Cloud Data Sense Nutzen

Cloud Data Sense

NetApp
December 15, 2022

Inhaltsverzeichnis

Cloud Data Sense Nutzen

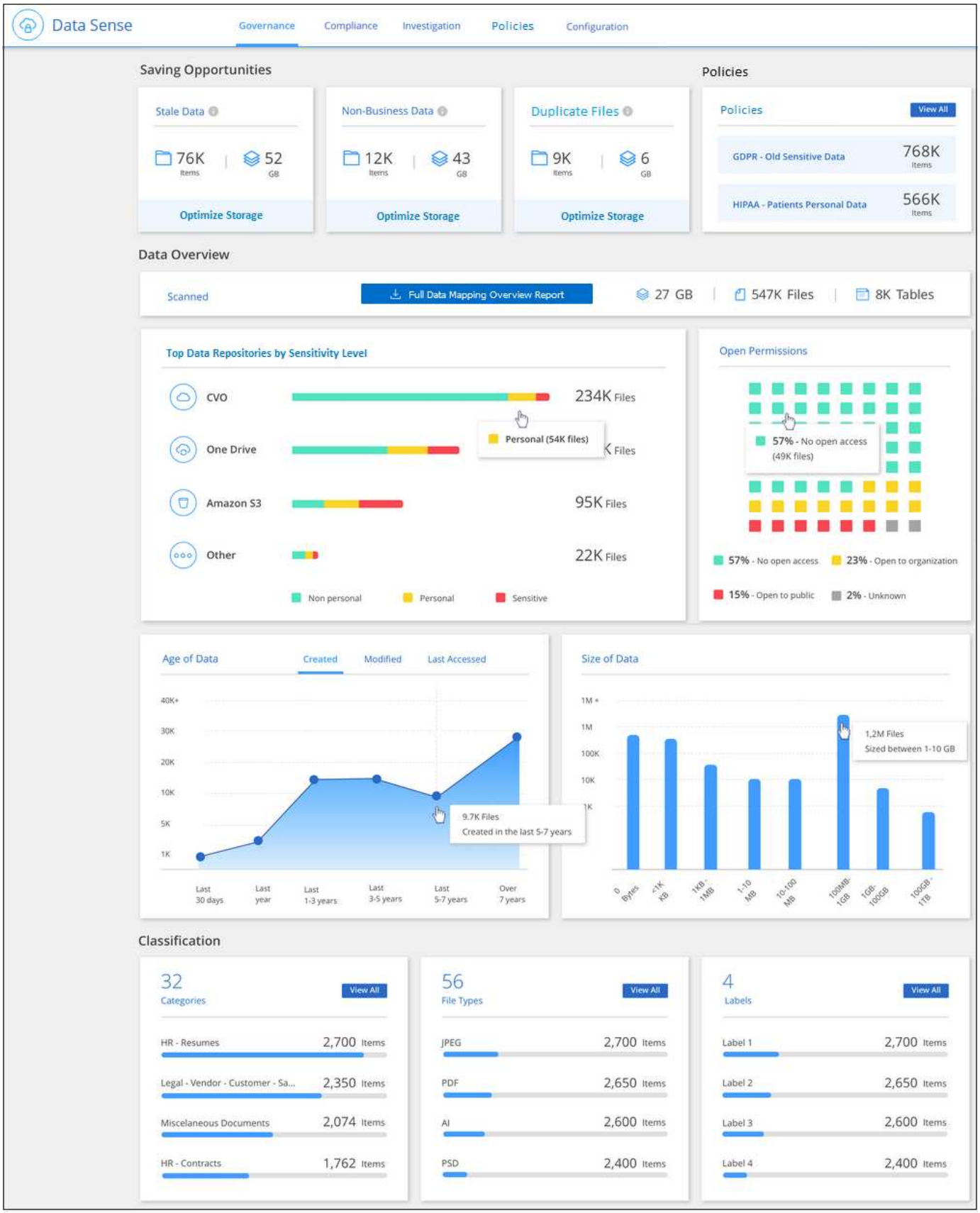
Anzeigen von Governance-Details zu den in Ihrem Unternehmen gespeicherten Daten

Behalten Sie die Kontrolle über die Kosten im Zusammenhang mit Daten auf den Storage-Ressourcen Ihres Unternehmens. Cloud Data Sense identifiziert die Menge der veralteten Daten, nicht Geschäftsdaten, duplizierten Dateien und sehr großen Dateien in Ihren Systemen. Somit können Sie entscheiden, ob Sie einige Dateien entfernen oder auf kostengünstigerem Objekt-Storage aufstellen möchten.

Wenn Sie Daten von On-Premises-Standorten in die Cloud migrieren möchten, können Sie vor der Verschiebung prüfen, ob alle Daten vertrauliche Informationen beinhalten.

Dashboard für Governance

Das Governance-Dashboard liefert Informationen, mit denen Sie die Effizienz steigern und die Kosten für die in Ihren Storage-Ressourcen gespeicherten Daten kontrollieren können.



Speichern Von Geschäftschancen

Möglicherweise möchten Sie die Elemente im Bereich „*Saving Opportunities*“ untersuchen, um zu sehen, ob es Daten gibt, die Sie löschen oder zu kostengünstigerem Objekt-Storage Tier verschieben sollten. Klicken Sie

auf die einzelnen Elemente, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen.

- **Veraltete Daten** - Daten die zuletzt vor über 3 Jahren geändert wurden.
- **Nicht-Geschäftsdaten** - Daten, die aufgrund ihrer Kategorie oder ihres Dateityps als nicht geschäftsbezogen gelten. Hierzu zählen folgende Optionen:
  - Applikationsdaten
  - Audio
  - Ausführbare Dateien
  - Bilder
  - Protokolle
  - Videos
  - Sonstiges (allgemeine Kategorie „Sonstige“)
- **Doppelte Dateien** - Dateien, die an anderen Orten in den Datenquellen, die Sie scannen, dupliziert werden. "Sehen Sie, welche Arten von duplizierten Dateien angezeigt werden".

Politik mit der größten Anzahl von Ergebnissen

Klicken Sie auf den Namen einer Richtlinie im Bereich *Policy*, um die Ergebnisse auf der Untersuchungsseite anzuzeigen. Klicken Sie auf **Alle anzeigen**, um die Liste aller verfügbaren Richtlinien anzuzeigen.

Klicken Sie Auf "Hier" Um mehr über Richtlinien zu erfahren.

Datenüberblick

Ein kurzer Überblick über alle Daten, die gescannt werden. Klicken Sie auf die Schaltfläche, um einen vollständigen Bericht zur Datenzuordnung herunterzuladen, der Nutzungskapazität, Alter der Daten, Größe der Daten und Dateitypen für alle Arbeitsumgebungen und Datenquellen enthält. Siehe "Datenzuordnungsbericht" Vollständige Angaben.

Die wichtigsten Daten-Repositorys, die nach Sensibilität aufgeführt sind

Der Bereich *Top Data Repositories by Sensitivity Level* enthält bis zu den vier wichtigsten Daten-Repositorys (Arbeitsumgebungen und Datenquellen), die die sensibelsten Elemente enthalten. Das Balkendiagramm für jede Arbeitsumgebung ist in folgende Kategorien unterteilt:

- Nicht personenbezogene Daten
- Persönliche Daten
- Sensible personenbezogene Daten

Sie können mit der Maus auf jeden Abschnitt zeigen, um die Gesamtanzahl der Elemente in jeder Kategorie anzuzeigen.

Klicken Sie auf die einzelnen Bereiche, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen, damit Sie weitere Untersuchungen machen können.

Daten, die nach Typen der offenen Berechtigungen aufgeführt sind

Der Bereich „*Open Permissions*“ zeigt den Prozentsatz für jeden Berechtigungstyp an, der für alle Dateien vorhanden ist, die gescannt werden. Das Diagramm zeigt die folgenden Berechtigungstypen:

- Kein Offener Zugriff
- Steht Unternehmen offen
- Öffentlich zugänglich
- Unbekannter Zugriff

Sie können mit der Maus auf jeden Abschnitt zeigen, um die Gesamtzahl der Dateien jeder Kategorie anzuzeigen. Klicken Sie auf die einzelnen Bereiche, um die gefilterten Ergebnisse auf der Untersuchungsseite anzuzeigen, damit Sie weitere Untersuchungen machen können.

