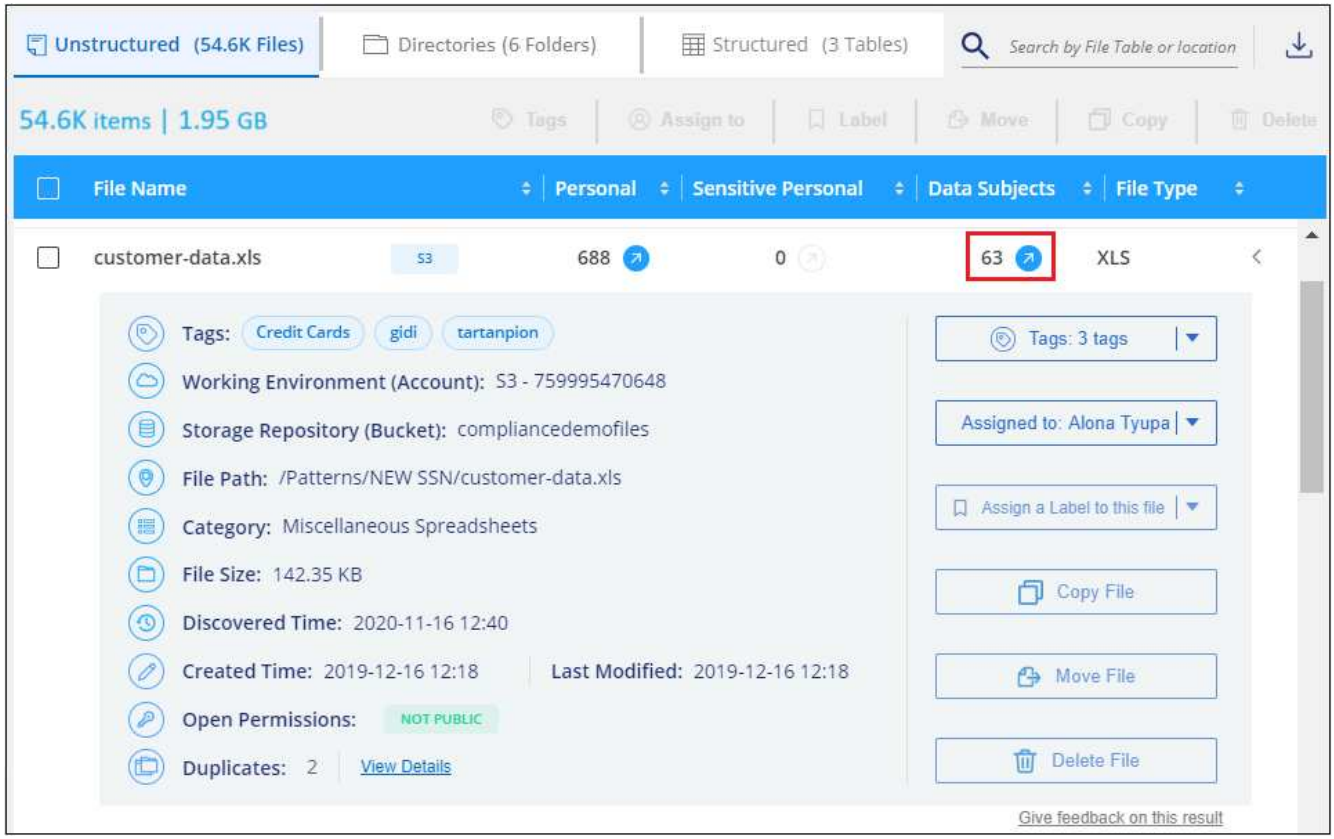
1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Per esaminare i dettagli di tutti i dati personali, fare clic sull'icona accanto alla percentuale dei dati personali.

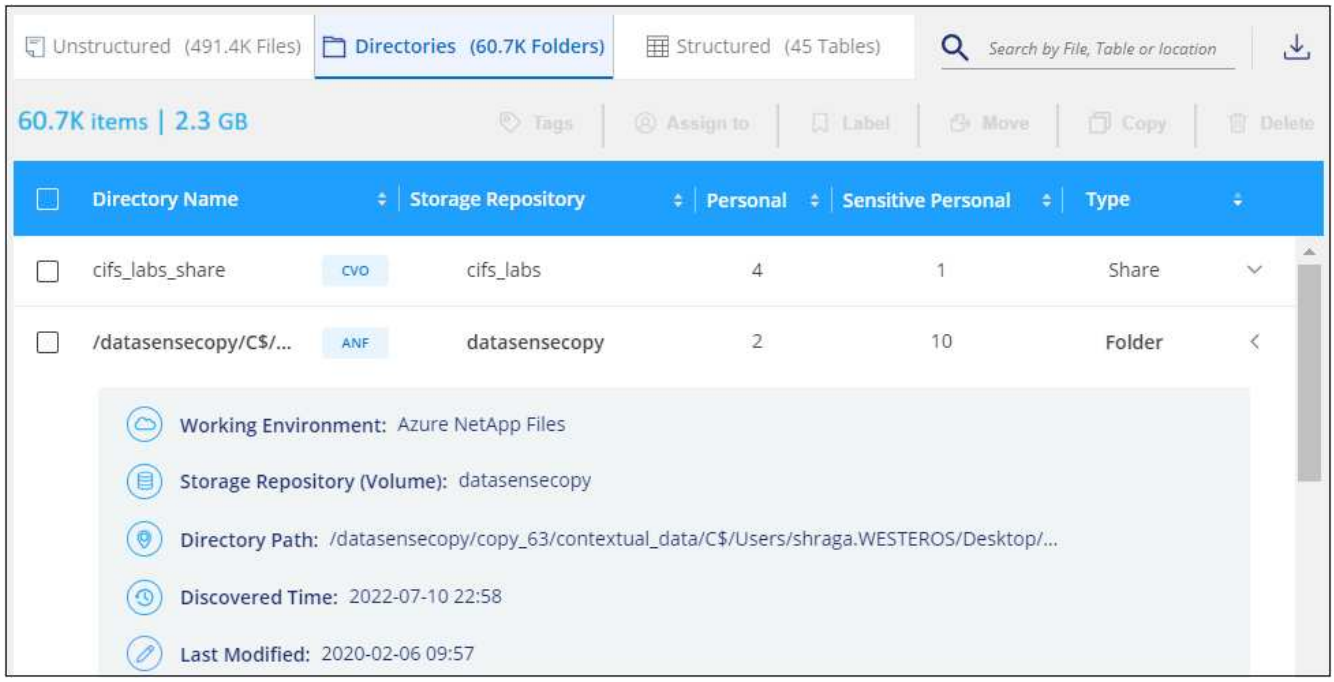
3. Per esaminare i dettagli di un tipo specifico di dati personali, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali, ad esempio indirizzi e-mail.



4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

   Le 2 schermate riportate di seguito mostrano i dati personali presenti nei singoli file e contenuti nei file all'interno delle directory (condivisioni e cartelle). È inoltre possibile selezionare la scheda **Structured** per visualizzare i dati personali trovati nei database.





Consente di visualizzare i file che contengono dati personali sensibili

La classificazione BlueXP identifica automaticamente tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy, ad esempio "articoli 9 e 10 del GDPR". Ad esempio, informazioni relative alla salute, all'origine etnica o all'orientamento sessuale di una persona. "Consulta l'elenco completo". La classificazione BlueXP identifica questo tipo di informazioni nei singoli file, nei file all'interno delle directory (condivisioni e cartelle) e nelle tabelle dei database.

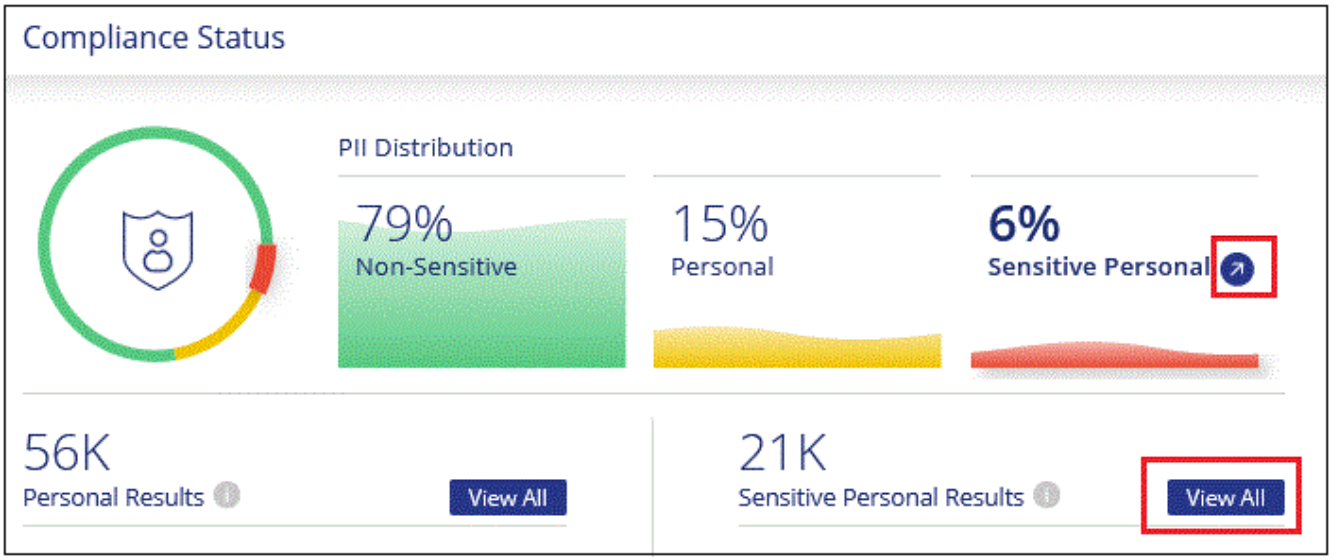
La classificazione BlueXP utilizza l'intelligenza artificiale (ai), l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il calcolo cognitivo (CC) per comprendere il significato del contenuto che scansiona al fine di estrarre le entità e classificarlo di conseguenza.

Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità NLP, la classificazione BlueXP è in grado di distinguere la differenza tra una frase che recita "George is Mexican" (che indica i dati sensibili come specificato nell'articolo 9 del GDPR) e "George is Eating Mexican Food" (George sta mangiando cibo messicano).

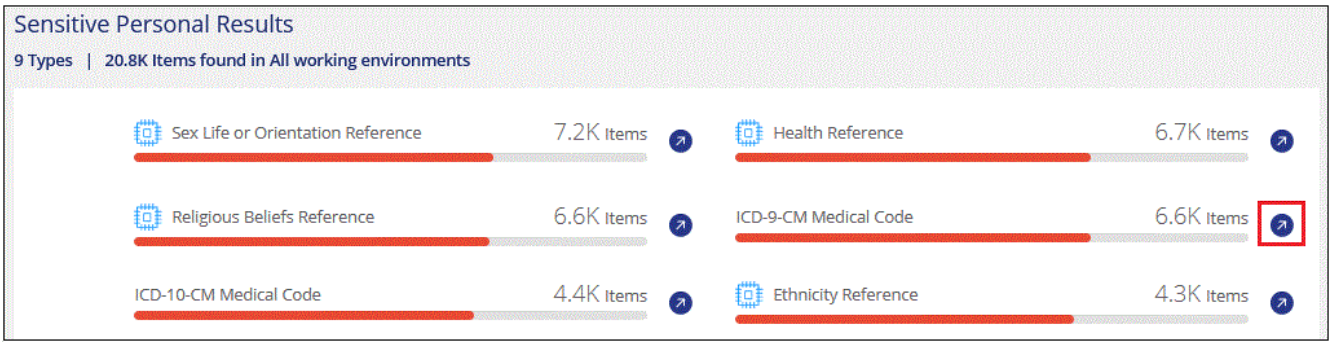
> Quando si esegue la scansione di dati personali sensibili, è supportata solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Per esaminare i dettagli di tutti i dati personali sensibili, fare clic sull'icona accanto alla percentuale dei dati personali sensibili.



3. Per esaminare i dettagli di un tipo specifico di dati personali sensibili, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali sensibili.



4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Visualizzare i file per categorie

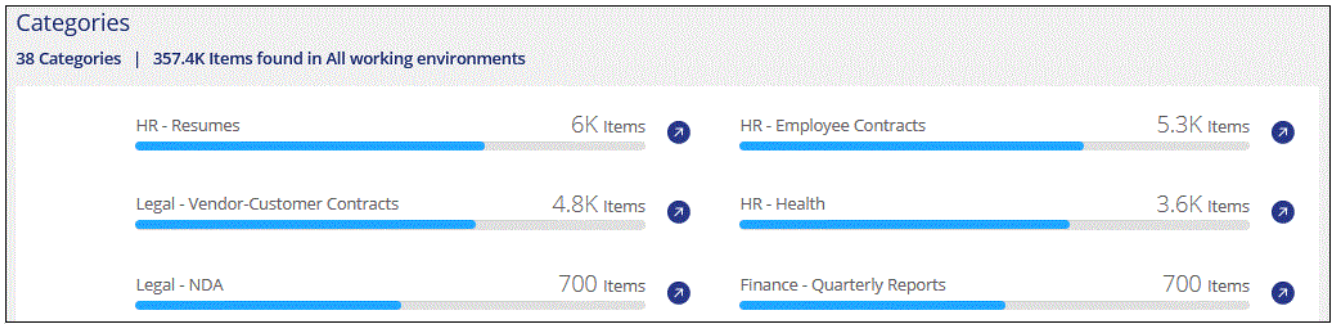
La classificazione BlueXP prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Vedere l'elenco delle categorie".

Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come i curriculum o i contratti dei dipendenti può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

> Le categorie sono supportate in inglese, tedesco e spagnolo. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Fare clic sull'icona **esamina risultati** di una delle 4 categorie principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto** e quindi sull'icona corrispondente a una delle categorie.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

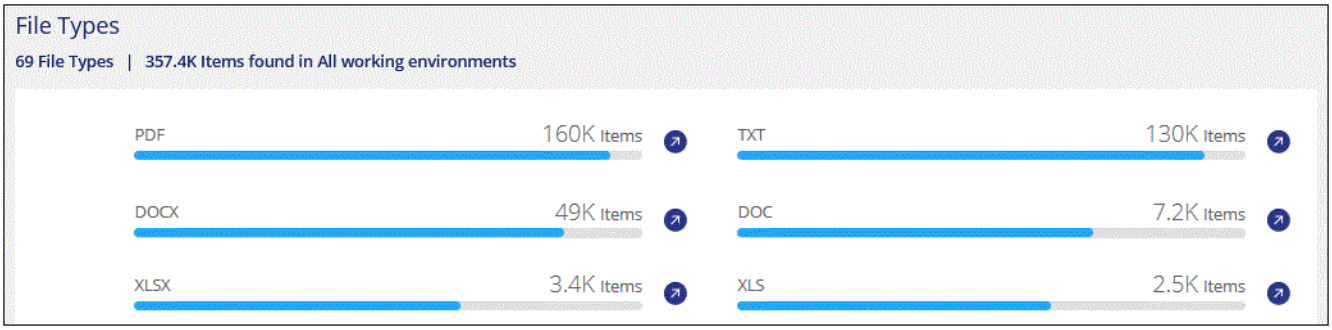
Visualizzare i file in base ai tipi di file

La classificazione BlueXP prende i dati sottoposti a scansione e li suddivide in base al tipo di file. La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere memorizzati correttamente. "Vedere l'elenco dei tipi di file".

Ad esempio, è possibile memorizzare file CAD che includono informazioni molto sensibili sull'organizzazione. Se non sono protetti, è possibile assumere il controllo dei dati sensibili limitando le autorizzazioni o spostando i file in un'altra posizione.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**, quindi fare clic sulla scheda **Compliance**.
2. Fare clic sull'icona **esamina risultati** per uno dei 4 tipi di file principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto**, quindi fare clic sull'icona corrispondente a uno qualsiasi dei tipi di file.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

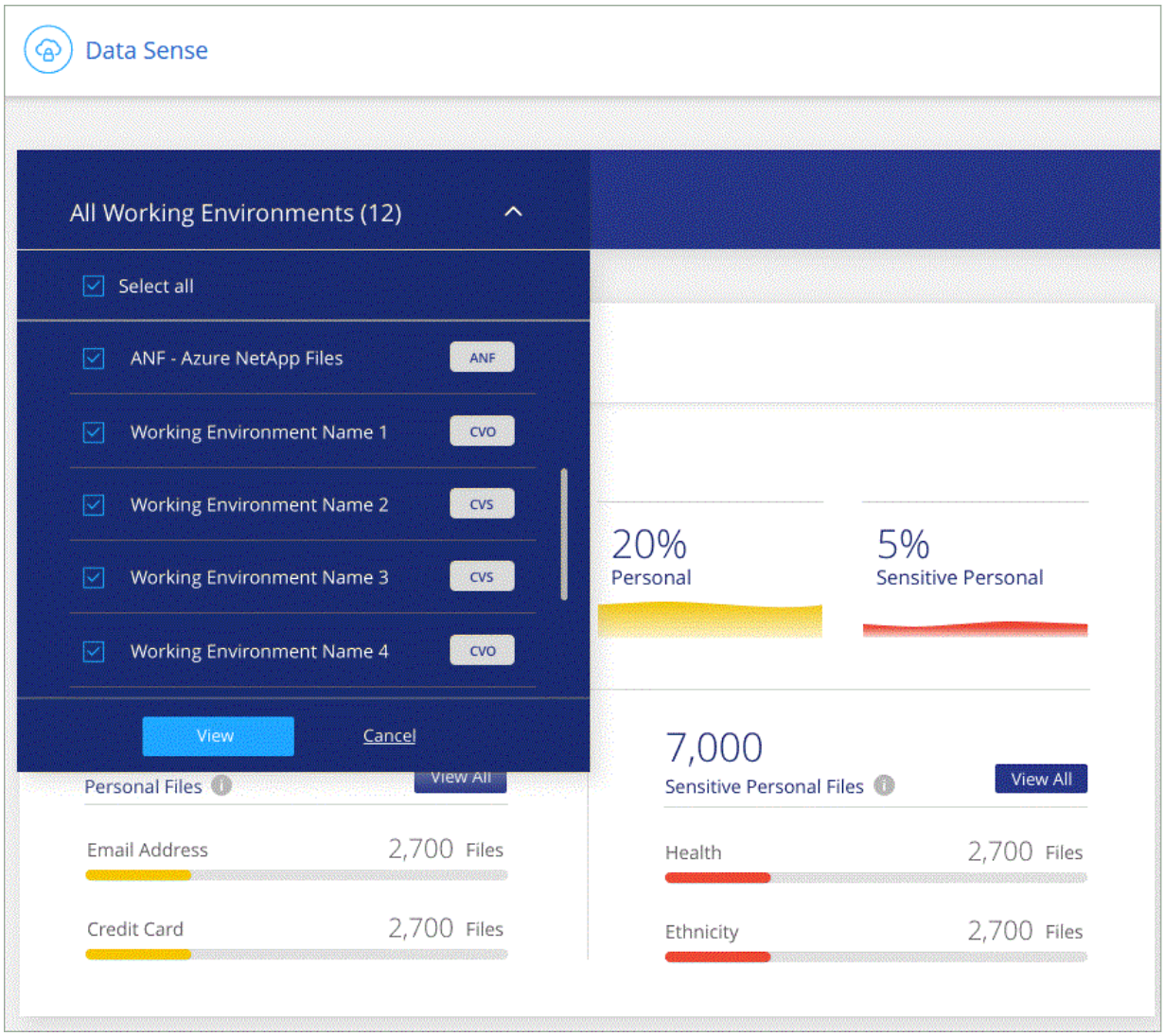
Visualizza i dati del dashboard per ambienti di lavoro specifici

È possibile filtrare il contenuto della dashboard di classificazione BlueXP per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando si filtra la dashboard, la classificazione BlueXP regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).



Categorie di dati privati

Esistono molti tipi di dati privati che la classificazione BlueXP può identificare nei volumi, nei bucket Amazon S3, nei database, nelle cartelle OneDrive, negli account SharePoint, E Google Drive. Vedere le categorie riportate di seguito.

> Se hai bisogno della classificazione BlueXP per identificare altri tipi di dati privati, come ad esempio numeri di identificazione nazionali aggiuntivi o identificatori sanitari, invia un'email a ng-contact-data-sense@netapp.com con la tua richiesta.

Tipi di dati personali

I dati personali contenuti nei file possono essere dati personali di carattere generale o identificativi nazionali. La terza colonna nella tabella seguente indica se la classificazione BlueXP utilizza "convalida della prossimità" per convalidare i risultati per l'identificatore.

Le lingue in cui questi elementi possono essere riconosciuti sono identificate nella tabella.

Nota: È possibile aggiungere all'elenco dei dati personali presenti nei file. Se si esegue la scansione di un

server di database, la funzione *Data Fusion* consente di scegliere gli identificatori aggiuntivi che la classificazione BlueXP dovrà cercare nelle scansioni selezionando le colonne in una tabella di database. È inoltre possibile aggiungere parole chiave personalizzate da un file di testo o modelli personalizzati utilizzando un'espressione regolare. Vedere "Aggiunta di identificatori di dati personali alle scansioni di classificazione BlueXP" per ulteriori informazioni.

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
Generale	Numero della carta di credito	No	✓	✓	✓		✓
	Soggetti dei dati	No	✓	✓	✓		
	Indirizzo e-mail	No	✓	✓	✓		✓
	Numero IBAN (International Bank account Number)	No	✓	✓	✓		✓
	Indirizzo IP	No	✓	✓	✓		✓
	Password	Sì	✓	✓	✓		✓

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
Identificatori nazionali							
16							

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese

Tipo	Identificatore	Convalida della prossimità?	Inglese	Tedesco	Spagnolo	Francese	Giapponese
	ID svedese	Sì	✓	✓	✓		
	Texas driver's License	Sì	✓	✓	✓		
	REGNO UNITO ID (NINO)	Sì	✓	✓	✓		
	USA California driver's License	Sì	✓	✓	✓		
	USA, Indiana driver's License	Sì	✓	✓	✓		
	USA New York driver's License	Sì	✓	✓	✓		
	Numero di previdenza sociale (SSN) USA	Sì	✓	✓	✓		

Tipi di dati personali sensibili

I dati personali sensibili che la classificazione BlueXP può trovare nei file includono il seguente elenco.

Al momento, gli elementi di questa categoria possono essere riconosciuti solo in inglese.

Riferimento alle procedure penali
Dati relativi alle condanne e ai reati penali di una persona fisica.

Riferimento di etnia
Dati relativi alla razza o all'origine etnica di una persona fisica.

Riferimento di salute
Dati relativi alla salute di una persona fisica.

Codici medici ICD-9-CM
Codici utilizzati nel settore medico e sanitario.

Codici medici ICD-10-CM
Codici utilizzati nel settore medico e sanitario.

Riferimento alle credenze filosofiche
Dati relativi alle convinzioni filosofiche di una persona naturale.

Opinioni politiche riferimento
Dati relativi alle opinioni politiche di una persona fisica.

Riferimenti alle credenze religiose
Dati relativi alle convinzioni religiose di una persona fisica.

Sex Life o orientamento di riferimento
Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Tipi di categorie

La classificazione BlueXP classifica i tuoi dati nel modo seguente.

La maggior parte di queste categorie può essere riconosciuta in inglese, tedesco e spagnolo.

Categoria	Tipo	Inglese	Tedesco	Spagnolo
Finanza	Bilanci	✓	✓	✓
	Ordini di acquisto	✓	✓	✓
	Fatture	✓	✓	✓
	Report trimestrali	✓	✓	✓
FC	Controlli in background	✓		✓
	Piani di compensazione	✓	✓	✓
	Contratti con i dipendenti	✓		✓
	Recensioni dei dipendenti	✓		✓
	Salute	✓		✓
	Riprende	✓	✓	✓
Legale	NDA	✓	✓	✓
	Contratti fornitore-cliente	✓	✓	✓
Marketing	Campagne	✓	✓	✓
	Conferenze	✓	✓	✓
Operazioni	Report di audit	✓	✓	✓
Vendite	Ordini di vendita	✓	✓	
Servizi	RFI	✓		✓
	RFP	✓		✓
	SOW	✓	✓	✓
	Formazione	✓	✓	✓
Supporto	Reclami e biglietti	✓	✓	✓

I seguenti metadati sono anche classificati e identificati nelle stesse lingue supportate:

- Dati dell’applicazione
- Archiviare i file
- Audio
- Dati delle applicazioni di business
- File CAD
- Codice
- Corrotto
- Database e file di indice
- Classificazione BlueXP Breadcrumbs
- File di progettazione
- Email Application Data (dati applicazione email)

- Crittografato (file con un elevato punteggio di entropia)
- Eseguibili
- Dati delle applicazioni finanziarie
- Health Application Data
- Immagini
- Registri
- Documenti vari
- Presentazioni varie
- Fogli di calcolo vari
- Varie "Sconosciuto"
- File protetti da password
- Dati strutturati
- Video
- File a byte zero

Tipi di file

La classificazione BlueXP esegue la scansione di tutti i file per informazioni su categorie e metadati e visualizza tutti i tipi di file nella sezione tipi di file della dashboard.

Tuttavia, quando la classificazione BlueXP rileva le informazioni personali identificabili (PII) o quando esegue una ricerca DSAR, sono supportati solo i seguenti formati di file:

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

Accuratezza delle informazioni rilevate

NetApp non può garantire la precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla classificazione BlueXP. È sempre necessario convalidare le informazioni esaminando i dati.

In base ai nostri test, la tabella seguente mostra l'accuratezza delle informazioni rilevate dalla classificazione BlueXP. Lo suddivideremo per *precisione* e *richiamo*:

Precisione

La probabilità che la classificazione BlueXP trovi sia stata identificata correttamente. Ad esempio, un tasso di precisione del 90% per i dati personali significa che 9 file su 10 identificati come contenenti informazioni personali contengono effettivamente informazioni personali. 1 file su 10 sarebbe un falso positivo.

Ricorda

Probabilità che la classificazione BlueXP trovi ciò che dovrebbe. Ad esempio, un tasso di richiamo del 70% per i dati personali significa che la classificazione BlueXP può identificare 7 file su 10 che contengono effettivamente informazioni personali nella tua organizzazione. La classificazione di BlueXP non consentirebbe il 30% dei dati e non verrà visualizzata nella dashboard.

Stiamo costantemente migliorando la precisione dei nostri risultati. Tali miglioramenti saranno automaticamente disponibili nelle future release di classificazione BlueXP.

Tipo	Precisione	Ricorda
Dati personali - Generale	90%-95%	60%-80%
Dati personali - identificatori del Paese	30%-60%	40%-60%
Dati personali sensibili	80%-95%	20%-30%
Categorie	90%-97%	60%-80%

Esaminare i dati memorizzati nella propria organizzazione

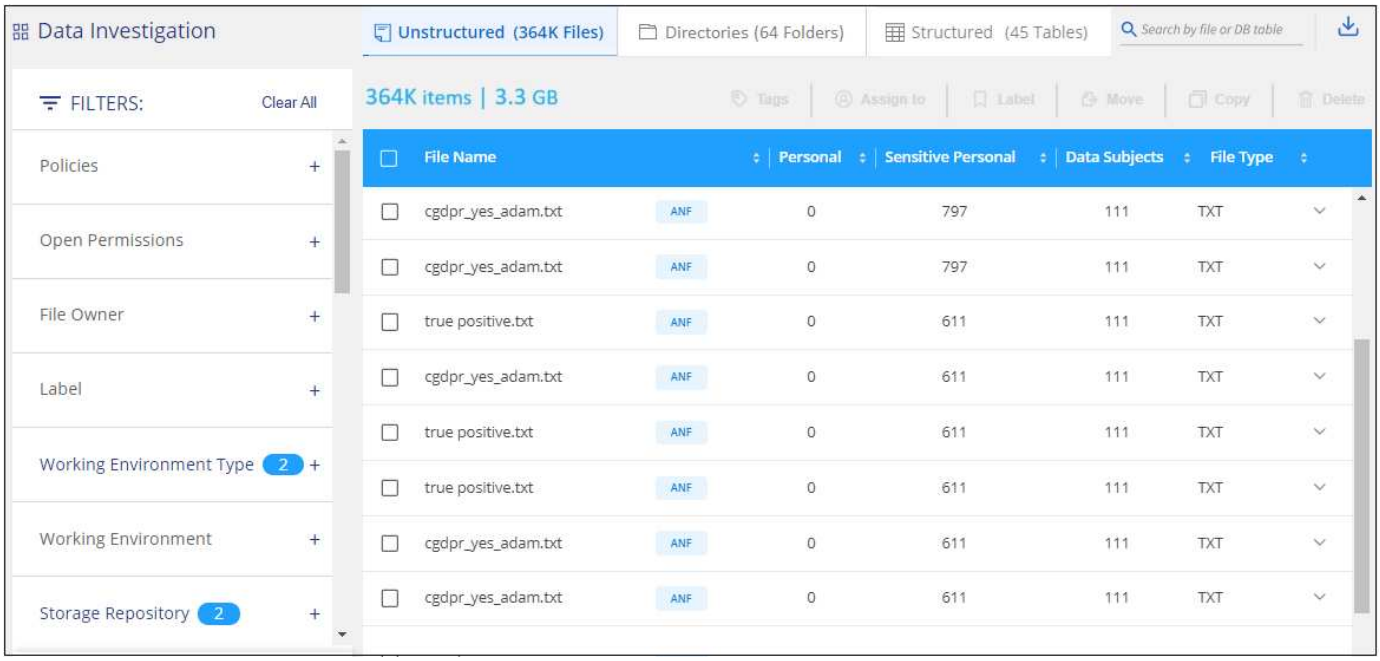
È possibile analizzare i dati dell'organizzazione visualizzando i dettagli nella pagina Data Investigation. È possibile accedere a questa pagina da molte aree dell'interfaccia utente di classificazione di BlueXP, tra cui le dashboard di governance e conformità.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

Filtrare i dati nella pagina analisi dati

È possibile filtrare il contenuto della pagina di analisi per visualizzare solo i risultati desiderati. Si tratta di una funzione molto potente, in quanto dopo aver perfezionato i dati, è possibile utilizzare la barra dei pulsanti nella parte superiore della pagina per eseguire una serie di azioni, tra cui la copia di file, lo spostamento di file, l'aggiunta di un tag o di un'etichetta AIP ai file e molto altro.

Se si desidera scaricare il contenuto della pagina come report dopo averlo perfezionato, fare clic su pulsante. Fare clic qui per ulteriori informazioni sul report Data Investigation.



- Le schede di livello superiore consentono di visualizzare i dati di file (dati non strutturati), directory (cartelle e condivisioni di file) o database (dati strutturati).
- I controlli nella parte superiore di ciascuna colonna consentono di ordinare i risultati in ordine numerico o

alfabetico.

- I filtri del riquadro sinistro consentono di perfezionare i risultati selezionando gli attributi descritti nelle sezioni successive.

Filtra i dati in base alla sensibilità e al contenuto

Utilizzare i seguenti filtri per visualizzare la quantità di informazioni sensibili contenute nei dati.

Filtro	Dettagli
Categoria	Selezionare "tipi di categorie".
Livello di sensibilità	Selezionare il livello di sensibilità: Personal (personale), Sensitive Personal (personale sensibile) o non Sensitive (non sensibile).
Numero di identificatori	Selezionare l'intervallo di identificatori sensibili rilevati per file. Include dati personali e dati personali sensibili. Durante il filtraggio nelle directory, la classificazione BlueXP totalizza le corrispondenze di tutti i file in ogni cartella (e sottocartelle). NOTA: La versione di dicembre 2023 (versione 1.26.6) ha temporaneamente rimosso l'opzione per calcolare il numero di dati personali identificabili (PII) per Directory.
Dati personali	Selezionare "tipi di dati personali".
Dati personali sensibili	Selezionare "tipi di dati personali sensibili".
Soggetto interessato	Inserire il nome completo o l'identificativo noto di un soggetto. "Scopri di più sugli argomenti dei dati qui".

Filtrare i dati in base al proprietario dell'utente e alle autorizzazioni dell'utente

Utilizzare i seguenti filtri per visualizzare i proprietari dei file e le autorizzazioni di accesso ai dati.

Filtro	Dettagli
Aprire permessi	Selezionare il tipo di permessi all'interno dei dati e all'interno di cartelle/condivisioni.
Autorizzazioni utente/gruppo	Selezionare uno o più nomi utente e/o nomi di gruppo oppure immettere un nome parziale.
Proprietario del file	Immettere il nome del proprietario del file.
Numero di utenti con accesso	Selezionare uno o più intervalli di categorie per visualizzare i file e le cartelle aperti a un determinato numero di utenti.

Filtrare i dati in base all'ora

Utilizzare i seguenti filtri per visualizzare i dati in base ai criteri temporali.

Filtro	Dettagli
Ora di creazione	Selezionare un intervallo di tempo in cui è stato creato il file. È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.

Filtro	Dettagli
Tempo scoperto	Selezionare un intervallo di tempo in cui la classificazione BlueXP ha rilevato il file. È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Ultima modifica	Selezionare un intervallo di tempo in cui il file è stato modificato per l'ultima volta. È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca.
Ultimo accesso	Selezionare un intervallo di tempo in cui è stato eseguito l'ultimo accesso al file o alla directory (solo CIFS o NFS). È inoltre possibile specificare un intervallo di tempo personalizzato per perfezionare ulteriormente i risultati della ricerca. Per i tipi di file sottoposti a scansione dalla classificazione BlueXP, questa è l'ultima volta che la classificazione BlueXP ha sottoposto a scansione il file. Si noti che la classificazione BlueXP non estrae l'ultimo tempo di accesso dalle seguenti origini dati: SharePoint Online, SharePoint on-premise (SharePoint Server), OneDrive, Google Drive e Amazon S3.

Filtra i dati in base ai metadati

Utilizzare i seguenti filtri per visualizzare i dati in base alla posizione, alle dimensioni e alla directory o al tipo di file.

Filtro	Dettagli
Percorso del file	Immettere fino a 20 percorsi parziali o completi che si desidera includere o escludere dalla query. Se si immettono entrambi i percorsi di inclusione ed esclusione, la classificazione BlueXP individua prima tutti i file nei percorsi inclusi, quindi rimuove i file dai percorsi esclusi e visualizza i risultati. Si noti che l'utilizzo di "*" in questo filtro non ha alcun effetto e che non è possibile escludere cartelle specifiche dalla scansione: Verranno acquisite tutte le directory e i file presenti in una condivisione configurata.
Tipo di directory	Selezionare il tipo di directory; "Share" (Condividi) o "Folder" (cartella).
Tipo di file	Selezionare "tipi di file".
Dimensione del file	Selezionare l'intervallo di dimensioni del file.
Hash del file	Inserire l'hash del file per trovare un file specifico, anche se il nome è diverso.

Filtrare i dati in base al tipo di storage

Utilizzare i seguenti filtri per visualizzare i dati in base al tipo di storage.

Filtro	Dettagli
Tipo di ambiente di lavoro	Selezionare il tipo di ambiente di lavoro. OneDrive, SharePoint e Google Drive sono classificati in "App".
Nome dell'ambiente di lavoro	Selezionare ambienti di lavoro specifici.

Filtro	Dettagli
Repository di storage	Selezionare il repository di storage, ad esempio un volume o uno schema.

Filtra i dati in base a tag, etichette, utenti assegnati e policy

Utilizzare i seguenti filtri per visualizzare i dati in base alle etichette o ai tag AIP.

Filtro	Dettagli
Policy	Selezionare una o più policy. Vai "qui" per visualizzare l'elenco dei criteri esistenti e creare criteri personalizzati.
Etichetta	Selezionare "Etichette AIP" assegnati ai file.
Tag	Selezionare "il tag o i tag" assegnati ai file.
Assegnato a.	Selezionare il nome della persona a cui è assegnato il file.

Filtrare i dati in base allo stato dell'analisi

Utilizzare il seguente filtro per visualizzare i dati in base allo stato di scansione della classificazione BlueXP.

Filtro	Dettagli
Stato dell'analisi	Selezionare un'opzione per visualizzare l'elenco dei file in attesa di prima scansione, completati in scansione, in attesa di scansione o che non sono stati sottoposti a scansione.
Evento di analisi della scansione	Selezionare se si desidera visualizzare i file che non sono stati classificati perché la classificazione BlueXP non ha potuto ripristinare l'ultimo tempo di accesso o i file che sono stati classificati anche se la classificazione BlueXP non ha potuto ripristinare l'ultimo tempo di accesso.

"Vedere i dettagli sull'indicatore data/ora dell'ultimo accesso" Per ulteriori informazioni sugli elementi visualizzati nella pagina di analisi durante il filtraggio utilizzando l'evento di analisi scansione.

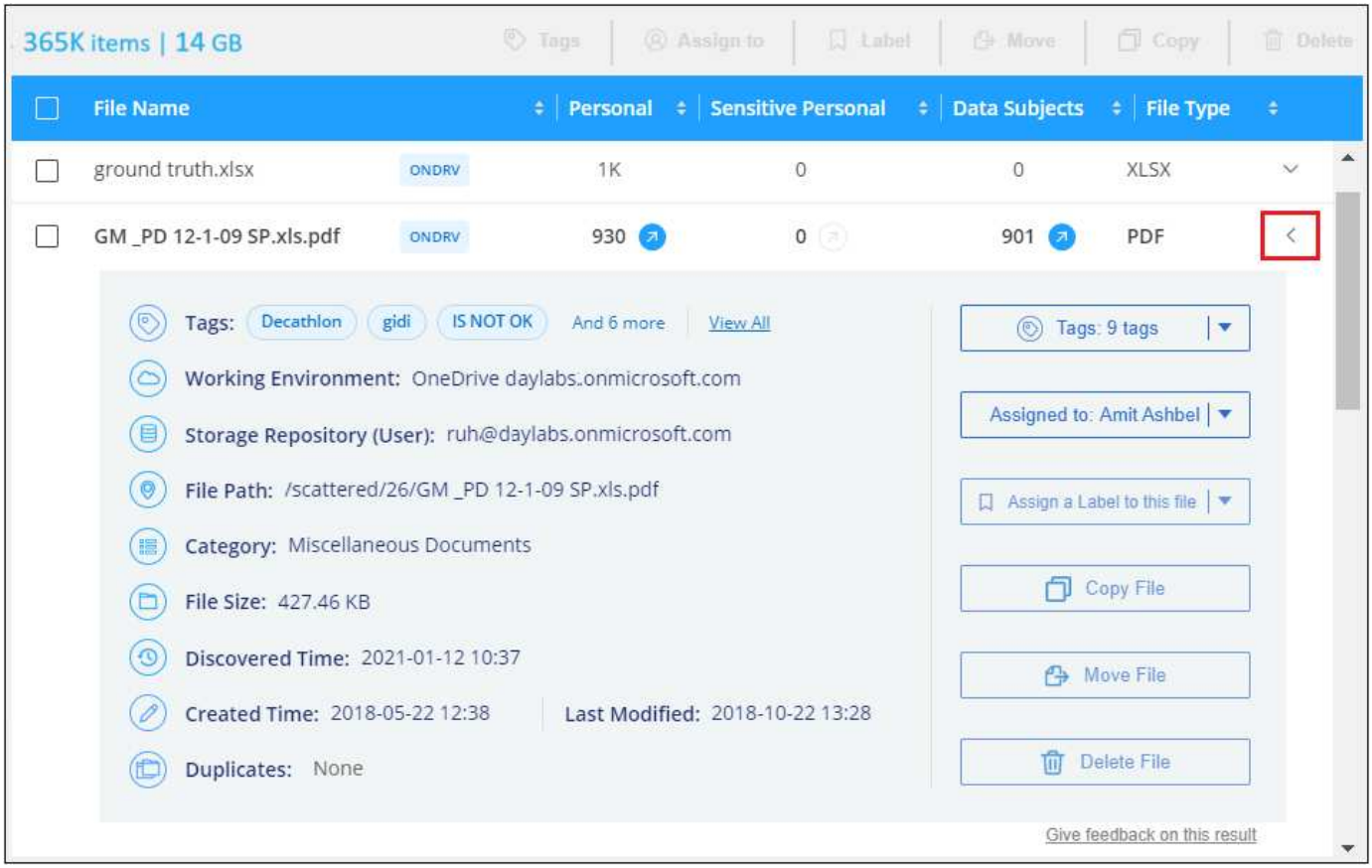
Filtra i dati in base ai duplicati

Utilizzare il seguente filtro per visualizzare i file duplicati nello storage.

Filtro	Dettagli
Duplicati	Selezionare se il file viene duplicato nei repository.

Visualizzare i metadati dei file

Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per visualizzare i metadati del file in un singolo file.



Oltre a mostrare l'ambiente di lavoro e il volume in cui si trova il file, i metadati mostrano molte più informazioni, tra cui le autorizzazioni del file, il proprietario del file, l'eventuale presenza di duplicati del file e l'etichetta AIP assegnata (se disponibile) "AIP integrato nella classificazione BlueXP"). Queste informazioni sono utili se stai pensando di "Creare policy" perché è possibile visualizzare tutte le informazioni che è possibile utilizzare per filtrare i dati.

Tenere presente che non tutte le informazioni sono disponibili per tutte le origini dati, ma solo quelle appropriate per tale origine. Ad esempio, il nome del volume, le autorizzazioni e le etichette AIP non sono rilevanti per i file di database.