Alter der Daten und Größe der Diagramme

Möglicherweise möchten Sie die Elemente in den Diagrammen *Age* und *Size* untersuchen, um zu sehen, ob Daten gelöscht oder in kostengünstigeren Objektspeicher verschoben werden sollten.

Sie können den Mauszeiger über einen Punkt in den Diagrammen bewegen, um Details zum Alter oder zur Größe der Daten in dieser Kategorie anzuzeigen. Klicken Sie hier, um alle Dateien anzuzeigen, die nach diesem Alter oder Größenbereich gefiltert sind.

- **Alter der Daten Graph** - kategorisiert Daten basierend auf dem Zeitpunkt der Erstellung, dem letzten Zugriff oder der letzten Änderung.
- **Größe des Datengraphen** - kategorisiert Daten basierend auf der Größe.

Die meisten ermittelten Datenklassifizierungen

Der Bereich *Classification* enthält eine Liste der am häufigsten identifizierten "Kategorien", "Dateitypen", und "AIP-Etiketten" In den gescannten Daten.

Kategorien

Kategorien können Ihnen dabei helfen, zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen, die Sie haben, zeigen. Beispielsweise kann eine Kategorie wie „Bewerbungen“ oder „Mitarbeiterverträge“ sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Siehe "Anzeigen von Dateien nach Kategorien" Finden Sie weitere Informationen.

Dateitypen

Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind.

Siehe "Anzeigen von Dateitypen" Finden Sie weitere Informationen.

AIP-Etiketten

Wenn Sie den Azure Information Protection (AIP) abonniert haben, können Sie Dokumente und Dateien klassifizieren und schützen, indem Sie Inhaltsetiketten anwenden. Durch die Überprüfung der am häufigsten verwendeten AIP-Etiketten, die Dateien zugeordnet sind, können Sie feststellen, welche Etiketten am häufigsten in Ihren Dateien verwendet werden.

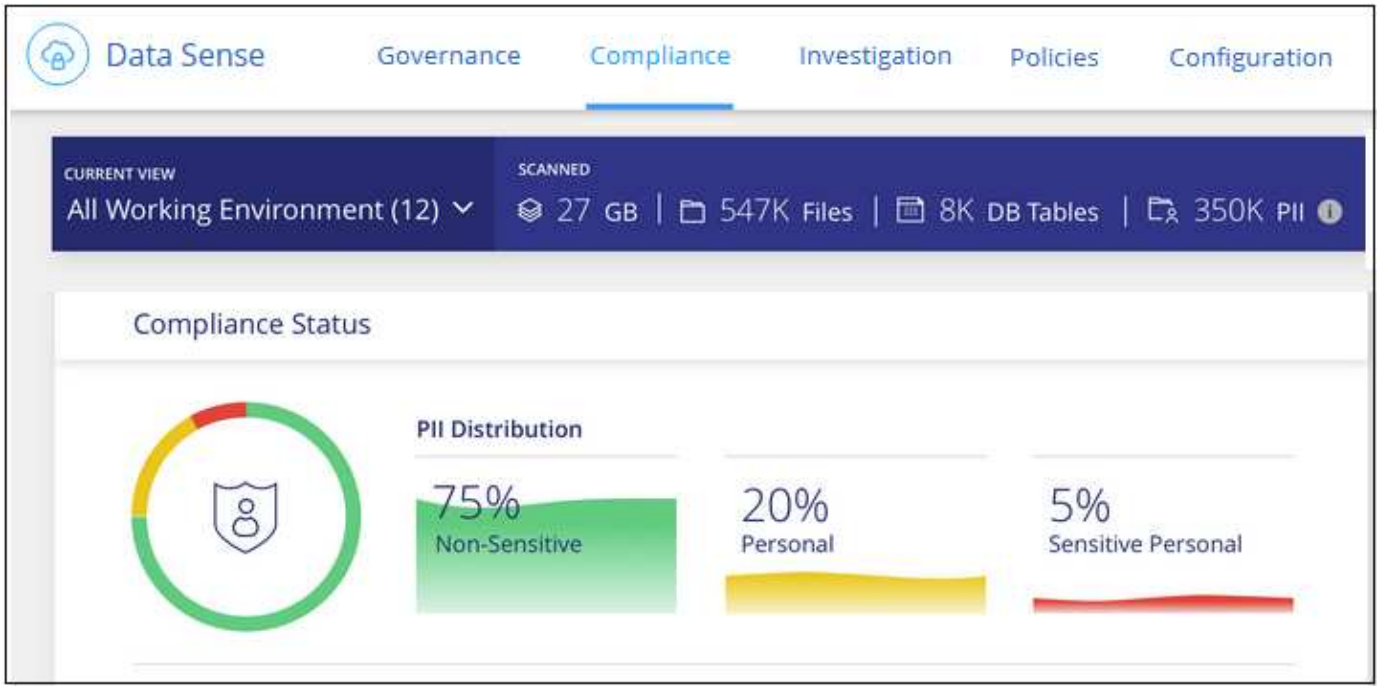
Siehe "AIP-Etiketten" Finden Sie weitere Informationen.

Anzeigen von Compliance-Details zu den in Ihrem Unternehmen gespeicherten Daten

Mehr Kontrolle über Ihre persönlichen Daten durch die Anzeige von Details zu den personenbezogenen Daten und vertraulichen personenbezogenen Daten in Ihrem Unternehmen. Lesen Sie auch die Kategorien und Dateitypen, die Cloud Data Sense in Ihren Daten finden, um für sich zu sorgen.

Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Standardmäßig werden im Cloud Data Sense Dashboard Compliance-Daten für alle Arbeitsumgebungen und Datenbanken angezeigt.



Wenn Sie Daten nur für einige der Arbeitsumgebungen sehen möchten, Wählen Sie diese Arbeitsumgebungen aus.

Sie können die Ergebnisse auch auf der Seite Datenuntersuchung filtern und einen Bericht der Ergebnisse als CSV-Datei herunterladen. Siehe Filtern von Daten auf der Seite „Datenuntersuchung“ Entsprechende Details.

Anzeigen von Dateien mit persönlichen Daten

Cloud Data Sense identifiziert automatisch bestimmte Wörter, Strings und Muster (Regex) in den Daten. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern, Kontonummern, Passwörter, Und vieles mehr. "Die vollständige Liste finden Sie hier". Data Sense identifiziert diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordnern) und in Datenbanktabellen.

Wenn Sie außerdem einen zu scannenden Datenbankserver hinzugefügt haben, können Sie mit der Funktion *Data Fusion* Ihre Dateien scannen, um festzustellen, ob eindeutige Identifikatoren aus Ihren Datenbanken in

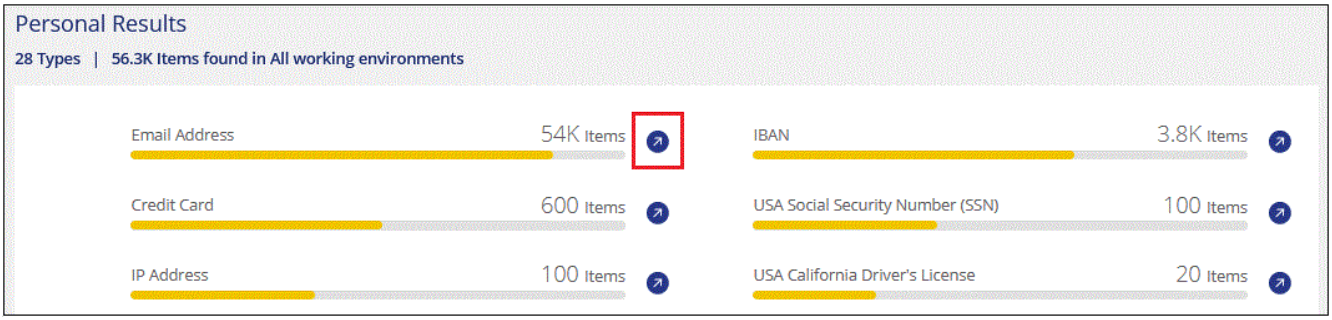
diesen Dateien oder anderen Datenbanken gefunden werden. Siehe "Hinzufügen von ID-Kennungen unter Verwendung von Data Fusion" Entsprechende Details.