Quando si visualizzano i dettagli di un singolo file, è possibile eseguire alcune operazioni sul file:

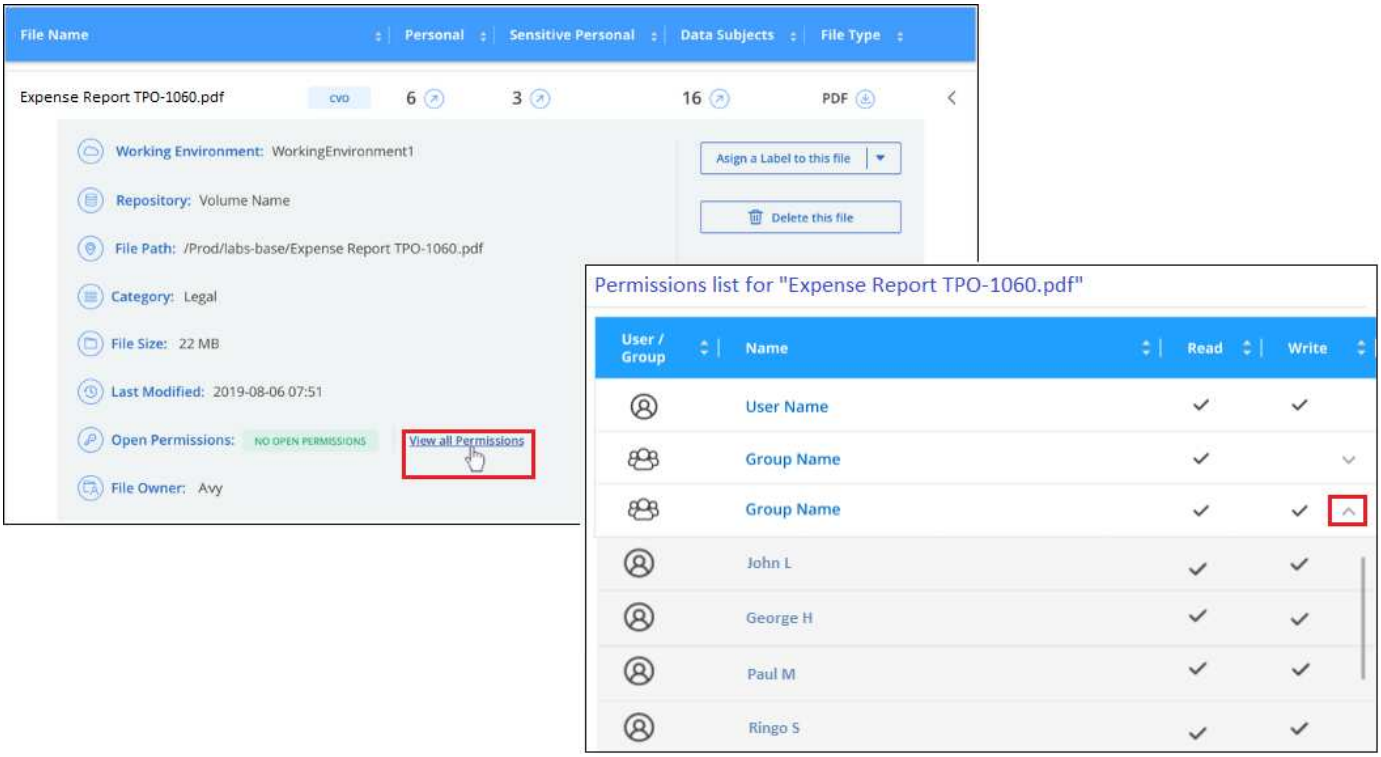
- È possibile spostare o copiare il file in qualsiasi condivisione NFS. Vedere "Spostamento dei file di origine in una condivisione NFS" e. "Copia dei file di origine in una condivisione NFS" per ulteriori informazioni.
- È possibile eliminare il file. Vedere "Eliminazione dei file di origine" per ulteriori informazioni.
- È possibile assegnare un determinato Stato al file. Vedere "Applicazione di tag" per ulteriori informazioni.
- È possibile assegnare il file a un utente BlueXP per essere responsabile di eventuali azioni di follow-up che devono essere eseguite sul file. Vedere "Assegnazione di utenti a un file" per ulteriori informazioni.
- Se sono state integrate etichette AIP con classificazione BlueXP, è possibile assegnare un'etichetta a questo file o modificarla se già esistente. Vedere "Assegnazione manuale delle etichette AIP" per ulteriori informazioni.

Visualizzare le autorizzazioni per file e directory

Per visualizzare un elenco di tutti gli utenti o gruppi che hanno accesso a un file o a una directory e i tipi di autorizzazioni di cui dispongono, fare clic su **Visualizza tutte le autorizzazioni**. Questo pulsante è disponibile

solo per i dati in condivisioni CIFS, SharePoint Online, SharePoint on-premise e OneDrive.

Si noti che se vengono visualizzati i SID (Security Identifier) invece dei nomi di utenti e gruppi, è necessario integrare Active Directory nella classificazione BlueXP. "Scopri come farlo".



Fare clic su ⌄ per consentire a qualsiasi gruppo di visualizzare l'elenco degli utenti che fanno parte del gruppo.

Inoltre, È possibile fare clic sul nome di un utente o di un gruppo e viene visualizzata la pagina di analisi con il nome dell'utente o del gruppo inserito nel filtro "User / Group Permissions" (autorizzazioni utente / gruppo), in modo da visualizzare tutti i file e le directory a cui l'utente o il gruppo ha accesso.

Verificare la presenza di file duplicati nei sistemi di storage

È possibile visualizzare se i file duplicati vengono memorizzati nei sistemi storage. Ciò è utile se si desidera identificare le aree in cui è possibile risparmiare spazio di storage. Può anche essere utile assicurarsi che alcuni file con autorizzazioni specifiche o informazioni sensibili non vengano duplicati inutilmente nei sistemi di storage.

Tutti i file (esclusi i database) di dimensioni pari o superiori a 1 MB e contenenti informazioni personali o riservate vengono confrontati per verificare se sono presenti duplicati. È possibile utilizzare i filtri della pagina di analisi "dimensione file" insieme a "duplicati" per vedere quali file di un determinato intervallo di dimensioni sono duplicati nell'ambiente in uso.

La classificazione BlueXP utilizza la tecnologia di hashing per determinare i file duplicati. Se un file ha lo stesso codice hash di un altro file, possiamo essere sicuri al 100% che i file siano duplicati esatti - anche se i nomi dei file sono diversi.

È possibile scaricare l'elenco dei file duplicati e inviarlo all'amministratore dello storage in modo che possa decidere quali file, se presenti, possono essere cancellati. Oppure è possibile "eliminare il file" se si è sicuri che non è necessaria una versione specifica del file.

Visualizzare tutti i file duplicati

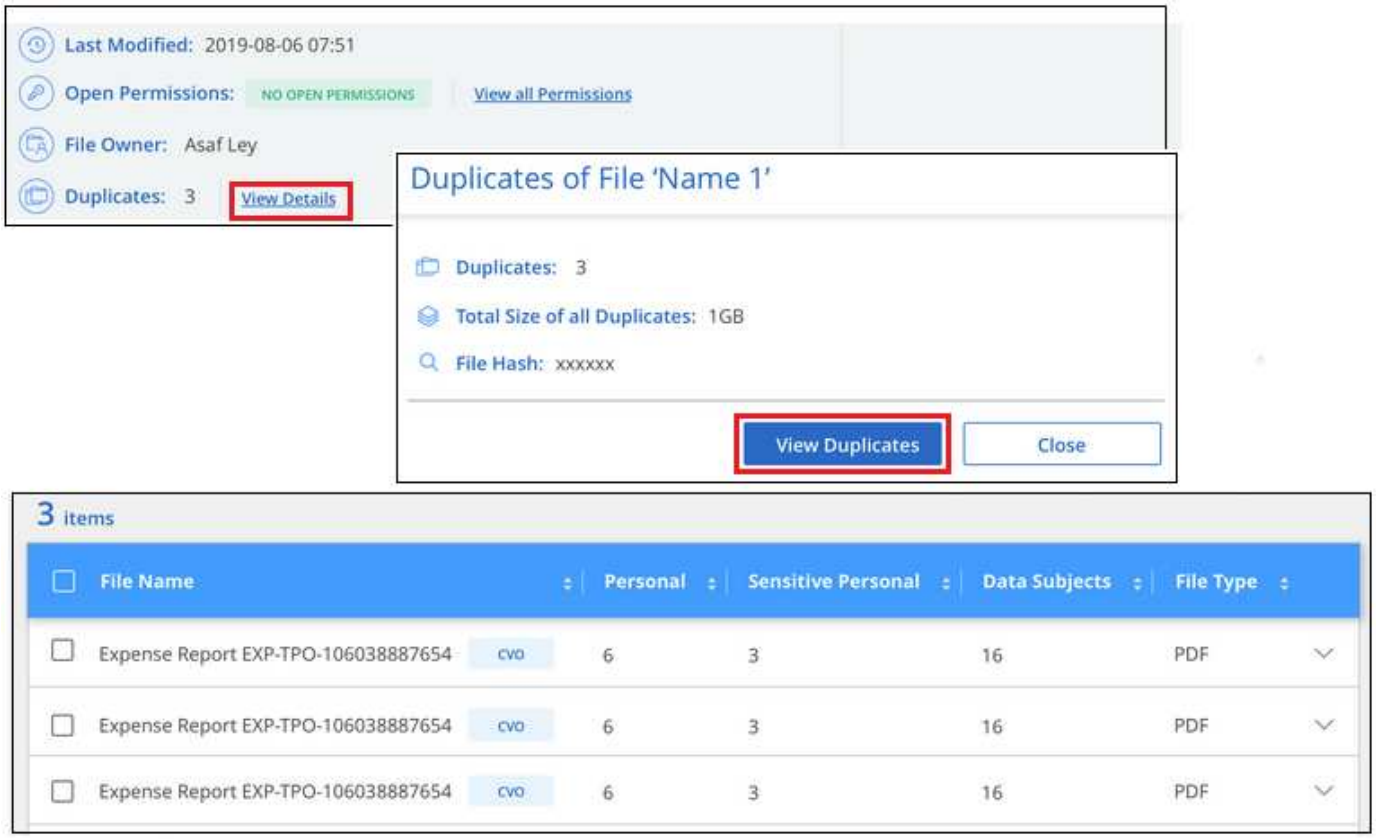
Se si desidera un elenco di tutti i file duplicati negli ambienti di lavoro e nelle origini dati in scansione, è possibile utilizzare il filtro **duplicati > ha duplicati** nella pagina analisi dati.

Tutti i file duplicati vengono visualizzati nella pagina risultati.

Visualizzare se un file specifico è duplicato

Se si desidera vedere se un singolo file ha duplicati, fare clic su nel riquadro risultati analisi dati ⌄ per visualizzare i metadati del file in un singolo file. Se sono presenti duplicati di un determinato file, queste informazioni vengono visualizzate accanto al campo *duplicati*.

Per visualizzare l'elenco dei file duplicati e la loro posizione, fare clic su **View Details** (Visualizza dettagli). Nella pagina successiva, fare clic su **View Duplicates** (Visualizza duplicati) per visualizzare i file nella pagina di analisi.



È possibile utilizzare il valore "hash del file" fornito in questa pagina e immetterlo direttamente nella pagina di analisi per cercare un file duplicato specifico in qualsiasi momento, oppure utilizzarlo in un criterio.

Report sull'analisi dei dati

Il Data Investigation Report (Report analisi dati) è un download del contenuto filtrato della pagina Data Investigation (analisi dati).

Il rapporto è disponibile in due formati diversi:

- Come file .CSV che è possibile salvare sul computer locale.

  Questo rapporto può includere un massimo di 10.000 righe di dati.

- Come file .JSON esportato in una condivisione NFS.

  Se sono presenti più di 250.000 righe di dati, vengono creati file .JSON aggiuntivi.

  Quando si esporta in una condivisione file, assicurarsi che la classificazione BlueXP disponga delle autorizzazioni corrette per l'accesso all'esportazione.

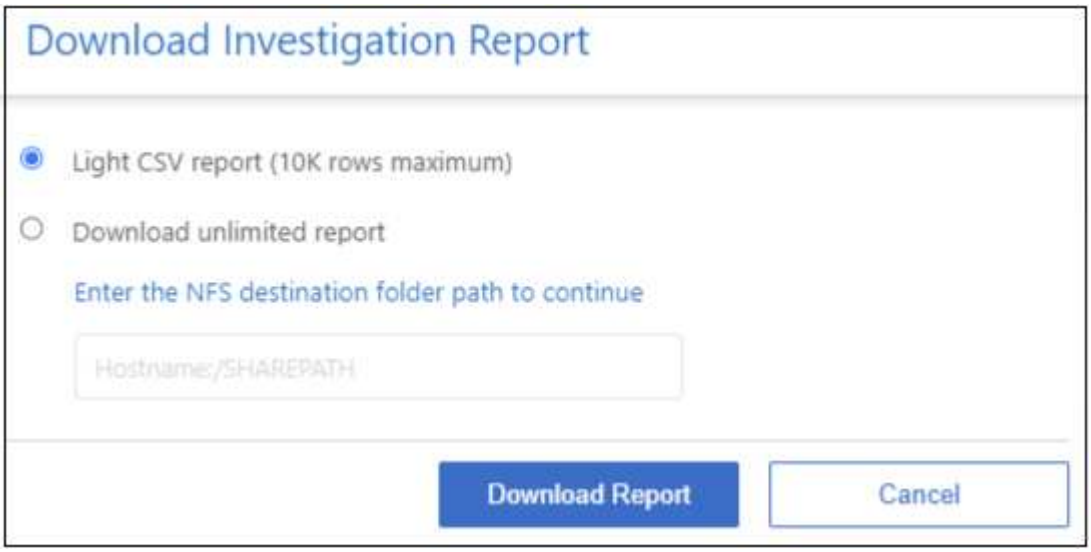
Se la classificazione BlueXP sta scansionando file (dati non strutturati), directory (cartelle e condivisioni di file) e database (dati strutturati), possono essere scaricati fino a tre file di report.

Generare il rapporto analisi dati

Fasi

1. Dalla pagina Data Investigation (analisi dati), fare clic su nella parte superiore destra della pagina.
2. Selezionare se si desidera scaricare un report .CSV o .JSON dei dati e fare clic su **Download Report**.

   Quando si seleziona un report .JSON, inserire il nome della condivisione NFS in cui verrà scaricato il report nel formato `<host_name>:/<share_path>`.



Risultato

Viene visualizzata una finestra di dialogo che indica che i report sono in fase di download.

È possibile visualizzare lo stato di avanzamento della generazione di report JSON in "Riquadro Actions Status (Stato azioni)".

Contenuto di ciascun report di analisi dei dati

Il **Report dati file non strutturati** include le seguenti informazioni sui file:

- Nome del file
- Tipo di ubicazione

- Nome dell’ambiente di lavoro
- Repository di storage (ad esempio, un volume, un bucket, condivisioni)
- Tipo di repository
- Percorso del file
- Tipo di file
- Dimensioni file (in MB)
- Ora di creazione
- Ultima modifica
- Ultimo accesso
- Proprietario del file
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Autorizzazioni aperte
- Errore analisi scansione
- Data di rilevamento dell’eliminazione

  Una data di rilevamento dell’eliminazione identifica la data in cui il file è stato cancellato o spostato. In questo modo è possibile identificare quando sono stati spostati file sensibili. I file cancellati non fanno parte del numero di file visualizzato nella dashboard o nella pagina di analisi. I file vengono visualizzati solo nei report CSV.

Il **Report dati directory non strutturate** include le seguenti informazioni relative alle cartelle e alle condivisioni di file:

- Tipo di ambiente di lavoro
- Nome dell’ambiente di lavoro
- Nome directory
- Repository di storage (ad esempio, una cartella o condivisioni di file)
- Proprietario directory
- Ora di creazione
- Tempo scoperto
- Ultima modifica
- Ultimo accesso
- Autorizzazioni aperte
- Tipo di directory

Il **Structured Data Report** include le seguenti informazioni sulle tabelle di database:

- DB Nome tabella
- Tipo di ubicazione

- Nome dell'ambiente di lavoro
- Repository di storage (ad esempio, uno schema)
- Numero di colonne
- Numero di righe
- Informazioni personali
- Informazioni personali sensibili

Organizzare i dati privati

La classificazione BlueXP offre diversi modi per gestire e organizzare i dati privati. In questo modo è più semplice visualizzare i dati più importanti per te.

- Se si è abbonati a. "Azure Information Protection (AIP)" Per classificare e proteggere i file, è possibile utilizzare la classificazione BlueXP per gestire le etichette AIP.

> La release di dicembre 2023 (v1.26.6) ha temporaneamente rimosso l'opzione di integrare i dati utilizzando le etichette AIP (Azure Information Protection).

- È possibile aggiungere tag ai file che si desidera contrassegnare per l'organizzazione o per alcuni tipi di follow-up.
- È possibile assegnare un utente BlueXP a un file specifico o a più file, in modo che la persona possa essere responsabile della gestione del file.
- Utilizzando la funzionalità "Policy" è possibile creare query di ricerca personalizzate in modo da visualizzare facilmente i risultati facendo clic su un pulsante.
- È possibile inviare avvisi e-mail agli utenti di BlueXP o a qualsiasi altro indirizzo e-mail, quando alcuni criteri critici restituiscono risultati.

> Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.

È necessario utilizzare tag o etichette?

Di seguito è riportato un confronto tra il tag di classificazione BlueXP e l'etichettatura Azure Information Protection.

Tag	Etichette
I tag di file sono parte integrante della classificazione BlueXP.	Richiede l'iscrizione a Azure Information Protection (AIP).
Il tag viene conservato solo nel database di classificazione BlueXP e non viene scritto nel file. Il file non viene modificato, né il file a cui si accede o modificato.	L'etichetta fa parte del file e quando l'etichetta cambia, il file cambia. Questa modifica modifica modifica modifica anche i tempi di accesso e modifica del file.
È possibile avere più tag su un singolo file.	È possibile avere un'etichetta su un singolo file.

Tag	Etichette
Il tag può essere utilizzato per l'azione di classificazione interna di BlueXP, come copia, spostamento, eliminazione, esecuzione di un criterio, ecc.	Altri sistemi in grado di leggere il file possono vedere l'etichetta, che può essere utilizzata per un'ulteriore automazione.
Viene utilizzata solo una singola chiamata API per verificare se un file ha un tag.	

Categorizzare i dati utilizzando le etichette AIP

È possibile gestire le etichette AIP nei file che la classificazione BlueXP sta analizzando, se si è abbonati "Azure Information Protection (AIP)". AIP consente di classificare e proteggere documenti e file applicando etichette ai contenuti. La classificazione BlueXP consente di visualizzare le etichette già assegnate ai file, aggiungere etichette ai file e modificare le etichette quando esiste già un'etichetta.

La classificazione BlueXP supporta le etichette AIP nei seguenti tipi di file: .DOC, .DOCX, .PDF, .PPTX, .XLS, XLSX.

- Al momento non è possibile modificare le etichette in file di dimensioni superiori a 30 MB. Per gli account OneDrive, SharePoint e Google Drive, la dimensione massima del file è di 4 MB.
- Se un file ha un'etichetta che non esiste più in AIP, la classificazione BlueXP lo considera come un file senza un'etichetta.
- Se la classificazione BlueXP è stata implementata in un'area governativa o in una posizione on-premise che non dispone di accesso a Internet (nota anche come sito oscuro), la funzionalità dell'etichetta AIP non è disponibile.

Integrare le etichette AIP nell'area di lavoro

Prima di poter gestire le etichette AIP, è necessario integrare la funzionalità dell'etichetta AIP nella classificazione BlueXP accedendo all'account Azure esistente. Una volta attivata, è possibile gestire le etichette AIP all'interno dei file per tutti "origini dati" Nello spazio di lavoro BlueXP.

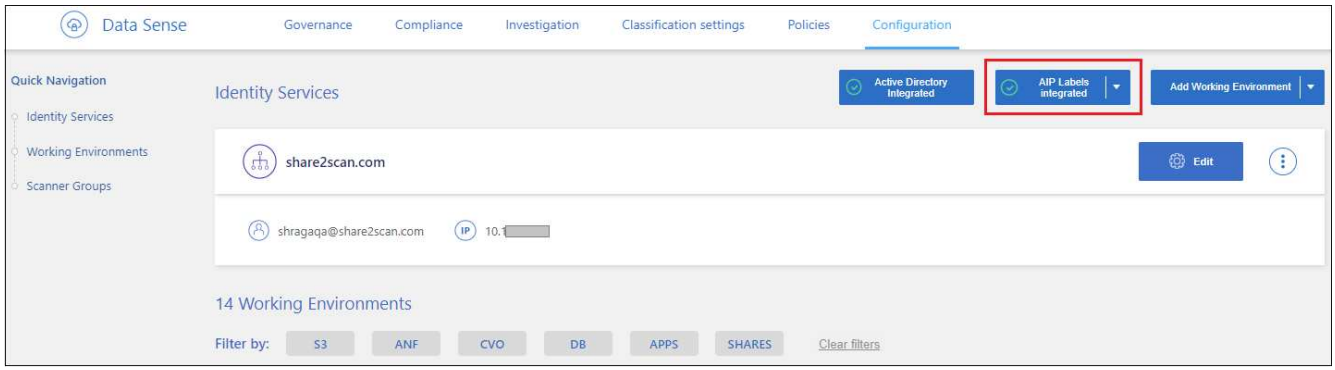
Requisiti

- È necessario disporre di un account e di una licenza di Azure Information Protection.
- È necessario disporre delle credenziali di accesso per l'account Azure.
- Se intendi modificare le etichette nei file che risiedono nei bucket Amazon S3, assicurati che l'autorizzazione sia `s3:PutObject` È incluso nel ruolo IAM. Vedere "Impostazione del ruolo IAM".

Fasi

1. Dalla pagina di configurazione della classificazione BlueXP, fare clic su **integra etichette AIP**.

2. Nella finestra di dialogo integra etichette AIP, fare clic su **Accedi ad Azure**.
3. Nella pagina Microsoft visualizzata, selezionare l'account e immettere le credenziali richieste.
4. Tornare alla scheda classificazione BlueXP e viene visualizzato il messaggio "*AIP Labels Were successfully Integrated with the account <account_name>*" (le etichette AIP sono state integrate correttamente con l'account BlueXP_).
5. Fare clic su **Close** (Chiudi) per visualizzare il testo *AIP Labels Integrated* (etichette AIP integrate) nella parte superiore della pagina.



Risultato

È possibile visualizzare e assegnare le etichette AIP dal riquadro dei risultati della pagina di analisi. È inoltre possibile assegnare etichette AIP ai file utilizzando i criteri.

Visualizzare le etichette AIP nei file

È possibile visualizzare l'etichetta AIP corrente assegnata a un file.

Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.

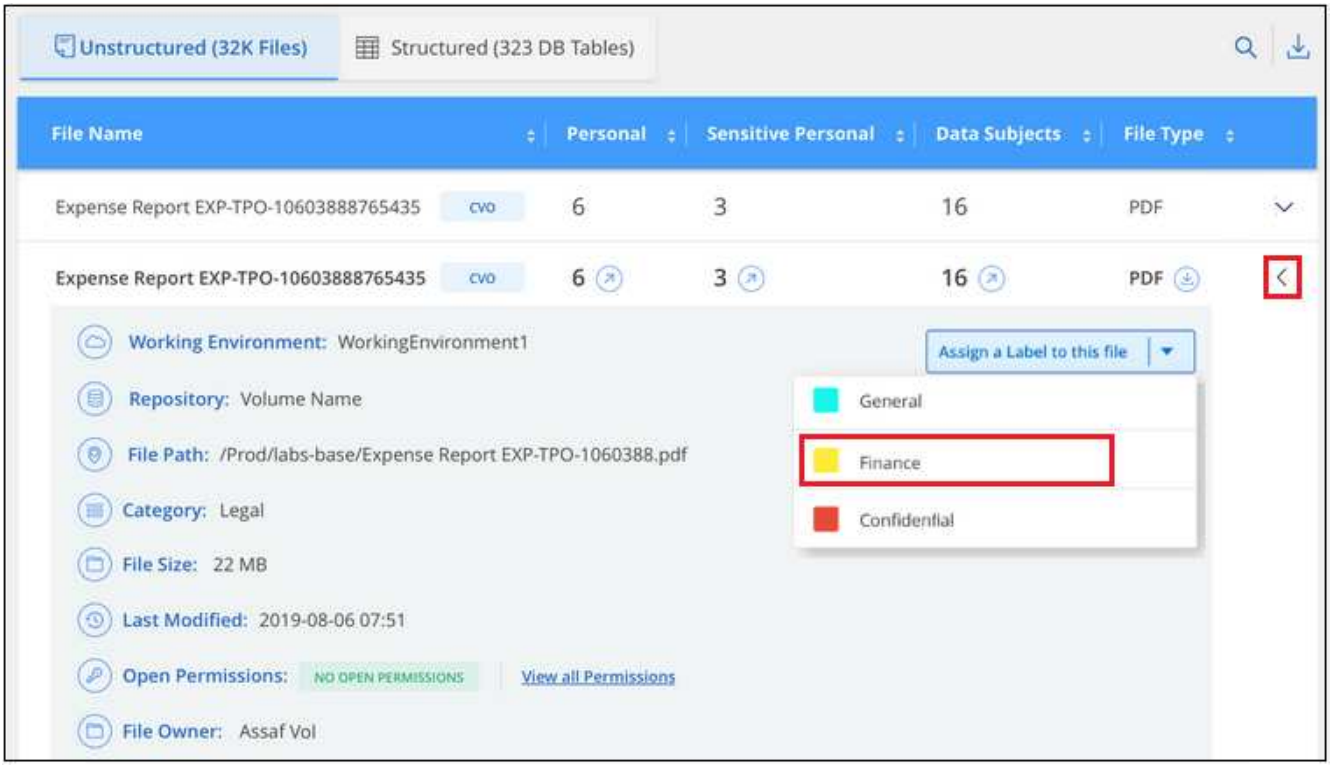
Assegnare manualmente le etichette AIP

È possibile aggiungere, modificare e rimuovere le etichette AIP dai file utilizzando la classificazione BlueXP.

Per assegnare un'etichetta AIP a un singolo file, procedere come segue.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.



2. Fare clic su **Assegna un'etichetta a questo file**, quindi selezionare l'etichetta.

   L'etichetta viene visualizzata nei metadati del file.

Per assegnare un'etichetta AIP a più file, procedere come segue. Nota: È possibile assegnare un'etichetta AIP a un massimo di 20 file alla volta (una pagina nell'interfaccia utente).

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da etichettare.

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (☑ Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (☑ File Name).

2. Dalla barra dei pulsanti, fare clic su **etichetta** e selezionare l'etichetta AIP:

L'etichetta AIP viene aggiunta ai metadati di tutti i file selezionati.

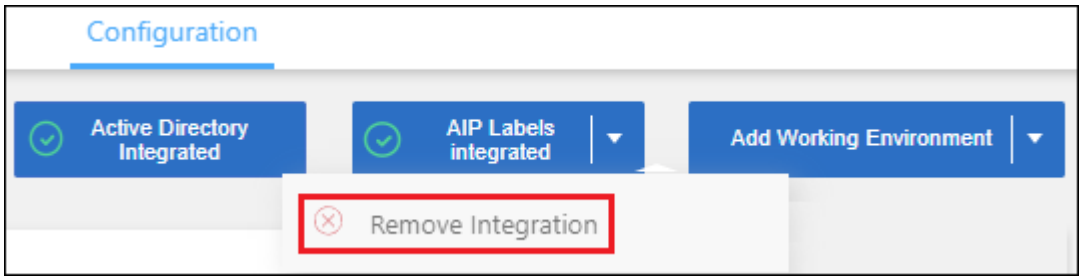
Rimuovere l'integrazione AIP

Se non si desidera più gestire le etichette AIP nei file, è possibile rimuovere l'account AIP dall'interfaccia di classificazione BlueXP.

Si noti che non vengono apportate modifiche alle etichette aggiunte utilizzando la classificazione BlueXP. Le etichette presenti nei file rimarranno quelle attualmente esistenti.

Fasi

1. Dalla pagina *Configuration*, fare clic su **AIP Labels Integrated > Remove Integration** (etichette AIP integrate > Rimuovi integrazione).



2. Fare clic su **Remove Integration** (Rimuovi integrazione) nella finestra di dialogo di conferma.

Applicare i tag per gestire i file digitalizzati

È possibile aggiungere un tag ai file che si desidera contrassegnare per alcuni tipi di follow-up. Ad esempio, è possibile che siano stati trovati alcuni file duplicati e si desidera eliminarne uno, ma è necessario controllare quale file eliminare. È possibile aggiungere un tag "Check to delete" al file in modo da sapere che questo file richiede una ricerca e un qualche tipo di azione futura.

La classificazione BlueXP consente di visualizzare i tag assegnati ai file, aggiungere o rimuovere tag dai file e modificare il nome o eliminare un tag esistente.

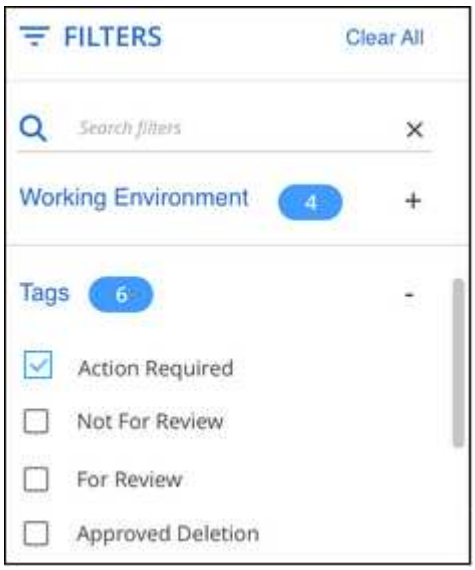
Tenere presente che il tag non viene aggiunto al file allo stesso modo in cui le etichette AIP fanno parte dei metadati del file. Il tag è appena visto dagli utenti di BlueXP che utilizzano la classificazione BlueXP in modo da poter vedere se un file deve essere cancellato o controllato per un certo tipo di follow-up.

I tag assegnati ai file nella classificazione BlueXP non sono correlati ai tag che è possibile aggiungere alle risorse, come volumi o istanze di macchine virtuali. I tag di classificazione BlueXP vengono applicati a livello di file.

Consente di visualizzare i file a cui sono stati applicati determinati tag

È possibile visualizzare tutti i file con tag specifici assegnati.

1. Fare clic sulla scheda **Investigation** dalla classificazione BlueXP.
2. Nella pagina Data Investigation (analisi dati), fare clic su **Tags** nel riquadro Filters (filtri), quindi selezionare i tag richiesti.



Il riquadro dei risultati dell'analisi visualizza tutti i file a cui sono stati assegnati i tag.

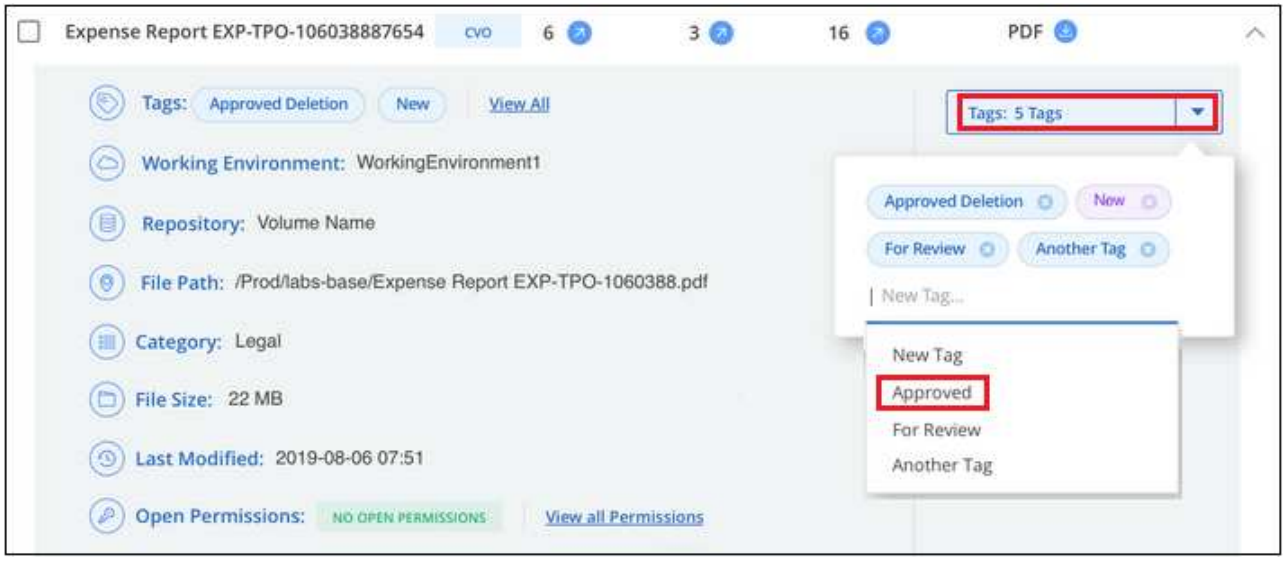
Assegnare tag ai file

È possibile aggiungere tag a un singolo file o a un gruppo di file.

Per aggiungere un tag a un singolo file:

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.
2. Fare clic sul campo **Tag** per visualizzare i tag attualmente assegnati.
3. Aggiungere il tag o i tag:
   - Per assegnare un tag esistente, fare clic nel campo **New Tag…** e iniziare a digitare il nome del tag. Quando viene visualizzato il tag desiderato, selezionarlo e premere **Invio**.
   - Per creare un nuovo tag e assegnarlo al file, fare clic nel campo **New Tag…**, inserire il nome del nuovo tag e premere **Invio**.



Il tag viene visualizzato nei metadati del file.

Per aggiungere un tag a più file:

Fasi

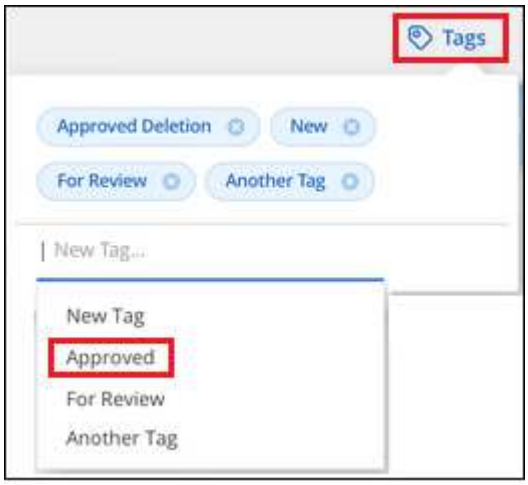
1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da contrassegnare.

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
   - Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

     È possibile applicare tag a un massimo di 100.000 file alla volta.

2. Dalla barra dei pulsanti, fare clic su **Tag** per visualizzare i tag attualmente assegnati.
3. Aggiungere il tag o i tag:
   - Per assegnare un tag esistente, fare clic nel campo **New Tag…** e iniziare a digitare il nome del tag. Quando viene visualizzato il tag desiderato, selezionarlo e premere **Invio**.

- Per creare un nuovo tag e assegnarlo al file, fare clic nel campo **New Tag…**, inserire il nome del nuovo tag e premere **Invio**.



4. Approva l'aggiunta dei tag nella finestra di dialogo di conferma e i tag vengono aggiunti ai metadati per tutti i file selezionati.

Eliminare i tag dai file

Puoi eliminare un tag se non ne hai più bisogno.

Fare clic sulla * x* per un tag esistente.

Se sono stati selezionati più file, il tag viene rimosso da tutti i file.

Assegnare agli utenti la gestione di determinati file

È possibile assegnare un utente BlueXP a un file specifico o a più file, in modo che la persona possa essere responsabile di eventuali azioni di follow-up che devono essere eseguite sul file. Questa funzionalità viene spesso utilizzata con la funzione per aggiungere tag di stato personalizzati a un file.

Ad esempio, è possibile che il file contenga alcuni dati personali che consentono a troppi utenti di accedere in lettura e scrittura (autorizzazioni aperte). È quindi possibile assegnare il tag di stato "Change permissions" e assegnare questo file all'utente "Joan Smith" in modo che possa decidere come risolvere il problema. Una volta risolto il problema, è possibile modificare il tag Status (Stato) in "Completed" (completato).

Si noti che il nome utente non viene aggiunto al file come parte dei metadati del file, ma viene visualizzato solo dagli utenti BlueXP quando si utilizza la classificazione BlueXP.

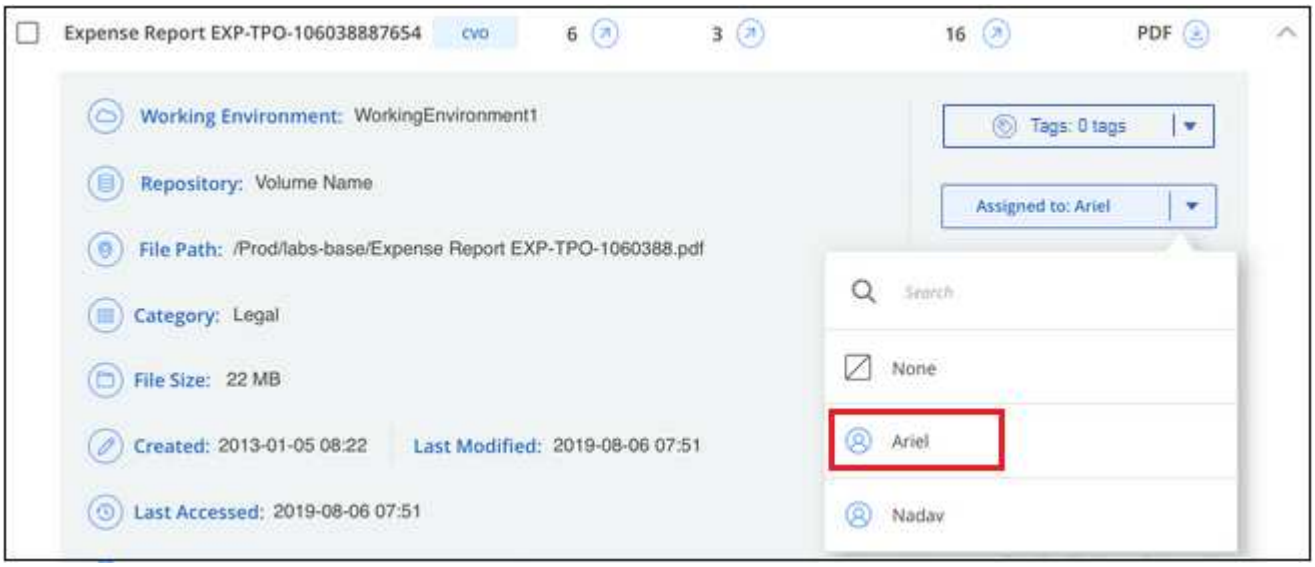
Un nuovo filtro nella pagina di analisi consente di visualizzare facilmente tutti i file con la stessa persona nel campo "assegnato a".

Per assegnare un utente a un singolo file, procedere come segue.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), fare clic su ⌄ per espandere i dettagli dei metadati del file.

2. Fare clic sul campo **assegnato a** e selezionare il nome utente.



Il nome utente viene visualizzato nei metadati del file.

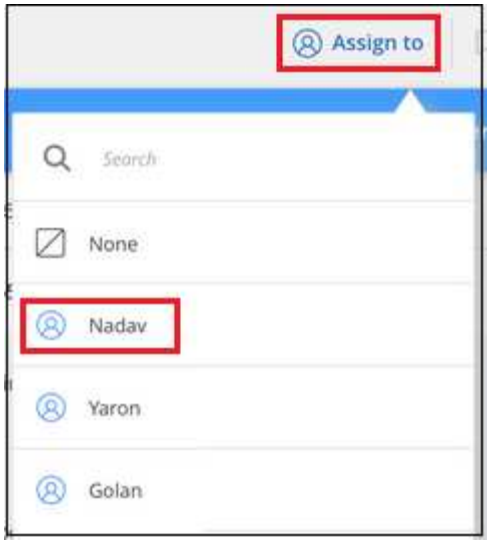
Per assegnare un utente a più file, procedere come segue. Nota: È possibile assegnare un utente a un massimo di 20 file alla volta (una pagina nell'interfaccia utente).

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file che si desidera assegnare a un utente.

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).

2. Dalla barra dei pulsanti, fare clic su **Assegna a** e selezionare il nome utente:



L'utente viene aggiunto ai metadati per tutti i file selezionati.

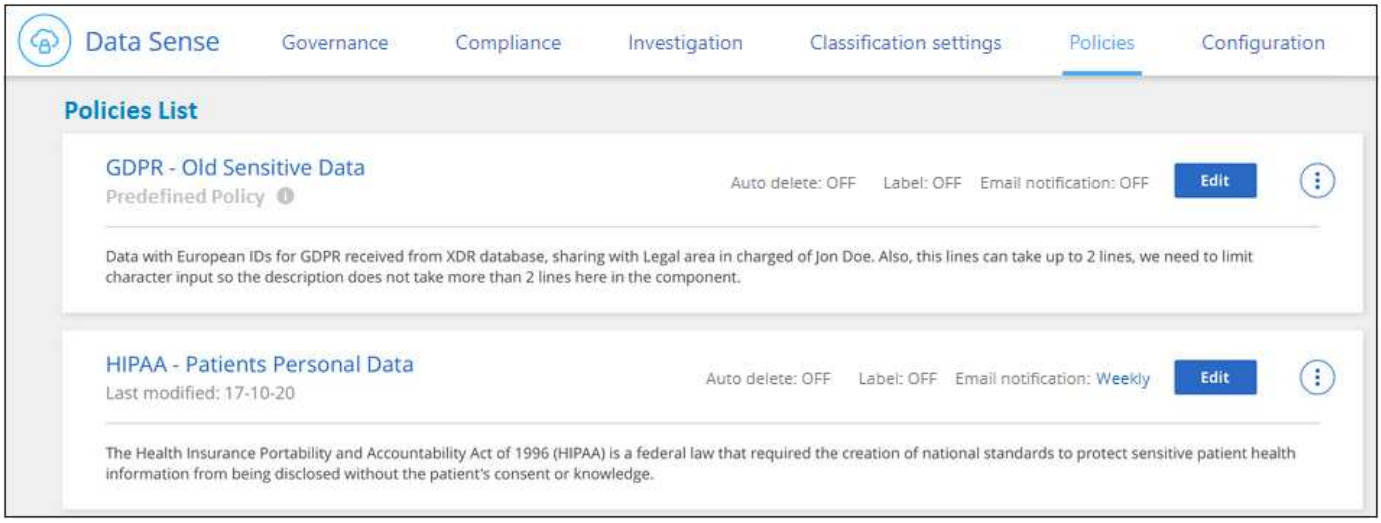
Assegnare policy ai dati

Le policy sono come un elenco preferito di filtri personalizzati che forniscono i risultati della ricerca nella pagina di analisi per le query di conformità più frequenti. La classificazione BlueXP offre una serie di policy predefinite basate sulle richieste più comuni dei clienti. È possibile creare policy personalizzate che forniscano risultati per ricerche specifiche della propria organizzazione.