Für einige Arten von persönlichen Daten verwendet Data Sense *Proximity Validation*, um seine Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. Data Sense identifiziert zum Beispiel ein US-amerikanisches Sozialversicherungsnummer (SSN) als SSN, wenn sie neben ihr ein Näherungswort sieht - zum Beispiel *SSN* oder *Sozialversicherung*. "Der Tisch der personenbezogenen Daten" Zeigt an, wenn Data Sense die Näherungsüberprüfung verwendet.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Um die Angaben zu allen personenbezogenen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz der persönlichen Daten.

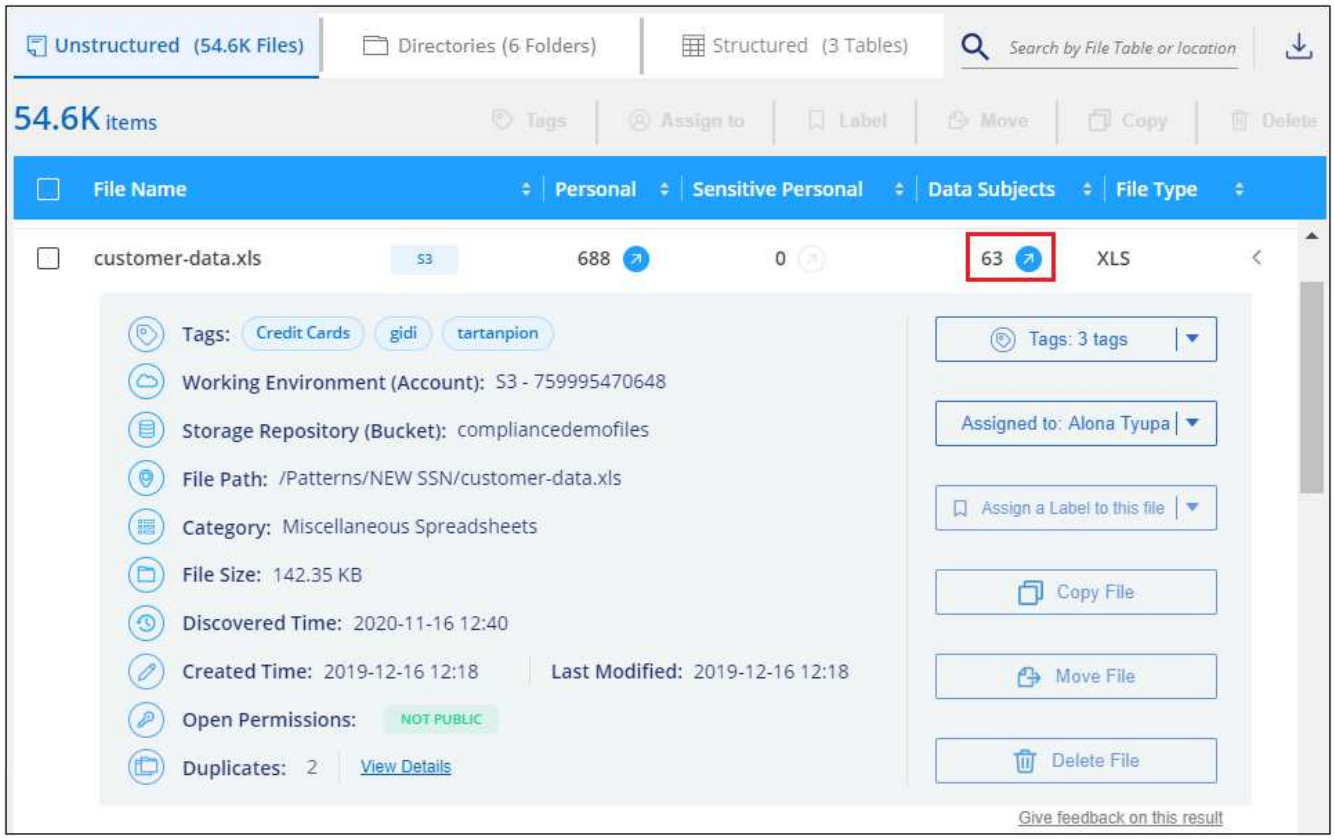
3. Um die Daten für eine bestimmte Art von personenbezogenen Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ von personenbezogenen Daten, z. B. E-Mail-Adressen.

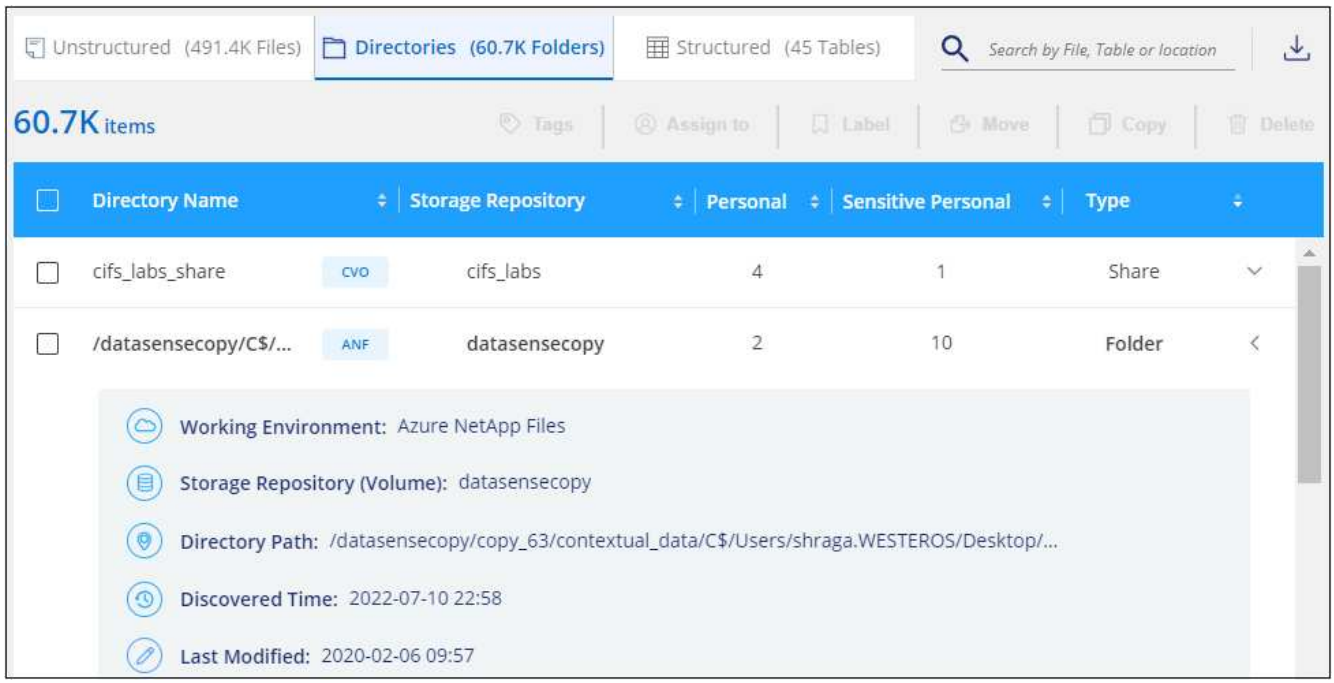


4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

   Die beiden Screenshots unten zeigen persönliche Daten in einzelnen Dateien gefunden, und in Dateien in Verzeichnissen (Freigaben und Ordner). Sie können auch die Registerkarte **Structured** auswählen, um

persönliche Daten in Datenbanken anzuzeigen.





Anzeigen von Dateien mit vertraulichen persönlichen Daten

Cloud Data Sense identifiziert automatisch spezielle Arten von sensiblen personenbezogenen Daten, wie sie in Datenschutzvorschriften wie z. B. definiert sind "Artikel 9 und 10 der DSGVO". Beispielsweise Informationen über die Gesundheit einer Person, ethnische Herkunft oder sexuelle Orientierung. "Die vollständige Liste finden Sie hier". Data Sense identifiziert diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb

von Verzeichnissen (Freigaben und Ordnern) und in Datenbanktabellen.