Le policy offrono le seguenti funzionalità:

- Policy predefinite NetApp in base alle richieste degli utenti
- Possibilità di creare policy personalizzate
- Aprire la pagina delle analisi con i risultati delle policy in un click
- Invia avvisi e-mail agli utenti BlueXP o a qualsiasi altro indirizzo e-mail, quando alcune policy critiche restituiscono risultati, in modo da poter ricevere notifiche per proteggere i tuoi dati
- Assegnare automaticamente le etichette AIP (Azure Information Protection) a tutti i file che corrispondono ai criteri definiti in una policy
- Elimina automaticamente i file (una volta al giorno) quando alcune policy restituiscono risultati, in modo da proteggere automaticamente i dati

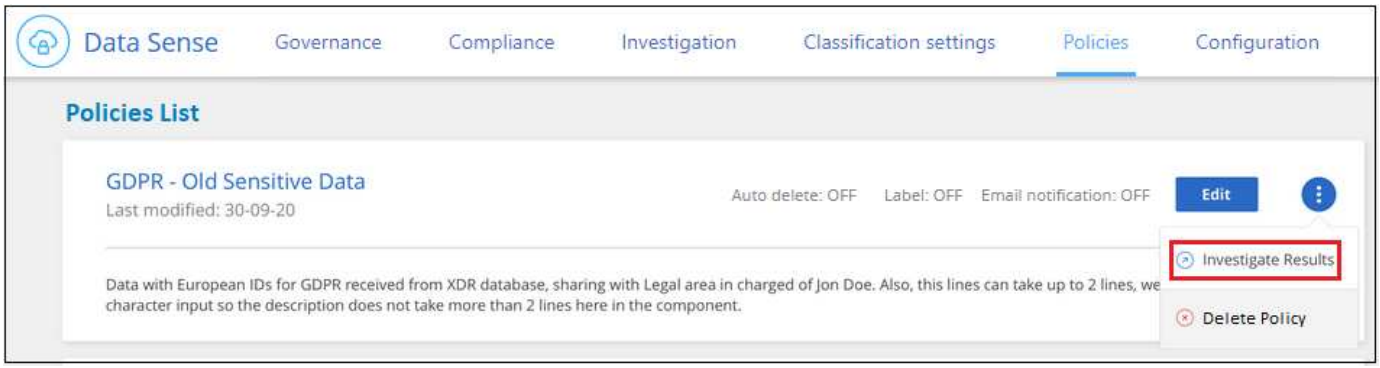
La scheda **Policies** nella dashboard di conformità elenca tutti i criteri predefiniti e personalizzati disponibili in questa istanza della classificazione BlueXP.



Inoltre, i criteri vengono visualizzati nell'elenco dei filtri della pagina di analisi.

Visualizzare i risultati dei criteri nella pagina di analisi

Per visualizzare i risultati di un criterio nella pagina analisi, fare clic su ⋮ Per una policy specifica, quindi selezionare **esamina risultati**.



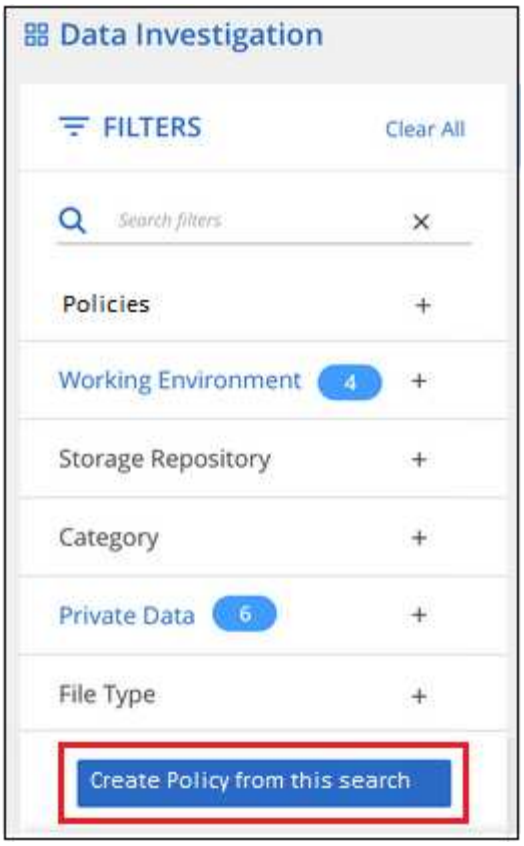
Creare criteri personalizzati

È possibile creare policy personalizzate che forniscano risultati per le ricerche specifiche della propria organizzazione. I risultati vengono restituiti per tutti i file e le directory (condivisioni e cartelle) che corrispondono ai criteri di ricerca.

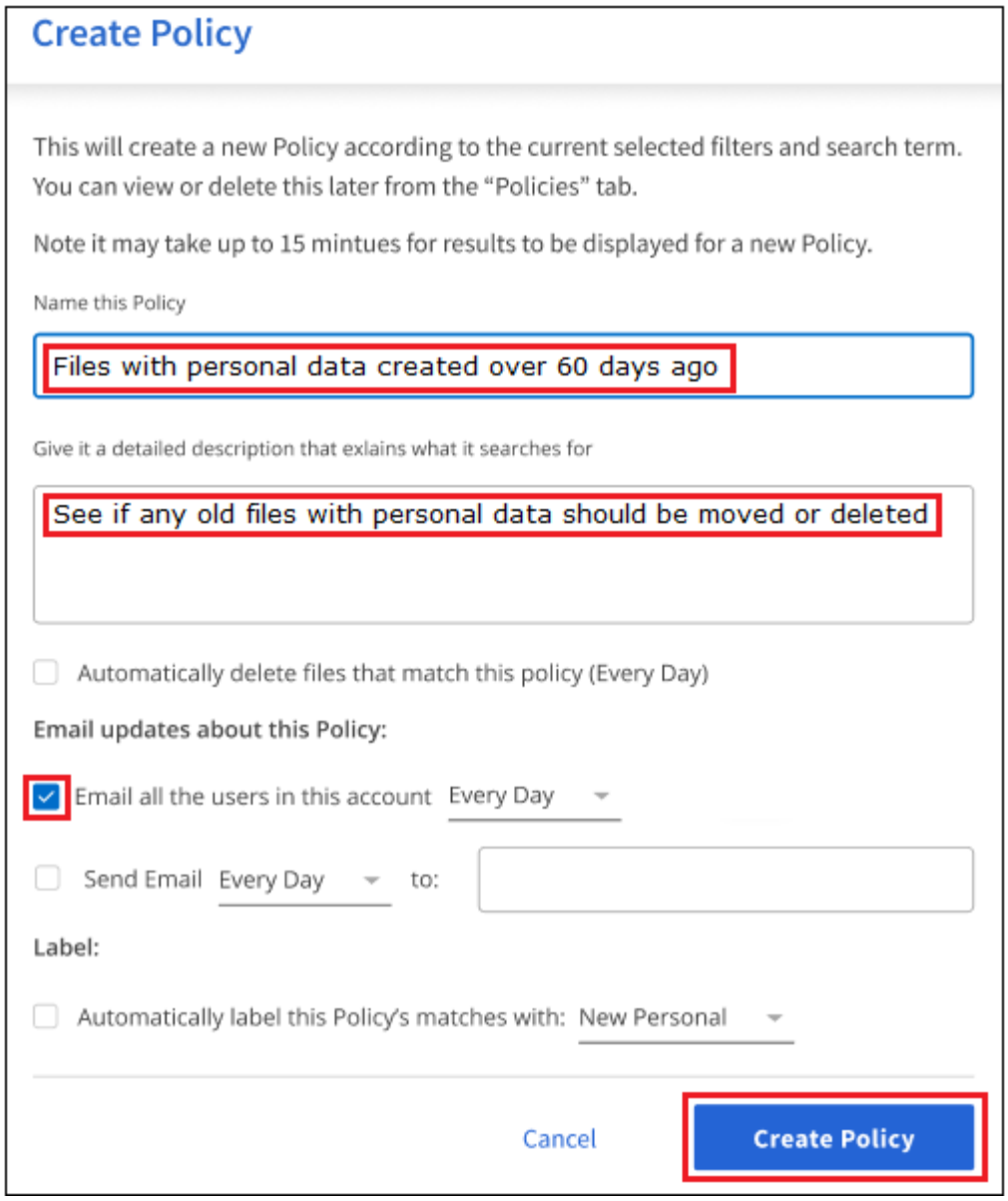
Tenere presente che le azioni per l'eliminazione dei dati e l'assegnazione delle etichette AIP in base ai risultati dei criteri sono valide solo per i file. Le directory che corrispondono ai criteri di ricerca non possono essere eliminate automaticamente o assegnate etichette AIP.

Fasi

1. Dalla pagina Data Investigation (analisi dati), definire la ricerca selezionando tutti i filtri che si desidera utilizzare. Vedere "Filtraggio dei dati nella pagina Data Investigation" per ulteriori informazioni.
2. Una volta che tutte le caratteristiche del filtro sono esattamente come desiderate, fare clic su **Create Policy from this search** (Crea policy da questa ricerca).



3. Assegnare un nome al criterio e selezionare altre azioni che possono essere eseguite dal criterio:
   a. Immettere un nome e una descrizione univoci.
   b. Se si desidera, selezionare la casella per eliminare automaticamente i file che corrispondono ai parametri del criterio. Scopri di più eliminazione dei file di origine mediante un criterio.
   c. Se si desidera inviare e-mail di notifica agli utenti BlueXP nell'account, selezionare la casella di controllo e scegliere l'intervallo di invio dell'e-mail. Scopri di più invio di avvisi e-mail in base ai risultati della policy.
   d. Se si desidera, selezionare la casella se si desidera che le e-mail di notifica vengano inviate ad altri utenti, immettere fino a 20 indirizzi e-mail e scegliere l'intervallo di invio dell'e-mail.
   e. Se si desidera, selezionare la casella per assegnare automaticamente le etichette AIP ai file che corrispondono ai parametri del criterio, quindi selezionare l'etichetta. (Solo se sono già state integrate le etichette AIP. Scopri di più "Etichette AIP".)
   f. Fare clic su **Crea policy**.



Risultato

Il nuovo criterio viene visualizzato nella scheda Criteri.

Invia avvisi e-mail quando vengono trovati dati non conformi

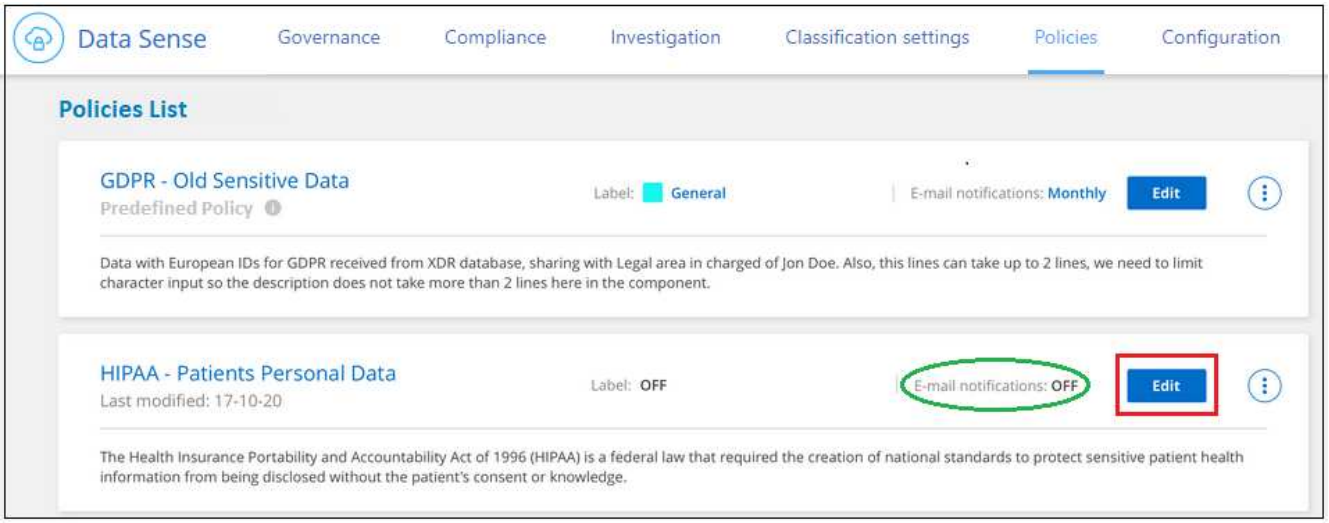
La classificazione BlueXP può inviare avvisi e-mail agli utenti BlueXP del tuo account quando alcune policy critiche restituiscono risultati, in modo da poter ricevere notifiche per proteggere i tuoi dati. È possibile scegliere di inviare le notifiche via email su base giornaliera, settimanale o mensile. Puoi anche scegliere di inviare avvisi e-mail a qualsiasi altro indirizzo e-mail (fino a 20 indirizzi e-mail) non presente nell'account BlueXP.

È possibile configurare questa impostazione quando si crea il criterio o quando si modifica un criterio.

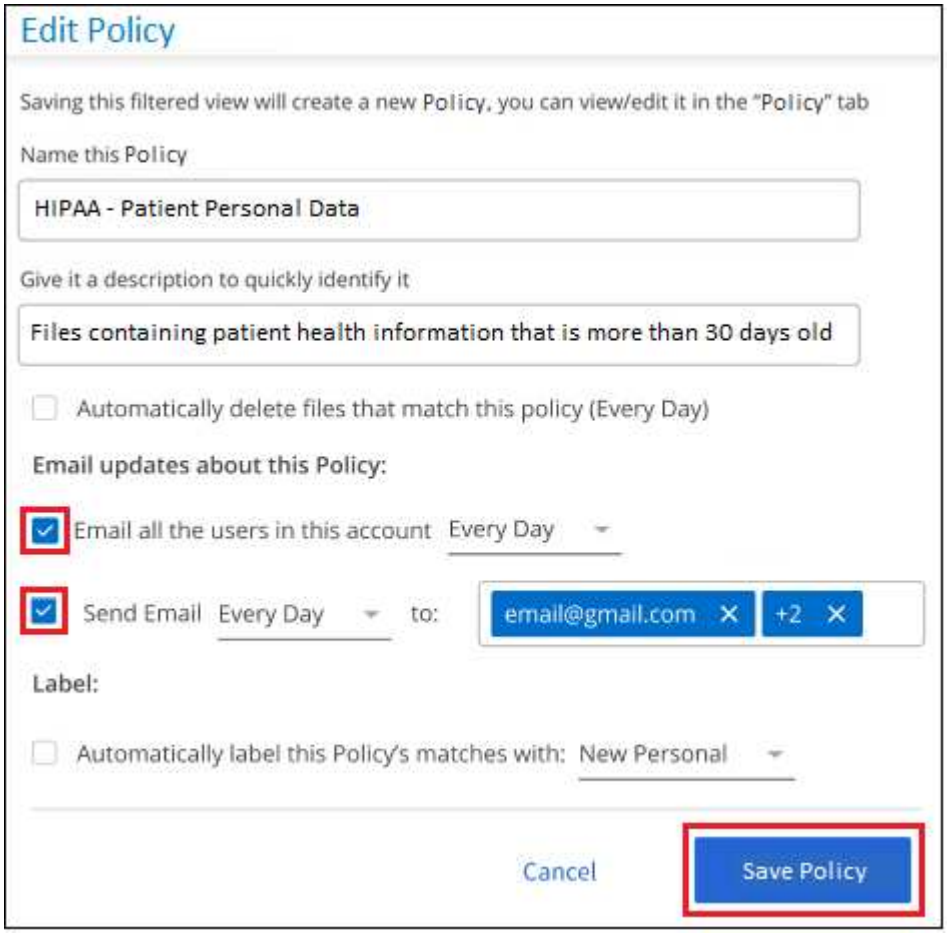
Per aggiungere aggiornamenti e-mail a una policy esistente, procedere come segue.

Fasi

1. Nella pagina elenco criteri, fare clic su **Modifica** per il criterio in cui si desidera aggiungere (o modificare) le impostazioni di posta elettronica.



2. Nella pagina Edit Policy (Modifica policy):
   a. Selezionare la casella "Email all the users in this account" (Invia tutti gli utenti di questo account) se si desidera inviare e-mail di notifica agli utenti dell'account BlueXP e scegliere l'intervallo di invio dell'e-mail (ad esempio, **Every Day**).
   b. Selezionare la casella "Send Email" (Invia e-mail) se si desidera inviare e-mail di notifica ad altri utenti, scegliere l'intervallo di invio e inserire fino a 20 indirizzi e-mail.



3. Fare clic su **Save Policy** (Salva policy) per visualizzare l'intervallo di invio del messaggio nella descrizione del criterio.

Risultato

La prima e-mail viene inviata ora se ci sono risultati dalla policy, ma solo se alcuni file soddisfano i criteri della policy. Non vengono inviate informazioni personali nelle e-mail di notifica. Il messaggio di posta elettronica indica la presenza di file che corrispondono ai criteri del criterio e fornisce un collegamento ai risultati del criterio.

Eliminare automaticamente i file di origine utilizzando i criteri

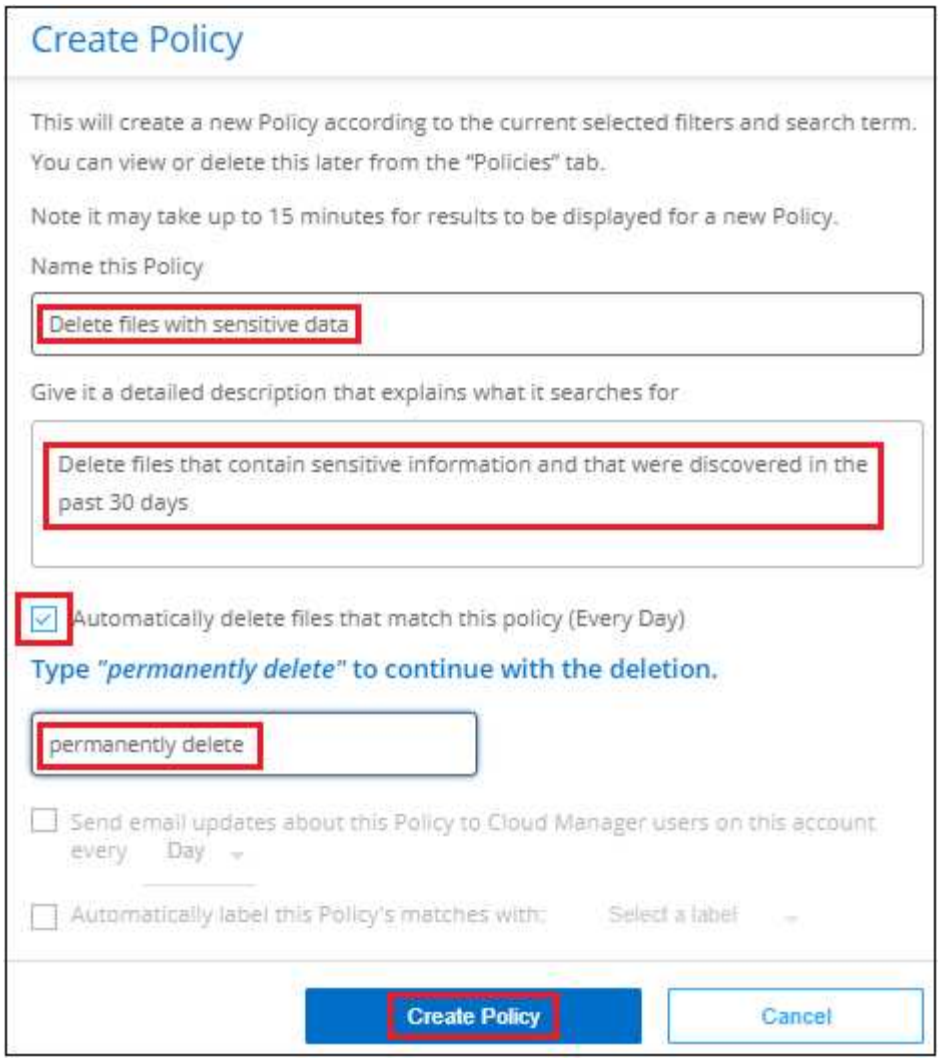
È possibile creare un criterio personalizzato per eliminare i file corrispondenti al criterio. Ad esempio, è possibile eliminare i file che contengono informazioni riservate e che sono stati rilevati dalla classificazione BlueXP negli ultimi 30 giorni.

Solo gli account Admins possono creare una policy per eliminare automaticamente i file.

> Tutti i file che corrispondono alla policy verranno eliminati definitivamente una volta al giorno.

Fasi

1. Dalla pagina Data Investigation (analisi dati), definire la ricerca selezionando tutti i filtri che si desidera utilizzare. Vedere "Filtraggio dei dati nella pagina Data Investigation" per ulteriori informazioni.
2. Una volta che tutte le caratteristiche del filtro sono esattamente come desiderate, fare clic su **Create Policy from this search** (Crea policy da questa ricerca).
3. Assegnare un nome al criterio e selezionare altre azioni che possono essere eseguite dal criterio:
   a. Immettere un nome e una descrizione univoci.
   b. Selezionare la casella "Elimina automaticamente i file corrispondenti a questa policy" e digitare **Elimina definitivamente** per confermare che si desidera che i file vengano eliminati in modo permanente da questa policy.
   c. Fare clic su **Crea policy**.



Risultato

Il nuovo criterio viene visualizzato nella scheda Criteri. I file che corrispondono al criterio vengono cancellati una volta al giorno quando il criterio viene eseguito.

È possibile visualizzare l'elenco dei file che sono stati eliminati in "Riquadro Actions Status (Stato azioni)".

Assegnare automaticamente le etichette AIP con i criteri

È possibile assegnare un'etichetta AIP a tutti i file che soddisfano i criteri del criterio. È possibile specificare l'etichetta AIP durante la creazione del criterio oppure aggiungerla quando si modifica un criterio.

Le etichette vengono aggiunte o aggiornate continuamente nei file mentre la classificazione BlueXP esegue la scansione dei file.