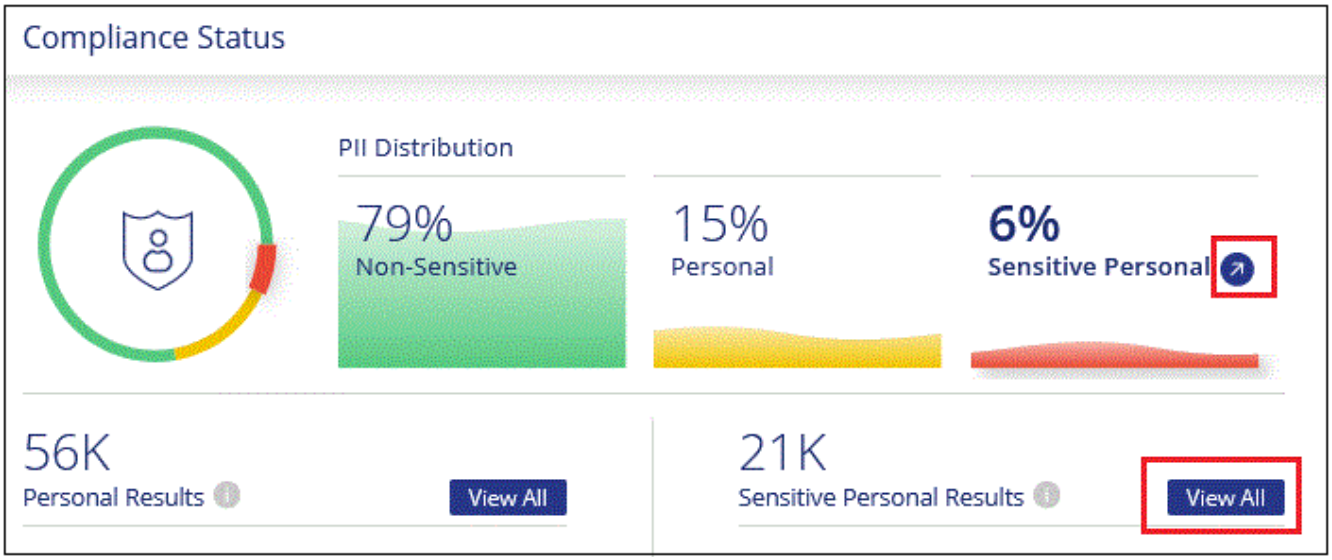
Cloud Data Sense verwendet künstliche Intelligenz (KI), NLP (Natural Language Processing), maschinelles Lernen (ML) und Cognitive Computing (CC), um die Bedeutung des Inhalts, den es scannt, zu verstehen, um Entitäten zu extrahieren und entsprechend zu kategorisieren.

Beispielsweise ist eine sensitive DSGVO-Datenkategorie ethnisch Ursprungs. Aufgrund seiner NLP-Fähigkeiten kann Data Sense den Unterschied zwischen einem Satz unterscheiden, der "George ist Mexican" (mit vertraulichen Daten wie in Artikel 9 der DSGVO angegeben), und "George isst mexikanische Lebensmittel".

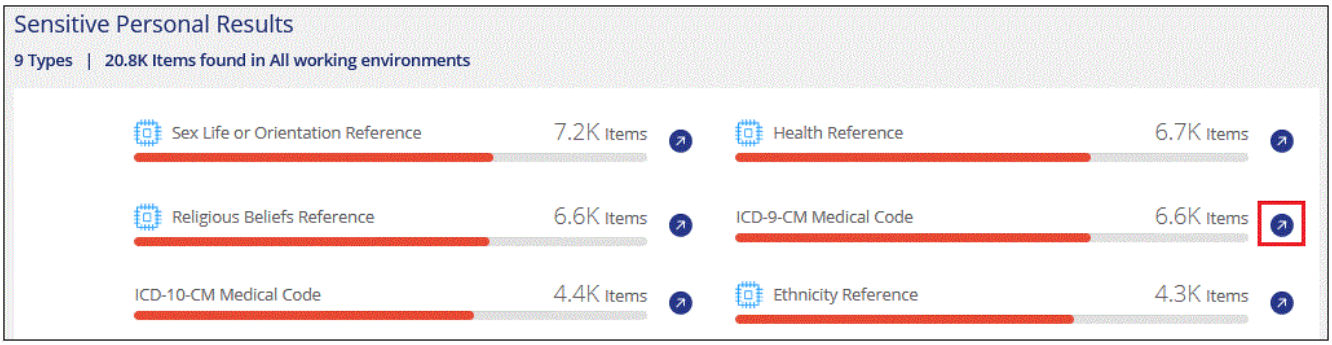
Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Um die Details für alle sensiblen persönlichen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz sensibler personenbezogener Daten.



3. Um die Details für eine bestimmte Art sensibler personenbezogener Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und klicken Sie dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ sensibler personenbezogener Daten.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern,

auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Anzeigen von Dateien nach Kategorien

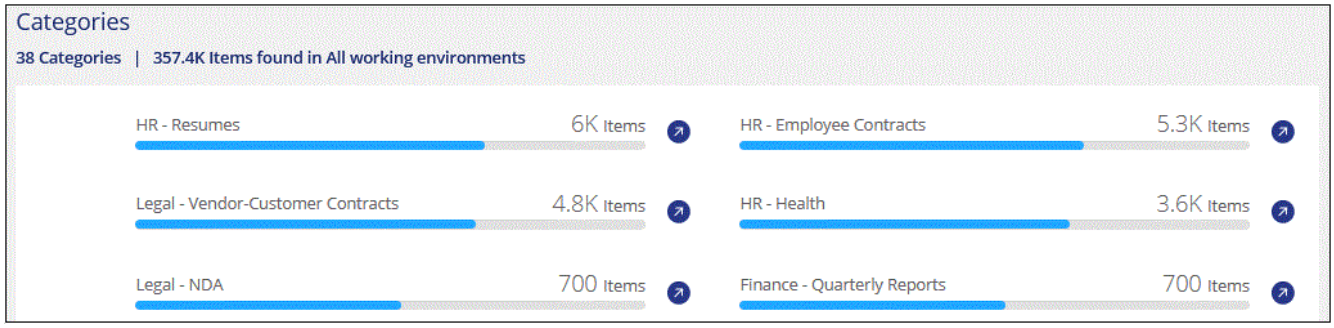
Cloud Data Sense verwendet die gescannten Daten und unterteilt sie in verschiedene Kategorien. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Siehe die Liste der Kategorien".

Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie Lebensläufe oder Mitarbeiterverträge sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Englisch, Deutsch und Spanisch werden für Kategorien unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für eine der 4 Top-Kategorien direkt im Hauptbildschirm oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für eine der Kategorien.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Anzeigen von Dateien nach Dateitypen

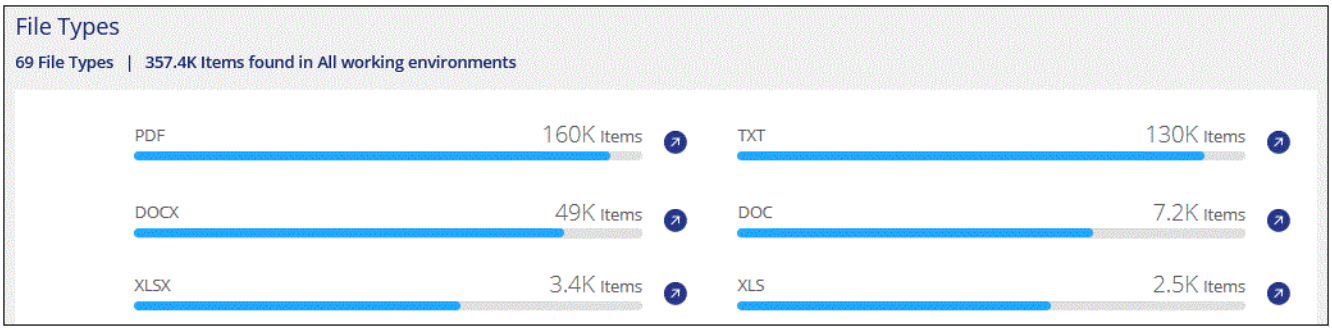
Cloud Data Sense verwendet die gescannten Daten und werden nach Dateityp unterteilt. Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind. "Siehe die Liste der Dateitypen".

Sie können beispielsweise CAD-Dateien speichern, die sehr sensible Informationen über Ihr Unternehmen enthalten. Wenn diese nicht gesichert sind, können Sie die Kontrolle über vertrauliche Daten übernehmen, indem Sie Berechtigungen beschränken oder Dateien an einen anderen Speicherort verschieben.

Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die Registerkarte **Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für einen der 4 wichtigsten Dateitypen direkt vom Hauptbildschirm aus, oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für einen der

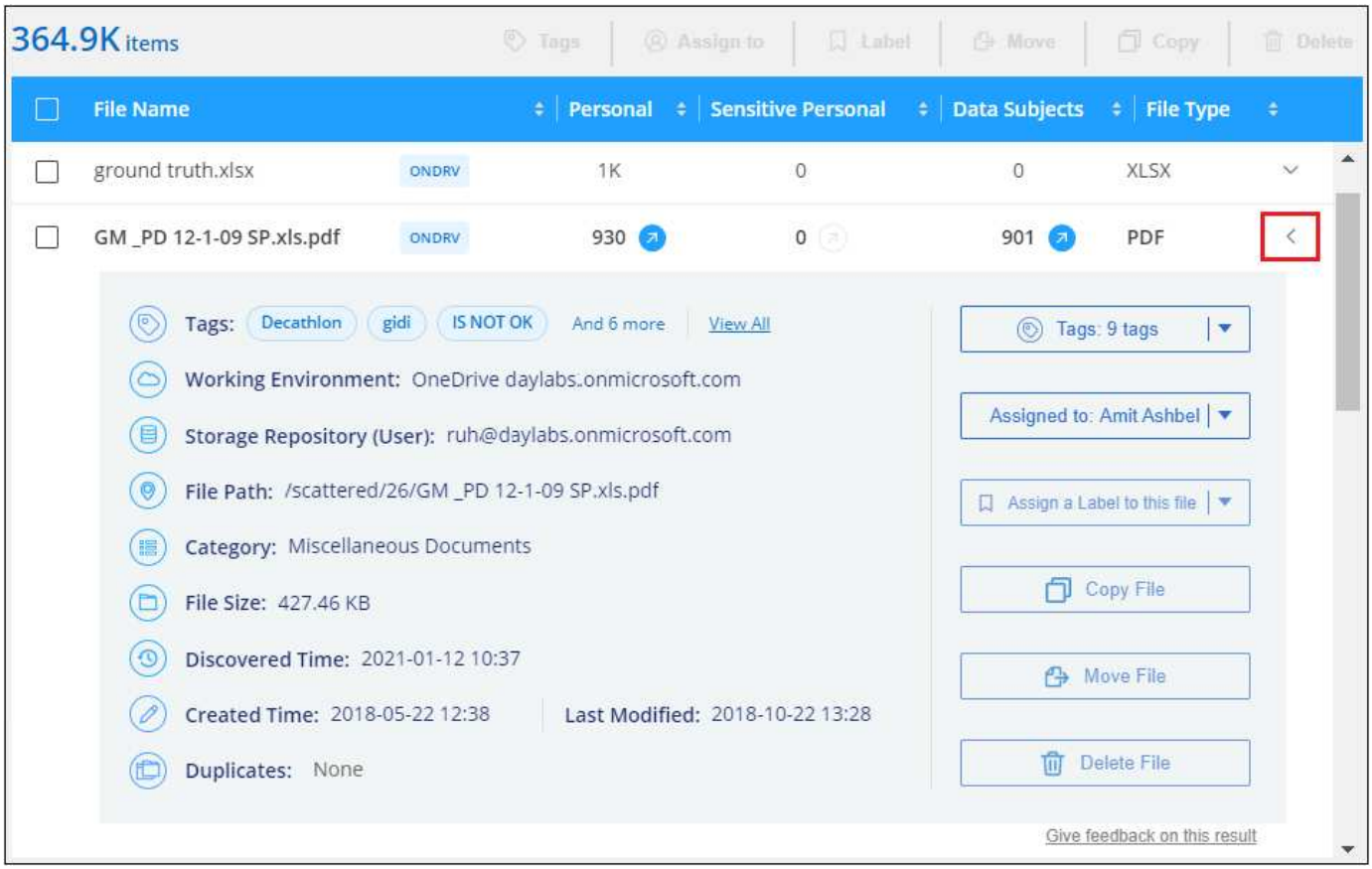
Dateitypen.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Anzeigen von Dateimetadaten

Klicken Sie im Bereich „Untersuchungsergebnisse“ auf Für jede einzelne Datei, um die Dateimetadaten anzuzeigen.



Zusätzlich zur Anzeige der Arbeitsumgebung und des Volumes, in dem sich die Datei befindet, werden durch die Metadaten viel mehr Informationen angezeigt, einschließlich der Dateiberechtigungen, des Dateieigentümers, ob es Duplikate dieser Datei gibt und des zugewiesenen AIP-Etiketts (falls vorhanden) "Integrierte AIP in Cloud Data Sense"). Diese Informationen sind hilfreich, wenn Sie Vorhaben "Erstellen von Richtlinien" Da Sie alle Informationen anzeigen können, die Sie zum Filtern Ihrer Daten verwenden können.

Beachten Sie, dass nicht alle Informationen für alle Datenquellen verfügbar sind – und genau die

Informationen, die sich für diese Datenquelle eignen. Beispielsweise sind der Volume-Name, die Berechtigungen und AIP-Labels nicht für Datenbankdateien relevant.

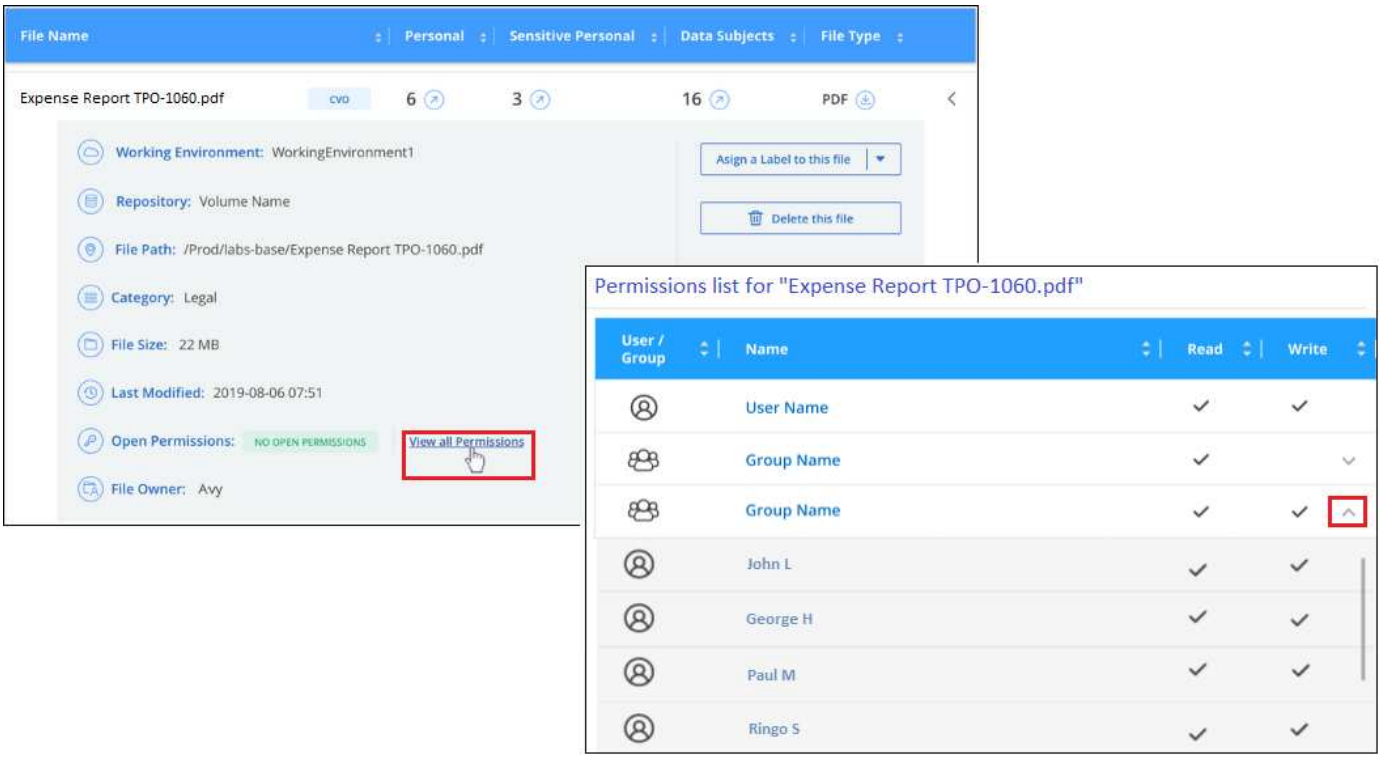
Wenn Sie die Details für eine einzelne Datei anzeigen, gibt es einige Aktionen, die Sie für die Datei ergreifen können:

- Sie können die Datei verschieben oder in eine beliebige NFS-Freigabe kopieren. Siehe "Quelldateien werden in eine NFS-Freigabe verschoben" Und "Quelldateien werden in eine NFS-Freigabe kopiert" Entsprechende Details.
- Sie können die Datei löschen. Siehe "Quelldateien werden gelöscht" Entsprechende Details.
- Sie können der Datei einen bestimmten Status zuweisen. Siehe "Tags werden angewendet" Entsprechende Details.
- Sie können die Datei einem BlueXP-Benutzer zuweisen, damit er für alle Follow-up-Aktionen verantwortlich ist, die in der Datei ausgeführt werden müssen. Siehe "Zuweisen von Benutzern zu einer Datei" Entsprechende Details.
- Wenn Sie AIP-Etiketten mit Cloud Data Sense integriert haben, können Sie dieser Datei eine Bezeichnung zuweisen oder zu einer anderen Bezeichnung wechseln, wenn sie bereits vorhanden ist. Siehe "Manuelles Zuweisen von AIP-Beschriftungen" Entsprechende Details.

Anzeigen von Berechtigungen für Dateien und Verzeichnisse

Um eine Liste aller Benutzer oder Gruppen anzuzeigen, die Zugriff auf eine Datei oder ein Verzeichnis haben, und die Arten von Berechtigungen, die sie haben, klicken Sie auf **Alle Berechtigungen anzeigen**. Diese Schaltfläche gilt nur für Daten in CIFS Shares, SharePoint Online, SharePoint On-Premises und OneDrive.

Beachten Sie, dass Sie Active Directory in Data Sense integrieren sollten, wenn Sie SIDs (Security Identifiers) anstelle von Benutzer- und Gruppennamen sehen. "So geht's".



Klicken Sie auf ⌄ Für jede Gruppe, um die Liste der Benutzer anzuzeigen, die Teil der Gruppe sind.

Darüber Hinaus Sie können auf den Namen eines Benutzers oder einer Gruppe klicken und die Untersuchungsseite wird mit dem Namen dieses Benutzers oder dieser Gruppe angezeigt, der im Filter „Benutzer-/Gruppenberechtigungen“ ausgefüllt ist, sodass Sie alle Dateien und Verzeichnisse sehen können, auf die der Benutzer oder die Gruppe Zugriff hat.

In den Storage-Systemen werden nach doppelten Dateien gesucht

Sie können sehen, ob doppelte Dateien auf Ihren Storage-Systemen gespeichert werden. Dies ist nützlich, wenn Sie Bereiche ermitteln möchten, in denen Sie Speicherplatz einsparen können. Zudem ist es hilfreich, sicherzustellen, dass Dateien mit bestimmten Berechtigungen oder vertraulichen Informationen in Ihren Speichersystemen nicht unnötig dupliziert werden.

Data Sense verwendet Hashing-Technologie zur Bestimmung doppelter Dateien. Wenn eine Datei den gleichen Hash-Code wie eine andere Datei hat, können wir zu 100% sicher sein, dass die Dateien exakte Duplikate sind - auch wenn die Dateinamen unterschiedlich sind.

Sie können die Liste mit doppelten Dateien herunterladen und an Ihren Storage-Administrator senden, damit er jederzeit entscheiden kann, welche Dateien gelöscht werden können. Oder Sie können "Löschen Sie die Datei" Wenn Sie sicher sind, dass keine bestimmte Version der Datei benötigt wird.

Anzeigen aller duplizierten Dateien

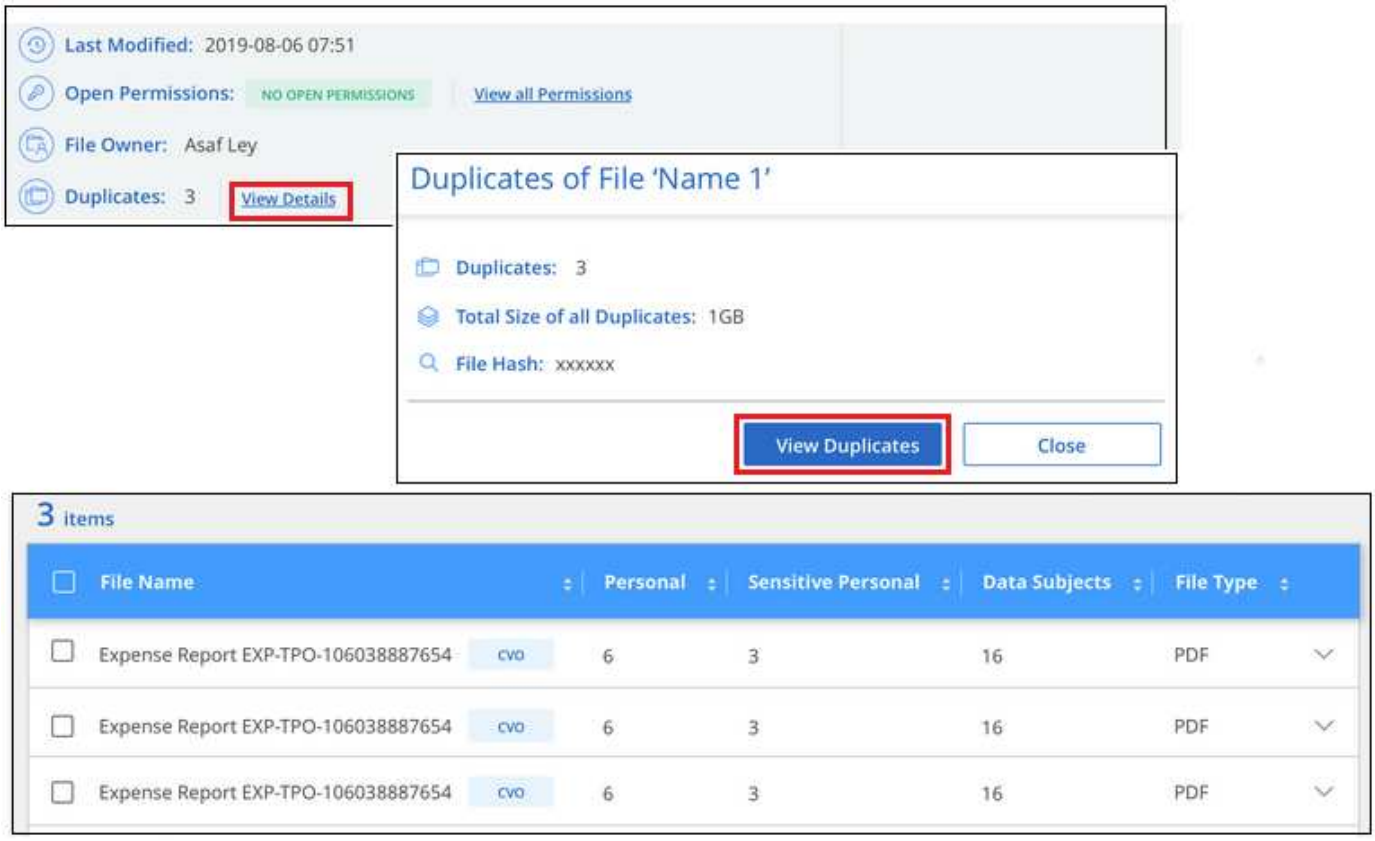
Wenn Sie eine Liste aller Dateien wünschen, die in den Arbeitsumgebungen und Datenquellen, die Sie scannen, dupliziert werden, können Sie den Filter **Duplicates > has Dubletten** auf der Seite Data Investigation verwenden.