A seconda che un'etichetta sia già applicata a un file e del livello di classificazione dell'etichetta, quando si modifica un'etichetta vengono eseguite le seguenti azioni:

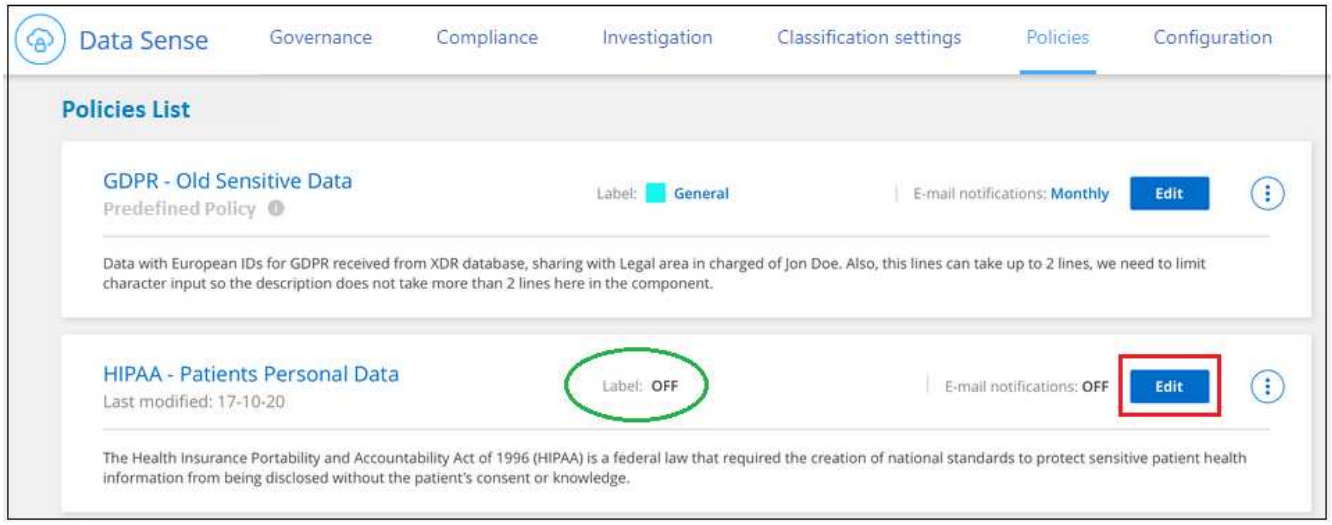
Se il file…	Quindi…
Non ha alcuna etichetta	L'etichetta viene aggiunta

Se il file…	Quindi…
Dispone di un'etichetta con un livello di classificazione inferiore	Viene aggiunta l'etichetta di livello superiore
Dispone di un'etichetta con un livello di classificazione superiore	Viene conservata l'etichetta di livello superiore
Viene assegnata un'etichetta sia manualmente che tramite un criterio	Viene aggiunta l'etichetta di livello superiore
Viene assegnata a due diverse etichette da due policy	Viene aggiunta l'etichetta di livello superiore

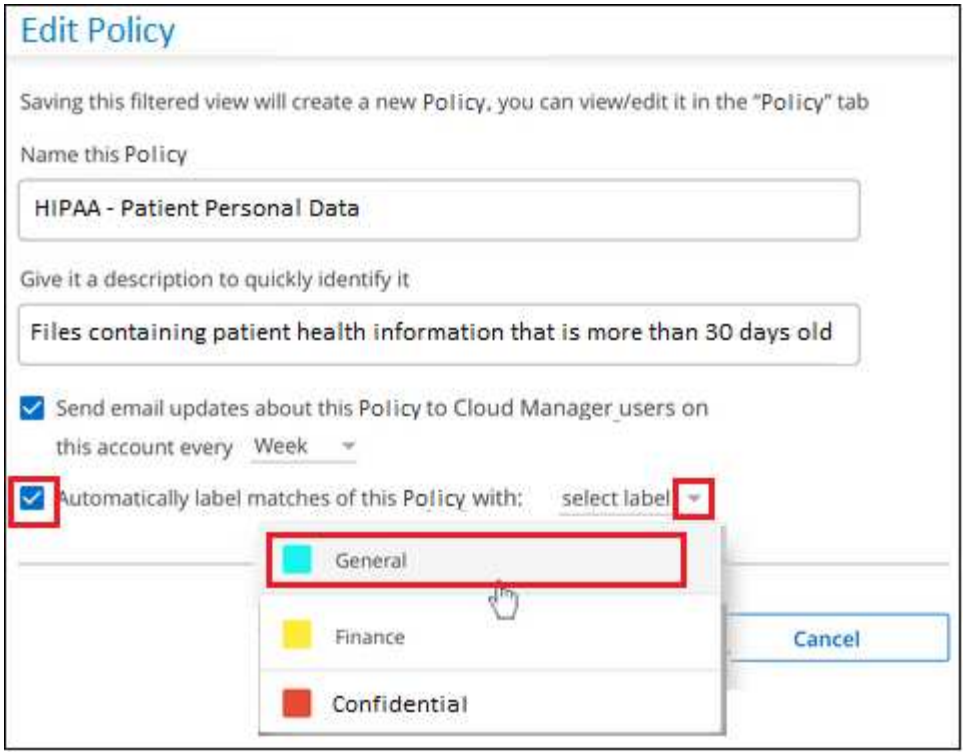
Per aggiungere un'etichetta AIP a una policy esistente, procedere come segue.

Fasi

1. Nella pagina elenco criteri, fare clic su **Modifica** per la policy in cui si desidera aggiungere (o modificare) l'etichetta AIP.



2. Nella pagina Edit Policy (Modifica policy), selezionare la casella per abilitare le etichette automatiche per i file che corrispondono ai parametri del Policy, quindi selezionare l'etichetta (ad esempio, **General**).



3. Fare clic su **Save Policy** (Salva policy) per visualizzare l'etichetta nella descrizione della policy.

> Se un criterio è stato configurato con un'etichetta, ma l'etichetta è stata rimossa da AIP, il nome dell'etichetta viene disattivato e l'etichetta non viene più assegnata.

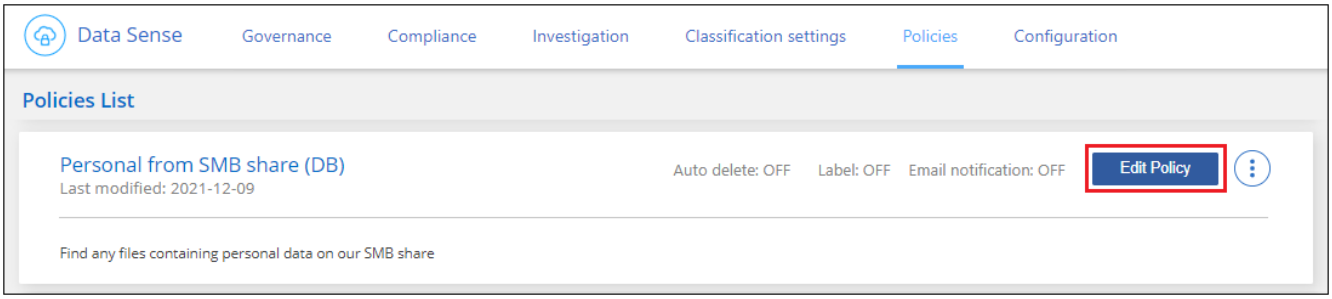
Modifica criteri

È possibile modificare qualsiasi criterio per un criterio esistente creato in precedenza. Questo può essere particolarmente utile se si desidera modificare la query (gli elementi definiti utilizzando filtri) per aggiungere o rimuovere determinati parametri.

Tenere presente che per le policy predefinite è possibile modificare solo se le notifiche e-mail vengono inviate e se vengono aggiunte etichette AIP. Non è possibile modificare altri valori.

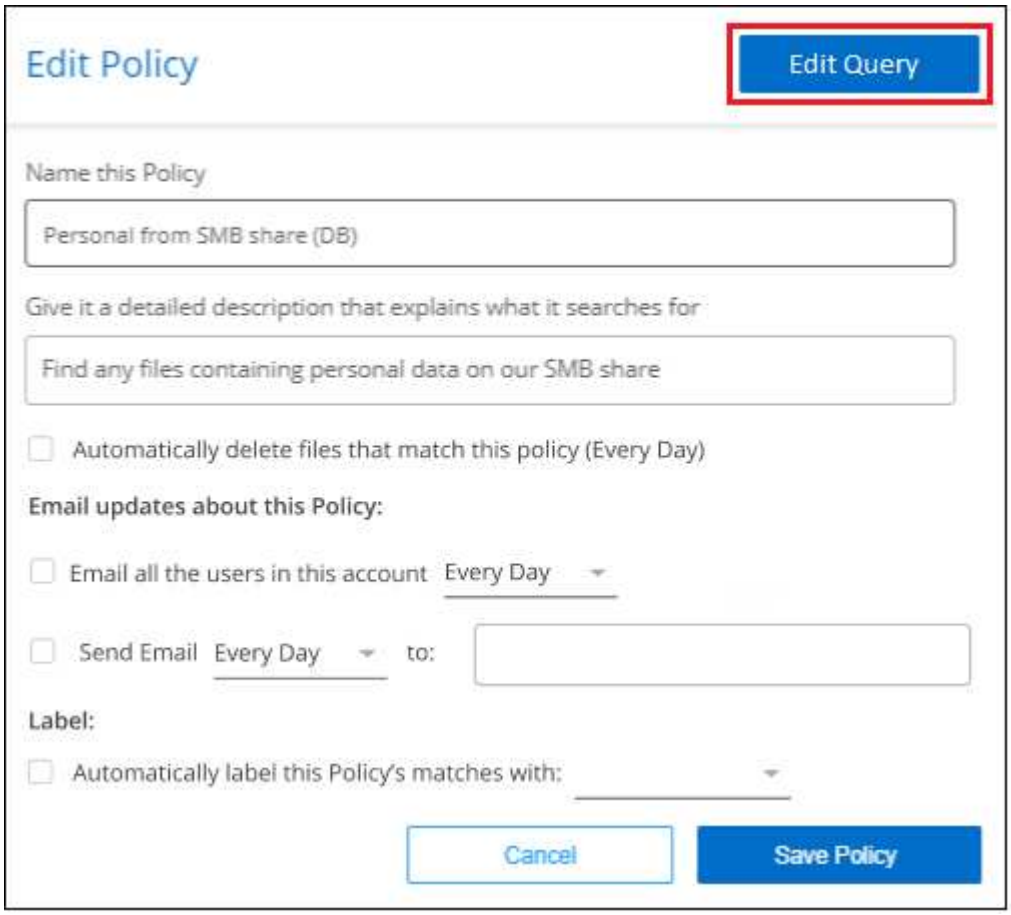
Fasi

1. Nella pagina elenco criteri, fare clic su **Modifica** per il criterio che si desidera modificare.

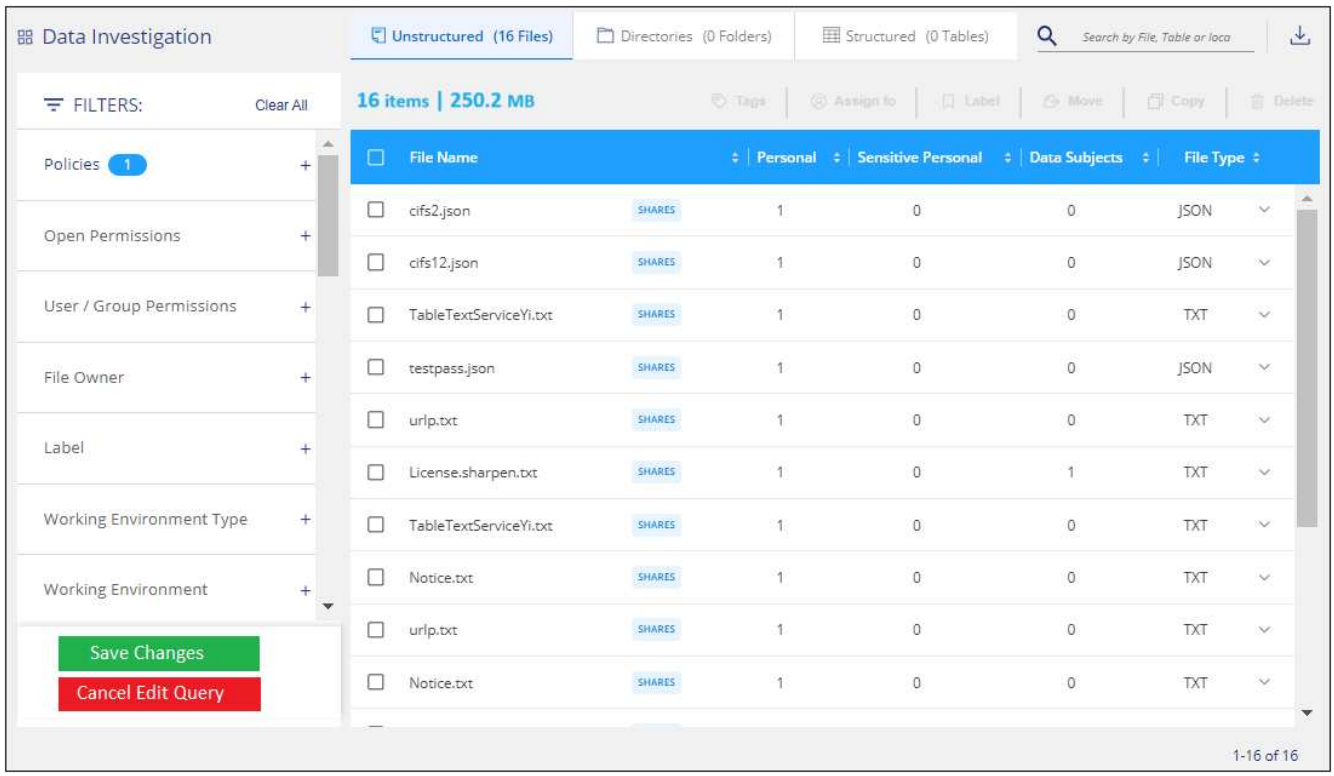


2. Se si desidera modificare gli elementi di questa pagina (nome, descrizione, invio di notifiche e-mail e aggiunta di etichette AIP), apportare la modifica e fare clic su **Save Policy** (Salva policy).

   Se si desidera modificare i filtri per la query salvata, fare clic su **Edit Query** (Modifica query).



3. Nella pagina di analisi che definisce la query, modificare la query aggiungendo, rimuovendo o personalizzando i filtri, quindi fare clic su **Save Changes** (Salva modifiche).



Risultato

La policy viene modificata immediatamente. Tutte le azioni definite per quel criterio per inviare un'email, aggiungere etichette AIP o eliminare file si verificheranno al successivo interno.

Delete Policy (Elimina policy)

È possibile eliminare qualsiasi policy personalizzata creata se non è più necessaria. Non è possibile eliminare alcuna policy predefinita.

Per eliminare un criterio, fare clic su Per una policy specifica, fare clic su **Delete Policy** (Elimina policy), quindi fare nuovamente clic su **Delete Policy** (Elimina policy) nella finestra di dialogo di conferma.

Elenco dei criteri predefiniti

La classificazione BlueXP fornisce le seguenti policy definite dal sistema:

Nome	Descrizione	Logica
S3 - dati privati esposti pubblicamente	Oggetti S3 contenenti informazioni personali o sensibili, con accesso pubblico aperto in lettura.	S3 Public E contiene informazioni personali o personali sensibili
PCI DSS - dati obsoleti in 30 giorni	File contenenti informazioni sulla carta di credito, modificati più di 30 giorni fa.	Contiene la carta di credito E l'ultima modifica in 30 giorni
HIPAA - dati obsoleti in 30 giorni	File contenenti informazioni sulla salute, modificati l'ultima volta 30 giorni fa.	Contiene i dati di salute (definiti come nel report HIPAA) E l'ultima modifica nell'arco di 30 giorni
Dati privati - obsoleti in 7 anni	File contenenti informazioni personali o sensibili, modificati da oltre 7 anni fa.	File contenenti informazioni personali o sensibili, modificati da oltre 7 anni fa
GDPR - cittadini europei	File contenenti più di 5 identificatori dei cittadini di un paese dell'UE o tabelle DB contenenti identificatori dei cittadini di un paese dell'UE.	File contenenti oltre 5 identificatori di un (uno) cittadino dell'UE o tabelle DB contenenti righe con oltre il 15% di colonne con identificatori UE di un paese. (Uno qualsiasi degli identificatori nazionali dei paesi europei. Non include Brasile, California, USA SSN, Israele, Sudafrica)
CCPA - residenti in California	File contenenti oltre 10 identificatori della licenza del driver California o tabelle DB con questo identificatore.	File contenenti oltre 10 identificatori della licenza di guida California O tabelle DB contenenti la licenza di guida California
Nomi dei soggetti dei dati - rischio elevato	File con oltre 50 nomi di soggetti dati.	File con oltre 50 nomi di soggetti dati
Indirizzi e-mail - rischio elevato	File con oltre 50 indirizzi e-mail o colonne DB con oltre il 50% delle righe contenenti indirizzi e-mail	File con oltre 50 indirizzi e-mail o colonne DB con oltre il 50% delle righe contenenti indirizzi e-mail
Dati personali - rischio elevato	File con oltre 20 ID dati personali o colonne DB con oltre il 50% delle righe contenenti identificativi dati personali.	File con oltre 20 colonne personali o DB con oltre il 50% delle righe contenenti dati personali

Nome	Descrizione	Logica
Dati personali sensibili - rischio elevato	File con oltre 20 identificatori di dati personali sensibili o colonne di database con oltre il 50% delle righe contenenti dati personali sensibili.	File con oltre 20 colonne personali sensibili o DB con oltre il 50% delle righe contenenti dati personali sensibili

Gestisci i tuoi dati privati

La classificazione BlueXP offre diversi modi per gestire i dati privati. Alcune funzionalità semplificano la preparazione alla migrazione dei dati, mentre altre funzionalità consentono di apportare modifiche ai dati.

- È possibile copiare i file in una condivisione NFS di destinazione se si desidera creare una copia di determinati dati e spostarli in una posizione NFS diversa.
- È possibile clonare un volume ONTAP in un nuovo volume, includendo solo i file selezionati dal volume di origine nel nuovo volume clonato. Ciò è utile per le situazioni in cui si esegue la migrazione dei dati e si desidera escludere alcuni file dal volume originale.
- È possibile copiare e sincronizzare i file da un repository di origine a una directory in una posizione di destinazione specifica. Questa funzione è utile per le situazioni in cui si esegue la migrazione dei dati da un sistema di origine a un altro mentre è ancora presente un'attività finale sui file di origine.
- Puoi spostare i file di origine che la classificazione BlueXP sta scansionando in qualsiasi condivisione NFS.
- È possibile eliminare i file che sembrano insicuri o troppo rischiosi da lasciare nel sistema di storage o che sono stati identificati come duplicati.

> - Le funzionalità descritte in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura non mostrano i dettagli a livello di file.
> - I dati degli account Google Drive al momento non possono utilizzare nessuna di queste funzionalità.

Copia dei file di origine

È possibile copiare qualsiasi file di origine sottoposto a scansione dalla classificazione BlueXP. Esistono tre tipi di operazioni di copia a seconda di ciò che si sta cercando di ottenere:

- **Copiare file** da volumi o origini dati uguali o diversi in una condivisione NFS di destinazione.

  Questo è utile se si desidera creare una copia di determinati dati e spostarli in una posizione NFS diversa.

- **Clonare un volume ONTAP** in un nuovo volume nello stesso aggregato, ma includere solo i file selezionati dal volume di origine nel nuovo volume clonato.

  Ciò è utile per le situazioni in cui si esegue la migrazione dei dati e si desidera escludere alcuni file dal volume originale. Questa azione utilizza "FlexClone di NetApp" funzionalità che consente di duplicare rapidamente il volume e rimuovere i file * non selezionati*.

- **Copiare e sincronizzare i file** da un singolo repository di origine (volume ONTAP, bucket S3, condivisione NFS, ecc.) a una directory in una destinazione specifica (destinazione).

Ciò è utile per le situazioni in cui si esegue la migrazione dei dati da un sistema di origine a un altro. Dopo la copia iniziale, il servizio sincronizza i dati modificati in base alla pianificazione impostata. Questa azione utilizza "Copia e sincronizzazione NetApp BlueXP" funzionalità per copiare e sincronizzare i dati da un'origine a una destinazione.

Copiare i file di origine in una condivisione NFS

Puoi copiare i file di origine che la classificazione BlueXP sta scansionando su qualsiasi condivisione NFS. La condivisione NFS non deve essere integrata con la classificazione BlueXP, devi solo conoscere il nome della condivisione NFS dove tutti i file selezionati verranno copiati nel formato `<host_name>:/<share_path>`.

Non è possibile copiare i file che risiedono nei database.