Alle Dateien mit Duplikaten aus allen Dateitypen (ohne Datenbanken), mit einer Mindestgröße von 50 MB und/oder mit persönlichen oder sensiblen persönlichen Informationen, werden auf der Ergebnisseite angezeigt.

Anzeigen, ob eine bestimmte Datei doppelt vorhanden ist

Wenn Sie sehen möchten, ob eine einzelne Datei Duplikate enthält, klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für jede einzelne Datei, um die Dateimetadaten anzuzeigen. Wenn es Duplikate einer bestimmten Datei gibt, werden diese Informationen neben dem Feld *Duplicates* angezeigt.

Klicken Sie auf **Details anzeigen**, um die Liste der duplizierten Dateien anzuzeigen und wo sie sich befinden. Klicken Sie auf der nächsten Seite auf **Duplicates anzeigen**, um die Dateien auf der Untersuchungsseite anzuzeigen.



Sie können den auf dieser Seite angegebenen "Datei-Hash"-Wert verwenden und direkt auf der Untersuchungsseite eingeben, um jederzeit nach einer bestimmten doppelten Datei zu suchen - oder Sie können sie in einer Richtlinie verwenden.

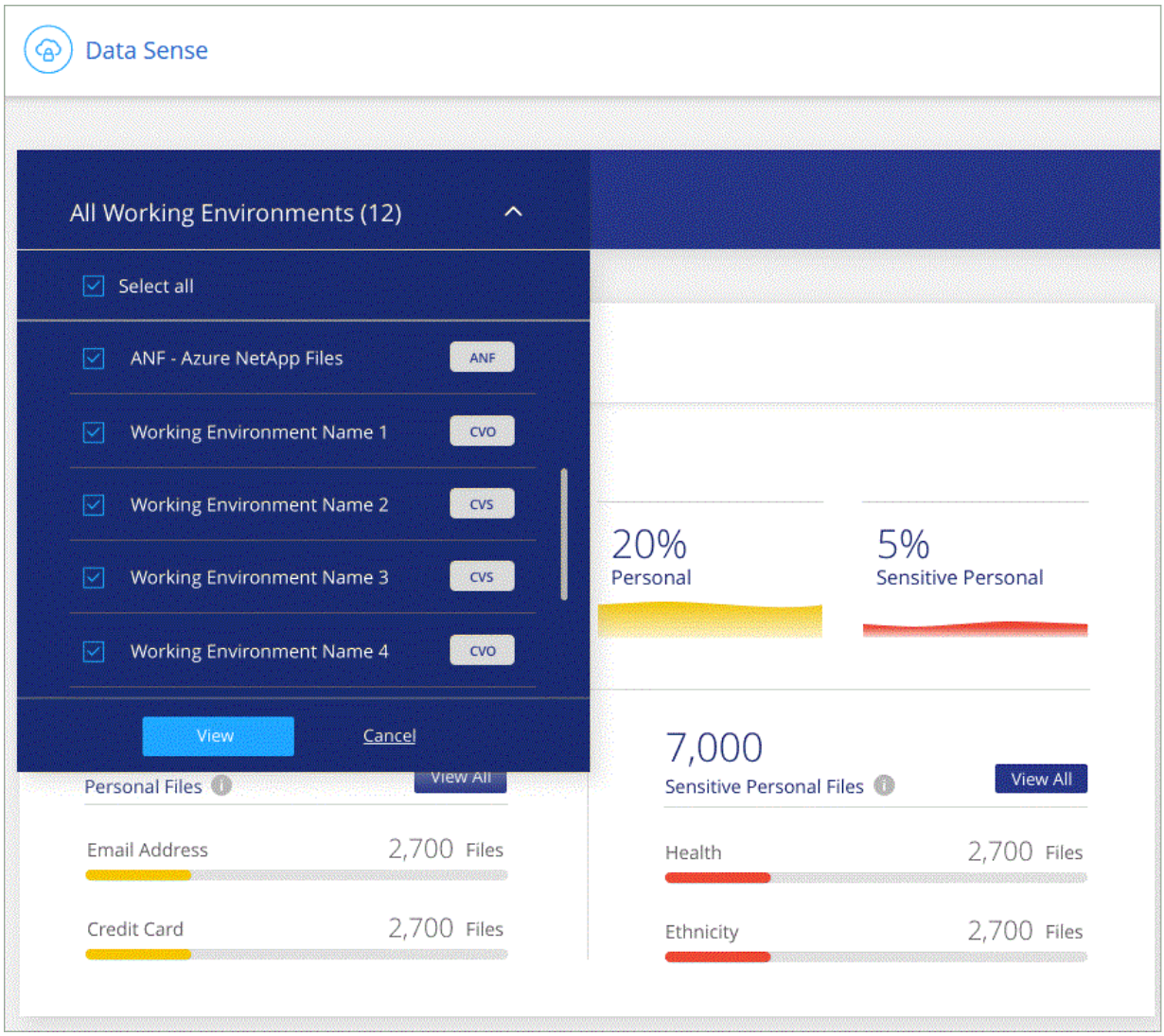
Anzeigen von Dashboard-Daten für bestimmte Arbeitsumgebungen

Sie können die Inhalte des Cloud Data Sense Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur bestimmte Arbeitsumgebungen anzuzeigen.

Wenn Sie das Dashboard filtern, können Sie mit Data Sense die Compliance-Daten und -Berichte genau auf die von Ihnen ausgewählten Arbeitsumgebungen anwenden.

Schritte

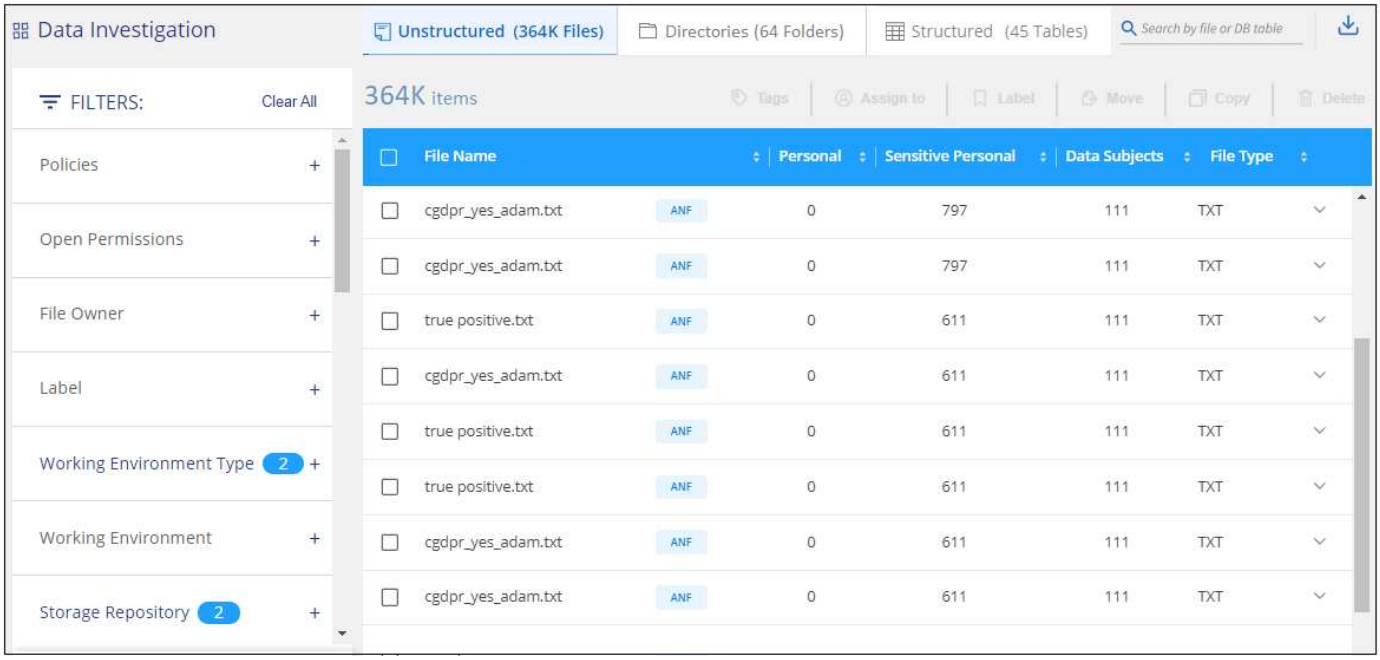
1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.