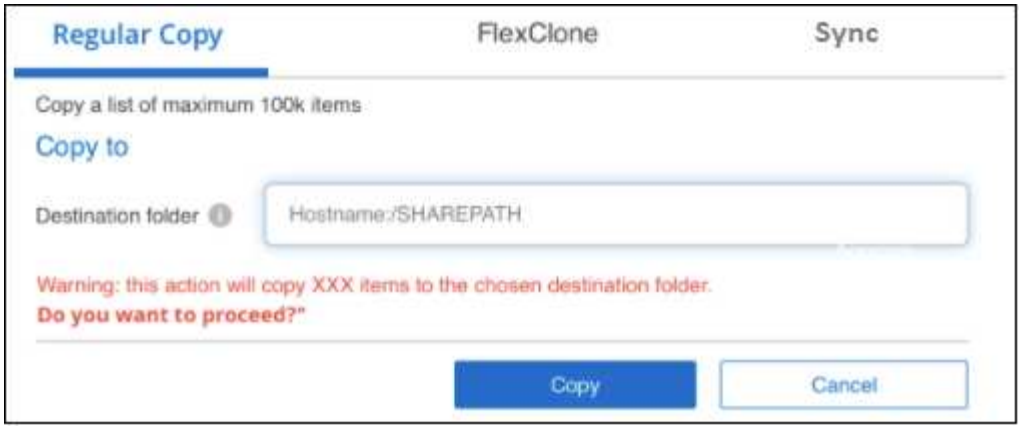
Requisiti

- Per copiare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- La copia dei file richiede che la condivisione NFS di destinazione consenta l'accesso dall'istanza di classificazione BlueXP.
- È possibile copiare da 1 a 100,000 file alla volta.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da copiare e fare clic su **Copy** (Copia).

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
   - Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.
2. Nella finestra di dialogo *Copy Files*, selezionare la scheda **Regular Copy**.



3. Immettere il nome della condivisione NFS in cui verranno copiati tutti i file selezionati nel formato `<host_name>:/<share_path>`E fare clic su **Copia**.

   Viene visualizzata una finestra di dialogo con lo stato dell'operazione di copia.

È possibile visualizzare l'avanzamento dell'operazione di copia in "Riquadro Actions Status (Stato azioni)".

Nota: È anche possibile copiare un singolo file quando si visualizzano i dettagli dei metadati di un file. Fare clic su **Copy file** (Copia file).

Clonazione dei dati del volume in un nuovo volume

È possibile clonare un volume ONTAP esistente sottoposto a scansione dalla classificazione BlueXP utilizzando la funzionalità NetApp *FlexClone*. Ciò consente di duplicare rapidamente il volume includendo solo i file selezionati. Ciò è utile se si stanno migrando i dati e si desidera escludere alcuni file dal volume originale o se si desidera creare una copia di un volume per il test.

Il nuovo volume viene creato nello stesso aggregato del volume di origine. Assicurarsi di disporre di spazio sufficiente per questo nuovo volume nell'aggregato prima di avviare questa attività. Se necessario, contattare l'amministratore dello storage.

Nota: i volumi FlexGroup non possono essere clonati perché non sono supportati da FlexClone.

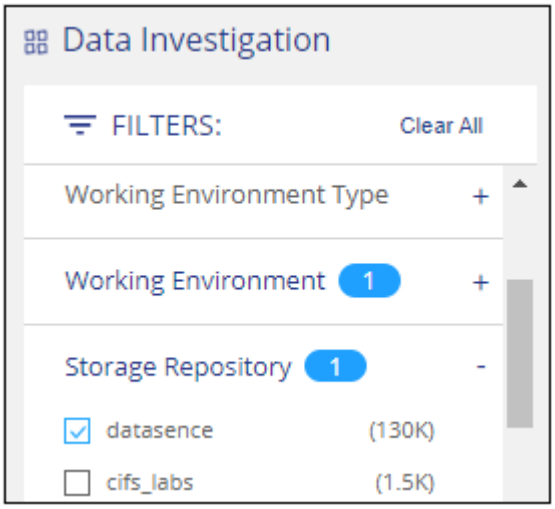
Requisiti

- Per copiare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).

- Selezionare un minimo di 20 file.
- Tutti i file selezionati devono provenire dallo stesso volume e il volume deve essere online.
- Il volume deve provenire da un sistema Cloud Volumes ONTAP o ONTAP on-premise. Al momento non sono supportate altre origini dati.
- La licenza FlexClone deve essere installata sul cluster. Questa licenza viene installata per impostazione predefinita sui sistemi Cloud Volumes ONTAP.

Fasi

1. Nel riquadro analisi dati, creare un filtro selezionando un singolo **ambiente di lavoro** e un singolo **repository di storage** per assicurarsi che tutti i file provengano dallo stesso volume ONTAP.



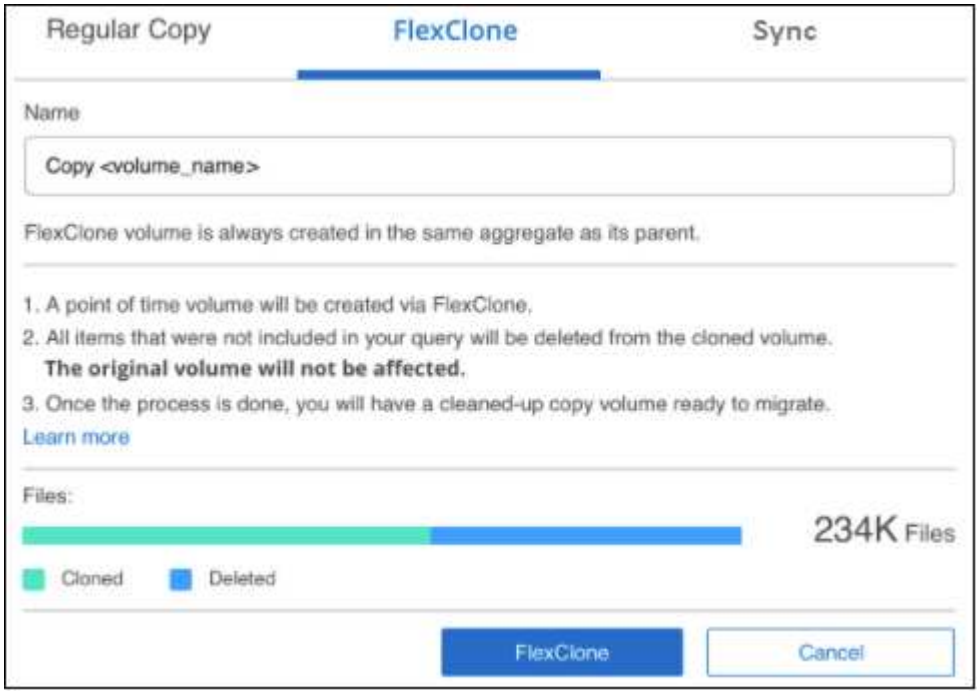
   Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera clonare nel nuovo volume.

2. Nel riquadro dei risultati dell'analisi, selezionare i file che si desidera clonare e fare clic su **Copy** (Copia).

   - Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
   - Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
   - Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

3. Nella finestra di dialogo *Copy Files*, selezionare la scheda **FlexClone**. Questa pagina mostra il numero

totale di file che verranno clonati dal volume (i file selezionati) e il numero di file che non vengono inclusi/cancellati (i file non selezionati) dal volume clonato.



4. Inserire il nome del nuovo volume e fare clic su **FlexClone**.

   Viene visualizzata una finestra di dialogo con lo stato dell'operazione di clonazione.

Risultato

Il nuovo volume clonato viene creato nello stesso aggregato del volume di origine.

È possibile visualizzare lo stato di avanzamento dell'operazione di clonazione in "Riquadro Actions Status (Stato azioni)".

Se inizialmente è stato selezionato **Map All Volumes** (mappatura di tutti i volumi) o **Map & Classify All Volumes** (mappatura e classificazione di tutti i volumi) quando è stata attivata la classificazione BlueXP per l'ambiente di lavoro in cui risiede il volume di origine, la classificazione BlueXP eseguirà automaticamente la scansione del nuovo volume clonato. Se inizialmente non si è utilizzata una di queste selezioni, è necessario eseguire la scansione di questo nuovo volume "attivare manualmente la scansione sul volume".

Copiare e sincronizzare i file di origine in un sistema di destinazione

È possibile copiare i file di origine che la classificazione BlueXP sta scansionando da qualsiasi origine dati non strutturata supportata in una directory in una posizione di destinazione specifica ("Posizioni di destinazione supportate dalla copia e dalla sincronizzazione BlueXP"). Dopo la copia iniziale, tutti i dati modificati nei file vengono sincronizzati in base alla pianificazione configurata.

Ciò è utile per le situazioni in cui si esegue la migrazione dei dati da un sistema di origine a un altro. Questa azione utilizza "Copia e sincronizzazione NetApp BlueXP" funzionalità per copiare e sincronizzare i dati da un'origine a una destinazione.

Non puoi copiare e sincronizzare i file che risiedono in database, account OneDrive o account SharePoint.

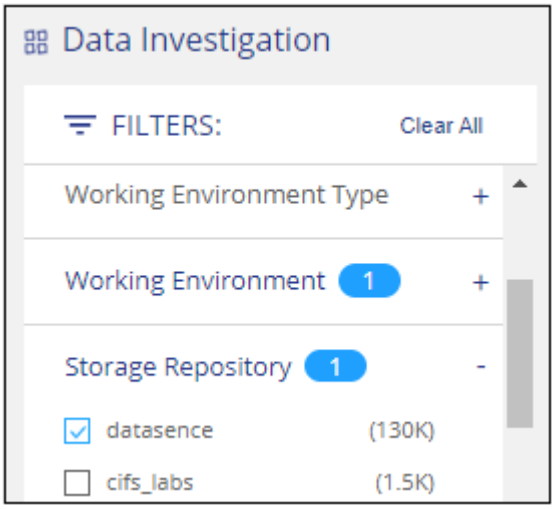
Requisiti

- Per copiare e sincronizzare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- Selezionare un minimo di 20 file.
- Tutti i file selezionati devono provenire dallo stesso repository di origine (volume ONTAP, bucket S3, condivisione NFS o CIFS, ecc.).
- È necessario attivare il servizio di copia e sincronizzazione BlueXP e configurare almeno un broker di dati da utilizzare per trasferire i file tra i sistemi di origine e di destinazione. Esaminare i requisiti di copia e sincronizzazione di BlueXP a partire da "Descrizione di avvio rapido".

  Si noti che il servizio di copia e sincronizzazione BlueXP prevede costi di servizio separati per le relazioni di sincronizzazione e comporta costi per le risorse se si implementa il broker di dati nel cloud.

Fasi

1. Nel riquadro Data Investigation (analisi dati), creare un filtro selezionando un singolo **Working Environment** e un singolo **Storage Repository** per assicurarsi che tutti i file provengano dallo stesso repository.

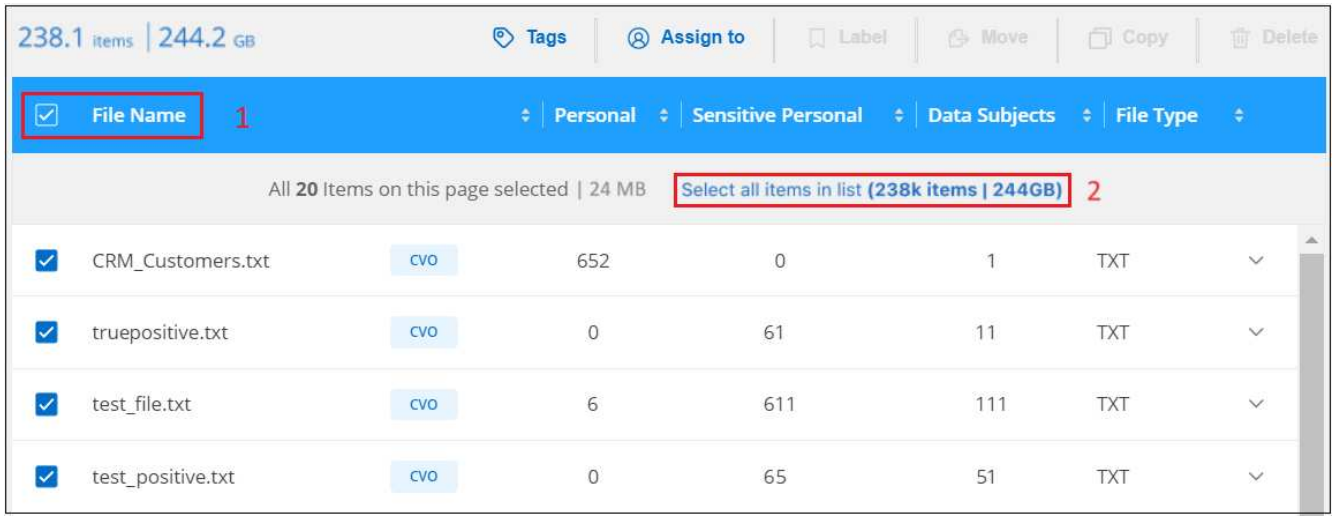


   Applicare eventuali altri filtri in modo da visualizzare solo i file che si desidera copiare e sincronizzare nel sistema di destinazione.

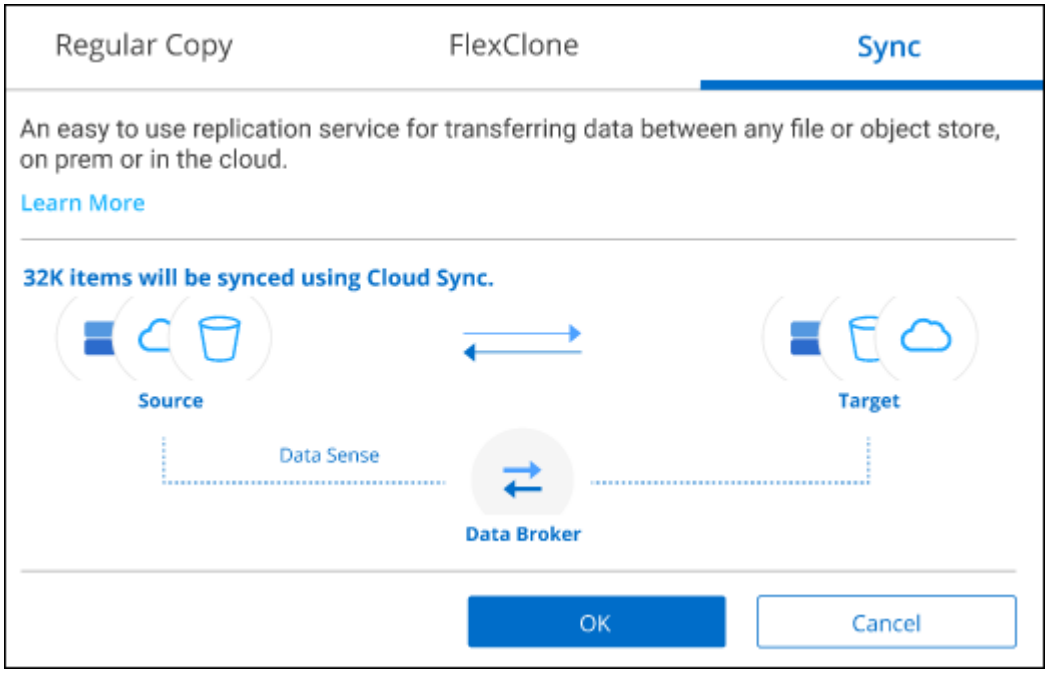
2. Nel riquadro dei risultati dell'analisi, selezionare tutti i file su tutte le pagine selezionando la casella nella riga del titolo (

), quindi nel messaggio a comparsa 

Fare clic su **Select All ITEMS in list (xxx ITEMS)** (Seleziona tutti gli elementi nell'elenco (xxx elementi)**, quindi fare clic su *Copy** (Copia).



3. Nella finestra di dialogo *Copy Files*, selezionare la scheda **Sync**.



4. Se si è certi di voler sincronizzare i file selezionati in una posizione di destinazione, fare clic su **OK**.

   L'interfaccia utente di copia e sincronizzazione di BlueXP viene aperta in BlueXP.

   Viene richiesto di definire la relazione di sincronizzazione. Il sistema di origine viene prepopolato in base al repository e ai file già selezionati nella classificazione BlueXP.

5. È necessario selezionare il sistema di destinazione e selezionare (o creare) il Data Broker che si desidera utilizzare. Esaminare i requisiti di copia e sincronizzazione di BlueXP a partire da "Descrizione di avvio rapido".

Risultato

I file vengono copiati nel sistema di destinazione e sincronizzati in base alla pianificazione definita. Se si seleziona una sincronizzazione una tantum, i file vengono copiati e sincronizzati una sola volta. Se si sceglie una sincronizzazione periodica, i file vengono sincronizzati in base alla pianificazione. Si noti che se il sistema di origine aggiunge nuovi file che corrispondono alla query creata utilizzando i filtri, questi *nuovi* file verranno

copiati nella destinazione e sincronizzati in futuro.

Si noti che alcune delle normali operazioni di copia e sincronizzazione di BlueXP sono disabilitate quando vengono richiamate dalla classificazione BlueXP:

- Non è possibile utilizzare i pulsanti **Delete Files on Source** o **Delete Files on Target**.
- L'esecuzione di un report è disattivata.

Spostare i file di origine in una condivisione NFS

Puoi spostare i file di origine che la classificazione BlueXP sta scansionando in qualsiasi condivisione NFS. Non è necessario integrare la condivisione NFS con la classificazione BlueXP.

In alternativa, è possibile lasciare un file breadcrumb nella posizione del file spostato. Un file breadcrumb aiuta gli utenti a capire perché un file è stato spostato dalla posizione originale. Per ogni file spostato, il sistema crea un file breadcrumb nella posizione di origine denominata `<filename>-breadcrumb-<date>.txt`. È possibile aggiungere del testo nella finestra di dialogo che verrà aggiunta al file breadcrumb per indicare la posizione in cui è stato spostato il file e l'utente che lo ha spostato.

Si noti che la struttura della sottodirectory dal file di origine viene ricreata sulla condivisione di destinazione quando il file viene spostato, in modo da comprendere più facilmente da dove è stato spostato il file. Se esiste un file con lo stesso nome nella posizione di destinazione, il file non verrà spostato.

Non è possibile spostare i file che risiedono nei database.

Requisiti

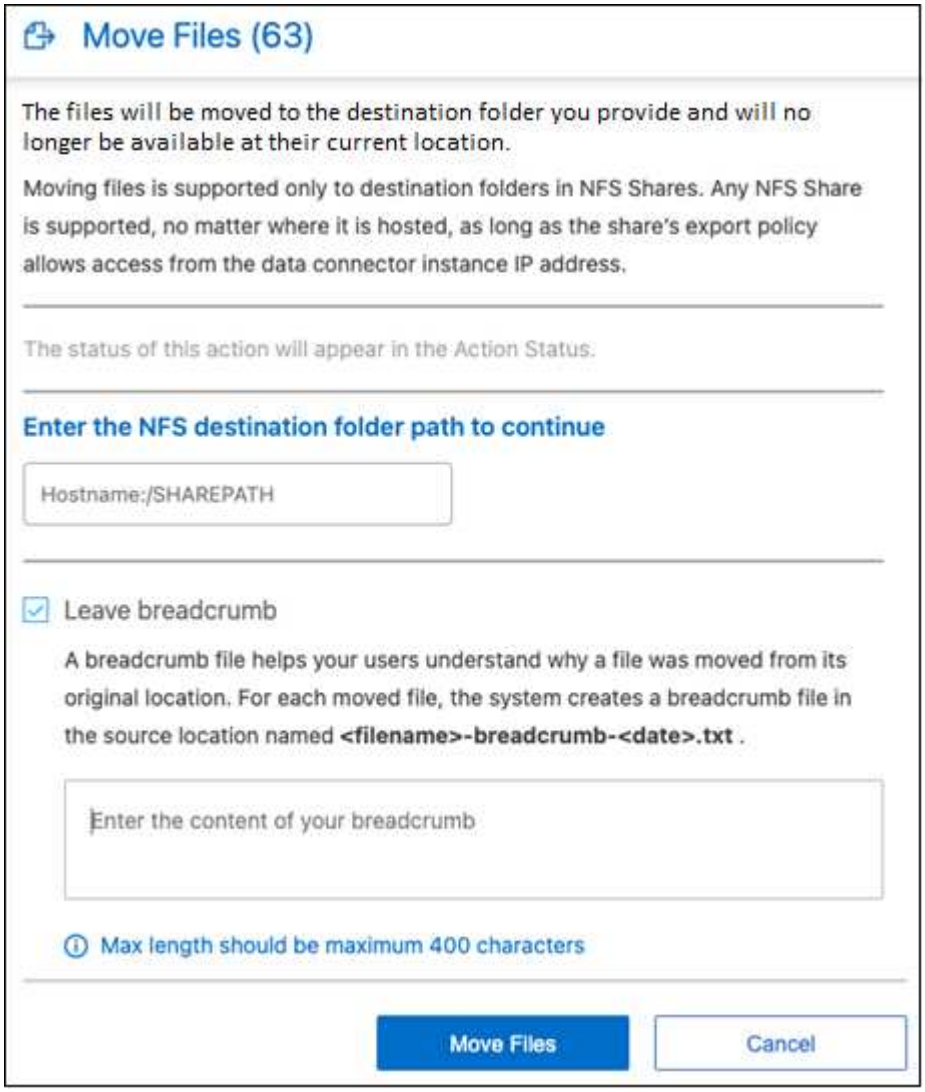
- Per spostare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- I file di origine possono trovarsi nelle seguenti origini dati: On-premise ONTAP, Cloud Volumes ONTAP, Azure NetApp Files, condivisioni file e SharePoint Online.
- È possibile spostare un massimo di 15 milioni di file alla volta.
- Vengono spostati solo i file di dimensioni pari o inferiori a 50 MB.
- La condivisione NFS di destinazione deve consentire l'accesso dall'indirizzo IP dell'istanza di classificazione BlueXP.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file da spostare.

- Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
- Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
- Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All 20 Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

2. Dalla barra dei pulsanti, fare clic su **Sposta**.



3. Nella finestra di dialogo *Move Files*, immettere il nome della condivisione NFS in cui verranno spostati tutti i file selezionati nel formato `<host_name>:/<share_path>`.
4. Se si desidera lasciare un file breadcrumb, selezionare la casella *Leave breadcrumb*. È possibile inserire del testo nella finestra di dialogo per indicare la posizione in cui è stato spostato il file, l'utente che lo ha spostato e qualsiasi altra informazione, come il motivo dello spostamento del file.
5. Fare clic su **Sposta file**.

Nota: È anche possibile spostare un singolo file quando si visualizzano i dettagli dei metadati di un file. Fare clic su **Sposta file**.

Eliminare i file di origine

È possibile rimuovere in modo permanente i file di origine che sembrano insicuri o troppo rischiosi da lasciare nel sistema di storage o che sono stati identificati come duplicati. Questa azione è permanente e non è possibile annullare o ripristinare.

È possibile eliminare i file manualmente dal riquadro analisi, oppure "Utilizzo automatico dei criteri".

> Non è possibile eliminare i file che risiedono nei database. Sono supportate tutte le altre origini dati.

L'eliminazione dei file richiede le seguenti autorizzazioni:

- Per i dati NFS - la policy di esportazione deve essere definita con permessi di scrittura.
- Per i dati CIFS - le credenziali CIFS devono disporre di permessi di scrittura.
- Per i dati S3 - il ruolo IAM deve includere la seguente autorizzazione: `s3:DeleteObject`.

Eliminare manualmente i file di origine

Requisiti

- Per eliminare i file, è necessario disporre del ruolo account Admin (Amministratore account) o Workspace Admin (Amministratore area di lavoro).
- È possibile eliminare un massimo di 100,000 file alla volta.

Fasi

1. Nel riquadro Data Investigation Results (risultati analisi dati), selezionare il file o i file che si desidera eliminare.

- Per selezionare singoli file, selezionare la casella corrispondente a ciascun file (Volume_1).
- Per selezionare tutti i file nella pagina corrente, selezionare la casella nella riga del titolo (File Name).
- Per selezionare tutti i file su tutte le pagine, selezionare la casella nella riga del titolo (File Name), quindi nel messaggio a comparsa All **20** Items on this page selected Select all Items in list (63K Items), Fare clic su **Seleziona tutti gli elementi nell'elenco (xxx elementi)**.

2. Dalla barra dei pulsanti, fare clic su **Delete** (Elimina).
3. Poiché l'operazione di eliminazione è permanente, digitare "**permanentemente delete**" nella successiva finestra di dialogo *Delete file* e fare clic su **Delete file**.

È possibile visualizzare l'avanzamento dell'operazione di eliminazione in "Riquadro Actions Status (Stato azioni)".

Nota: È anche possibile eliminare un singolo file quando si visualizzano i dettagli dei metadati di un file. Fare clic su **Delete file** (Elimina file).

Visualizza i report sulla conformità

La classificazione BlueXP fornisce report che è possibile utilizzare per comprendere meglio lo stato del programma per la privacy dei dati della tua organizzazione.

Per impostazione predefinita, le dashboard di classificazione di BlueXP visualizzano i dati di conformità e governance per tutti gli ambienti di lavoro, i database e le origini dati. Se si desidera visualizzare report contenenti dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

- I report descritti in questa sezione sono disponibili solo se si è scelto di eseguire una scansione di classificazione completa sulle origini dati. Le origini dati che hanno eseguito una scansione solo mappatura possono generare solo il report di mappatura dei dati.
- NetApp non può garantire la precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla classificazione BlueXP. È sempre necessario convalidare le informazioni esaminando i dati.

Report sulla valutazione dei rischi per la privacy

Il report sulla valutazione dei rischi per la privacy fornisce una panoramica dello stato di rischio per la privacy della tua organizzazione, come richiesto dalle normative sulla privacy come GDPR e CCPA. Il report contiene le seguenti informazioni:

Stato di compliance

R punteggio di severità e la distribuzione dei dati, sia che si tratti di dati personali, non sensibili o sensibili.

Panoramica della valutazione

Analisi dei tipi di dati personali rilevati, nonché delle categorie di dati.

Argomenti trattati in questa valutazione

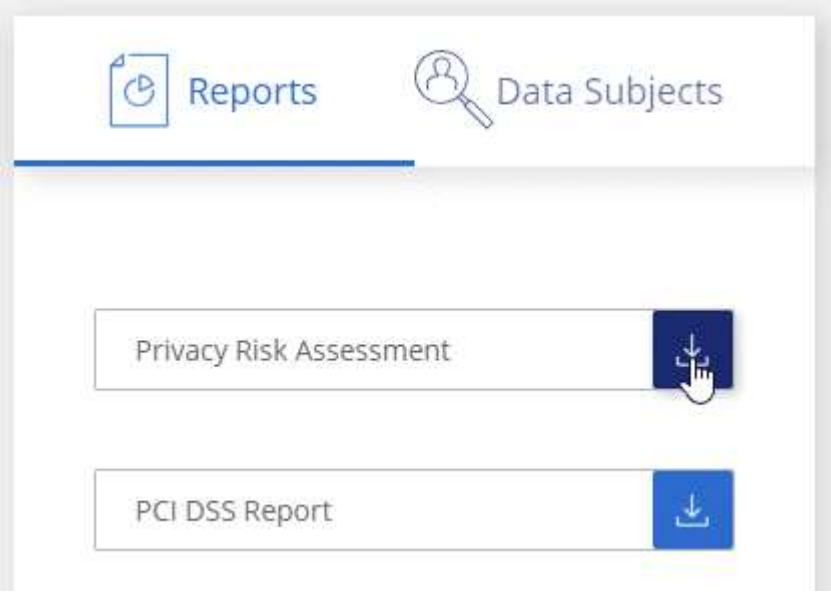
Il numero di persone, per località, per le quali sono stati trovati identificatori nazionali.

Generare Privacy Risk Assessment Report

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Compliance**, quindi fare clic sull'icona di download accanto a **Privacy Risk Assessment** sotto **Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in

base alle esigenze.

Punteggio di severità

La classificazione BlueXP calcola il punteggio di severità per il Privacy Risk Assessment Report sulla base di tre variabili:

- La percentuale di dati personali su tutti i dati.
- La percentuale di dati personali sensibili rispetto a tutti i dati.
- La percentuale di file che includono soggetti dati, determinata da identificatori nazionali come ID nazionali, numeri di previdenza sociale e numeri di identificazione fiscale.

La logica utilizzata per determinare il punteggio è la seguente:

Punteggio di severità	Logica
0	Tutte e tre le variabili sono esattamente 0%
1	Una delle variabili è maggiore dello 0%
2	Una delle variabili è maggiore del 3%
3	Due delle variabili sono maggiori del 3%
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono maggiori del 6%
7	Tre delle variabili sono maggiori del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono maggiori del 15%
10	Tre delle variabili sono maggiori del 15%

Report PCI DSS

Il report PCI DSS (Payment Card Industry Data Security Standard) consente di identificare la distribuzione delle informazioni sulle carte di credito nei file. Il report contiene le seguenti informazioni:

Panoramica

Quanti file contengono informazioni sulla carta di credito e in quali ambienti di lavoro.

Crittografia

La percentuale di file contenenti informazioni sulla carta di credito presenti in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware

La percentuale di file contenenti informazioni sulla carta di credito che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione

Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni della carta di credito per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sulla carta di credito

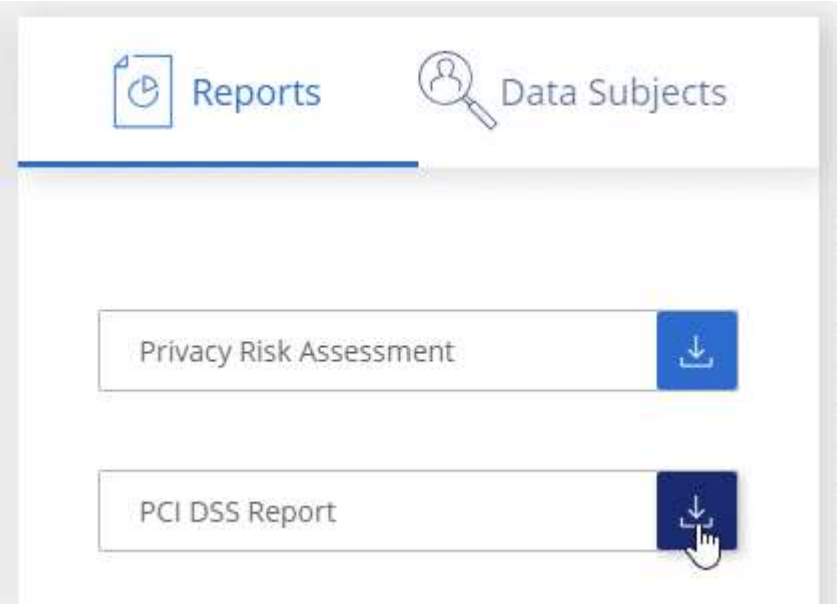
Gli ambienti di lavoro in cui sono state rilevate le informazioni sulla carta di credito e se sono attivate la crittografia e la protezione ransomware.

Generare il rapporto PCI DSS

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Compliance**, quindi fare clic sull'icona di download accanto a **PCI DSS Report** sotto **Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

Report HIPAA

Il report HIPAA (Health Insurance Portability and Accountability Act) consente di identificare i file contenenti informazioni sulla salute. È progettato per soddisfare i requisiti della tua organizzazione in materia di privacy dei dati HIPAA. Le informazioni che la classificazione BlueXP cerca includono:

- Schema di riferimento per lo stato di salute
- ICD-10-CM Codice medico
- Codice medico ICD-9-CM
- HR - Categoria di salute
- Categoria Health Application Data

Il report contiene le seguenti informazioni:

Panoramica

Quanti file contengono informazioni sullo stato di salute e in quali ambienti di lavoro.

Crittografia

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione

Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni sulla salute per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sanitarie

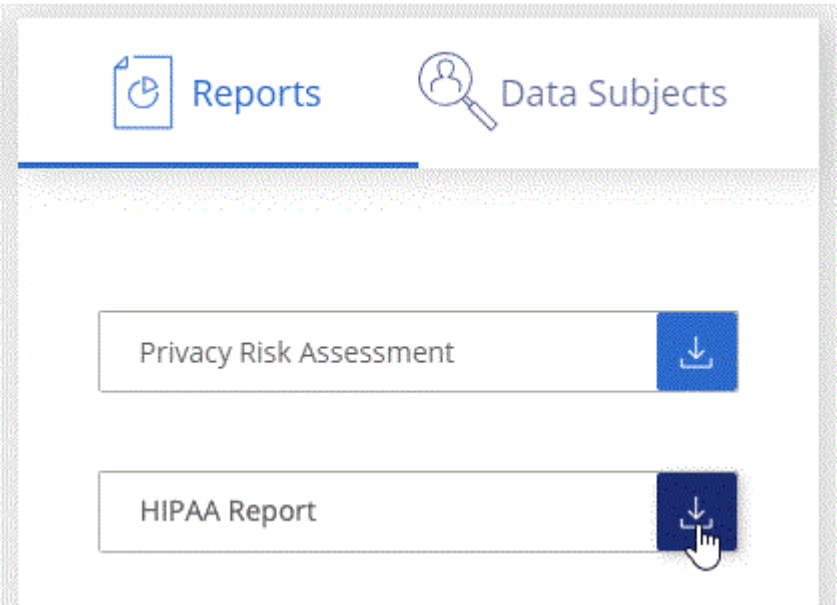
Gli ambienti di lavoro in cui sono state trovate le informazioni di salute e se sono attivate la crittografia e la protezione ransomware.

Generare il report HIPAA

Accedere alla scheda Compliance per generare il report.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Compliance**, quindi fare clic sull'icona di download accanto a **HIPAA Report** sotto **Report**.



Risultato

La classificazione BlueXP genera un report in formato PDF che è possibile rivedere e inviare ad altri gruppi in base alle esigenze.

Che cos’è una richiesta di accesso ai dati?

Le normative sulla privacy, come il GDPR europeo, concedono ai soggetti interessati (come clienti o dipendenti) il diritto di accedere ai propri dati personali. Quando un soggetto interessato richiede queste informazioni, queste vengono denominate DSAR (data subject access request). Le organizzazioni devono rispondere a queste richieste "senza ritardi indebito" e al più tardi entro un mese dalla ricezione.

È possibile rispondere a una DSAR cercando il nome completo di un soggetto o l’identificatore noto (ad esempio un indirizzo e-mail) e scaricando un report. Il report è stato progettato per aiutare l’organizzazione a rispettare il GDPR o leggi simili sulla privacy dei dati.

In che modo la classificazione BlueXP può aiutarti a rispondere a una DSAR?

Quando si esegue una ricerca dell’oggetto dati, la classificazione BlueXP trova tutti i file, i bucket, OneDrive e gli account SharePoint che contengono il nome o l’identificatore di tale persona. La classificazione BlueXP verifica i dati pre-indicizzati più recenti per il nome o l’identificatore. Non avvia una nuova scansione.

Una volta completata la ricerca, è possibile scaricare l’elenco di file per un report Data Subject Access Request. Il report aggrega le informazioni dei dati e le inserisce in termini legali che è possibile inviare alla persona.

> La ricerca dei dati non è attualmente supportata nei database.

Cercare gli argomenti dei dati e scaricare i report

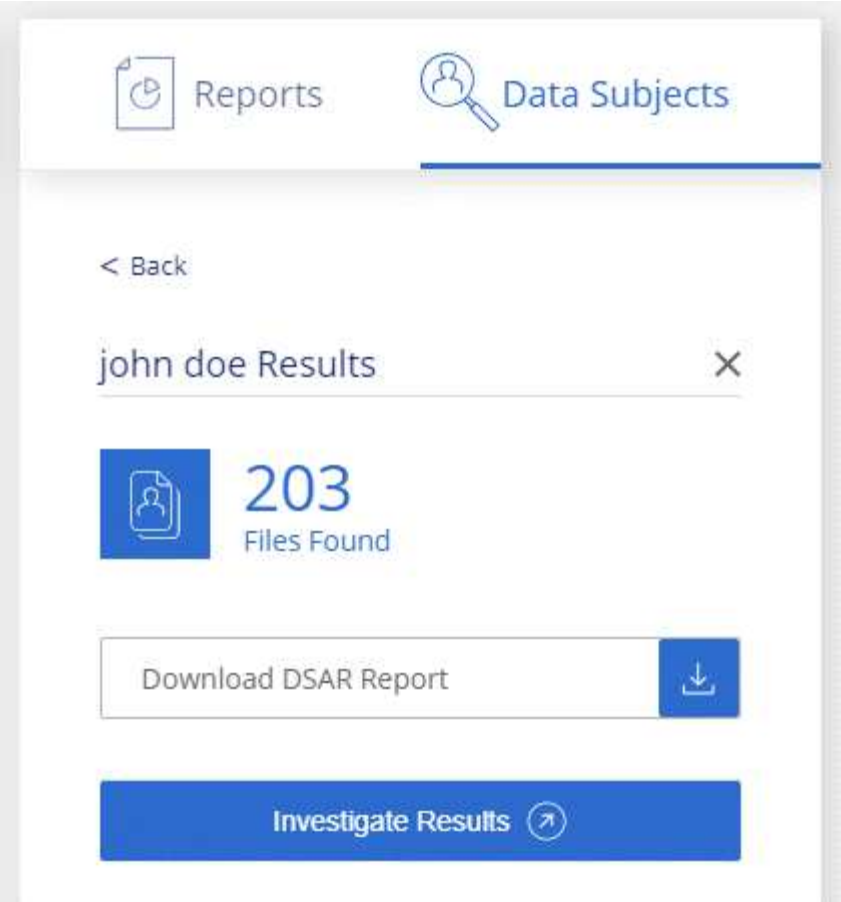
Cercare il nome completo o l’identificatore noto del soggetto interessato, quindi scaricare un report elenco file o un report DSAR. È possibile eseguire la ricerca in base a. "qualsiasi tipo di informazione personale".

> Sono supportati l’inglese, il tedesco, il giapponese e lo spagnolo durante la ricerca dei nomi degli argomenti dei dati. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Data subjects**.
3. Cercare il nome completo o l’identificativo noto dell’interessato.

   Ecco un esempio che mostra una ricerca per il nome *john Doe*:



4. Scegliere una delle opzioni disponibili:
   - **Download del report DSAR**: Una risposta formale alla richiesta di accesso che è possibile inviare al soggetto interessato. Questo report contiene informazioni generate automaticamente in base ai dati rilevati dalla classificazione BlueXP nell'oggetto dei dati ed è progettato per essere utilizzato come modello. Completare il modulo e esaminarlo internamente prima di inviarlo al soggetto interessato.
   - **Investigate Results**: Pagina che consente di analizzare i dati ricercando, ordinando, espandendo i dettagli di un file specifico e scaricando l'elenco dei file.

> Se sono presenti più di 10,000 risultati, nell'elenco dei file vengono visualizzati solo i primi 10,000 risultati.

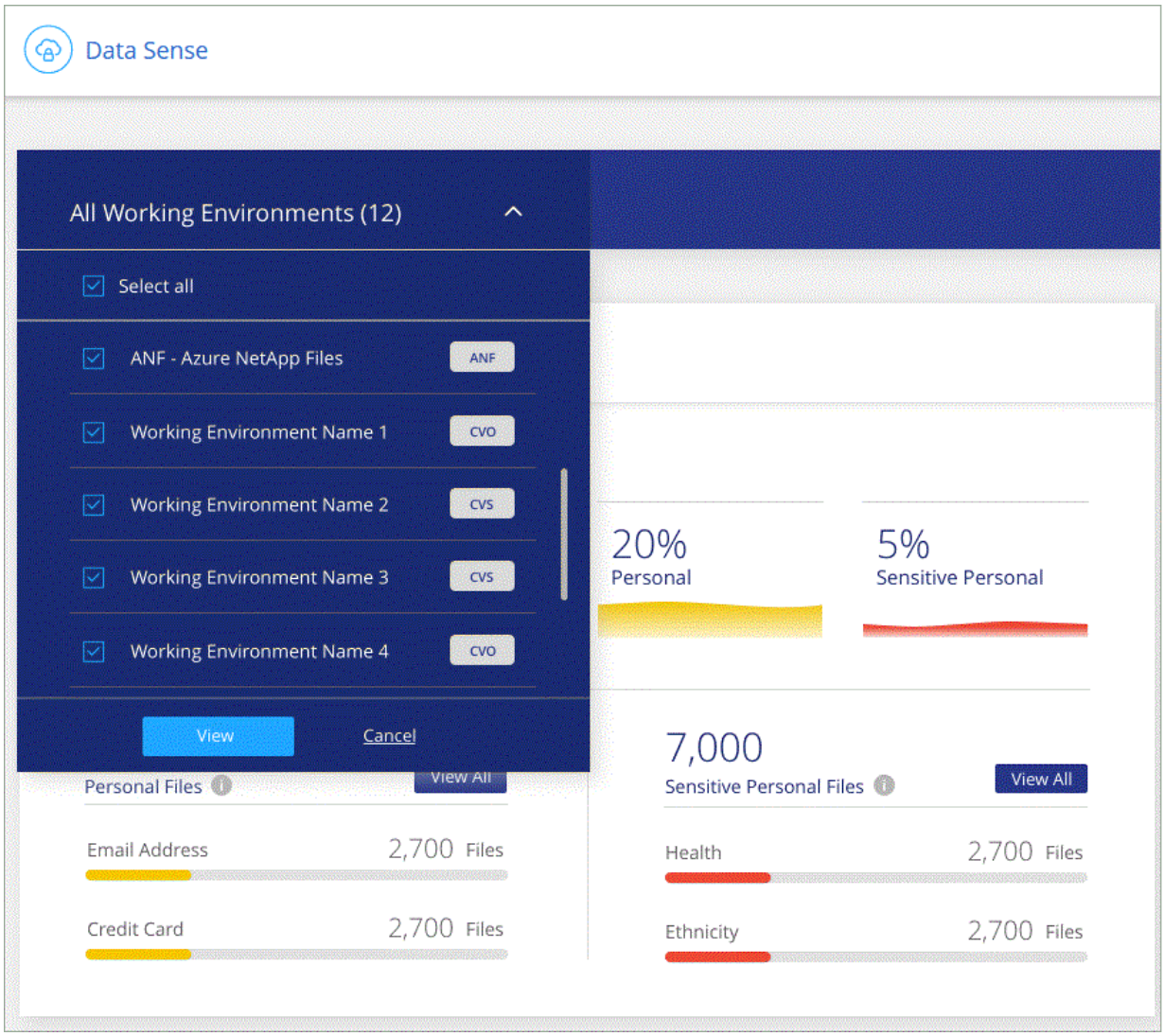
Selezionare gli ambienti di lavoro per i rapporti

È possibile filtrare i contenuti della dashboard di conformità della classificazione BlueXP per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando si filtra la dashboard, la classificazione BlueXP regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).


Data Sense
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
20%
Personal
5%
Sensitive Personal
Personal Files
View All
Email Address
2,700 Files
Credit Card
2,700 Files
7,000
Sensitive Personal Files
View All
Health
2,700 Files
Ethnicity
2,700 Files

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.