Filtern von Daten auf der Seite „Datenuntersuchung“

Sie können den Inhalt der Untersuchungsseite filtern, um nur die Ergebnisse anzuzeigen, die Sie sehen möchten. Dies ist eine sehr leistungsstarke Funktion, denn nachdem Sie die Daten verfeinert haben, können Sie die Buttonleiste oben auf der Seite verwenden, um eine Vielzahl von Aktionen durchzuführen, wie das Kopieren von Dateien, Verschieben von Dateien, Hinzufügen eines Tags oder AIP-Label zu den Dateien und vieles mehr.

Wenn Sie den Inhalt der Seite nach der Verarbeitung als Bericht herunterladen möchten, klicken Sie auf die Schaltfläche Schaltfläche. Sie können den Bericht lokal als .CSV-Datei (die bis zu 5,000 Datenzeilen umfassen kann) oder als JSON-Datei speichern, die Sie in eine NFS-Freigabe exportieren (die eine unbegrenzte Anzahl von Zeilen enthalten kann). "Weitere Informationen zu Untersuchungsberichten finden Sie hier".



- Auf den Registerkarten der obersten Ebene können Sie Daten aus Dateien (unstrukturierte Daten), Verzeichnissen (Ordner und Dateifreigaben) oder aus Datenbanken (strukturierte Daten) anzeigen.
- Mit den Steuerelementen oben in jeder Spalte können Sie die Ergebnisse in numerischer oder alphabetischer Reihenfolge sortieren.
- Mit den Filtern im linken Fensterbereich können Sie die Ergebnisse verfeinern, indem Sie aus den folgenden Attributen auswählen:

Filtern	Details
Richtlinien	Wählen Sie eine Richtlinie oder Richtlinien aus. Los "Hier" Um die Liste der vorhandenen Richtlinien anzuzeigen und eigene Richtlinien zu erstellen.
Analysestatus	Wählen Sie eine Option aus, um die Liste der Dateien anzuzeigen, die den ersten Scan ausstehend, den Scanvorgang abgeschlossen haben, den ausstehenden Rescan oder die nicht gescannt wurden.
Öffnen Sie Berechtigungen	Wählen Sie den Berechtigungstyp innerhalb der Daten und in Ordnern/Shares aus
Benutzer-/Gruppenberechtigungen	Wählen Sie einen oder mehrere Benutzernamen und/oder Gruppennamen aus, oder geben Sie einen Teilnamen ein
Dateieigentümer	Geben Sie den Namen des Dateieigentümers ein
Etikett	Wählen Sie "AIP-Etiketten" Die Ihren Dateien zugewiesen sind
Art Der Arbeitsumgebung	Wählen Sie den Typ der Arbeitsumgebung aus. OneDrive, SharePoint und Google Drive sind unter „Apps“ kategorisiert.
Name der Arbeitsumgebung	Wählen Sie spezielle Arbeitsumgebungen aus
Storage Repository	Wählen Sie das Speicher-Repository aus, z. B. ein Volume oder ein Schema
Dateipfad	Geben Sie einen Teil- oder vollständigen Pfad ein

Filtern	Details
Kategorie	Wählen Sie die aus "Arten von Kategorien"
Empfindlichkeitsstufe	Wählen Sie die Empfindlichkeitsstufe aus: Persönlich, sensibel persönlich oder nicht empfindlich
Anzahl der Kennungen	Wählen Sie den Bereich der erkannten empfindlichen Kennungen pro Datei aus. Hierzu zählen personenbezogene Daten und sensible personenbezogene Daten. Beim Filtern in Verzeichnissen werden die Matches von allen Dateien in jedem Ordner (und Unterordnern) angezeigt.
Persönliche Daten	Wählen Sie die aus "Arten personenbezogener Daten"
Sensible Personenbezogene Daten	Wählen Sie die aus "Arten sensibler personenbezogener Daten"
Betroffene Person	Geben Sie den vollständigen Namen oder die bekannte Kennung eines Betroffenen ein
Verzeichnistyp	Wählen Sie den Verzeichnistyp aus, entweder „Share“ oder „Folder“.
Dateityp	Wählen Sie die aus "Dateitypen"
Dateigröße	Wählen Sie den Dateigrößenbereich aus
Erstellungszeit	Wählen Sie einen Bereich aus, in dem die Datei erstellt wurde
Entdeckte Zeit	Wählen Sie einen Bereich aus, in dem Data Sense die Datei entdeckt hat
Zuletzt Geändert	Wählen Sie einen Bereich aus, in dem die Datei zuletzt geändert wurde
Zuletzt Aufgerufen	Wählen Sie einen Bereich aus, auf den die Datei zuletzt zugegriffen wurde. Bei den Dateitypen, die von Data Sense gescannt werden, ist dies das letzte Mal, wenn Data Sense die Datei gescannt hat.
Duplikate	Wählen Sie aus, ob die Datei in den Repositorys dupliziert wird
Datei-Hash	Geben Sie den Hash der Datei ein, um eine bestimmte Datei zu finden, selbst wenn der Name anders ist
Tags	Wählen Sie "Das Tag oder die Tags" Die Ihren Dateien zugewiesen sind
Zugewiesen Zu	Wählen Sie den Namen der Person aus, der die Datei zugeordnet ist

Beachten Sie, dass die in der Schaltflächenleiste und in den Richtlinien verfügbaren Aktionen derzeit nicht auf der Ebene „Verzeichnis“ unterstützt werden.

Organisieren von privaten Daten

Cloud Data Sense bietet zahlreiche Möglichkeiten für das Management und die Organisation von privaten Daten. Auf diese Weise können Sie die für Sie wichtigsten Daten besser einsehen.

- Wenn Sie abonniert sind "Azure Information Protection (AIP)" Zum Klassifizieren und Schützen Ihrer

Dateien können Sie Cloud Data Sense verwenden, um diese AIP-Etiketten zu verwalten.

- Sie können Tags zu Dateien hinzufügen, die Sie als Organisation oder für eine Art von Follow-up markieren möchten.
- Sie können einen BlueXP-Benutzer einer bestimmten Datei oder mehreren Dateien zuweisen, sodass diese Person für das Management der Datei verantwortlich ist.
- Mit der "Policy"-Funktion können Sie Ihre eigenen individuellen Suchanfragen erstellen, so dass Sie die Ergebnisse einfach durch Klicken auf eine Schaltfläche sehen können.
- Sie können Benachrichtigungen per E-Mail an BlueXP-Benutzer senden, wenn bestimmte kritische Richtlinien Ergebnisse liefern.

Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Sollte ich Etiketten oder Etiketten verwenden?

Nachfolgend sehen Sie einen Vergleich zwischen Data Sense Tagging und Azure Information Protection Labeling.

Tags	Etiketten
Datei-Tags sind ein integrierter Bestandteil von Data Sense.	Voraussetzung ist, dass Sie den Azure Information Protection (AIP) abonniert haben.
Das Tag wird nur in der Data Sense Datenbank gespeichert - es wird nicht in die Datei geschrieben. Die Datei oder die abgerufene oder geänderte Datei werden nicht geändert.	Die Bezeichnung ist Teil der Datei, und wenn sich die Bezeichnung ändert, ändert sich die Datei. Diese Änderung ändert auch die Zeiten, auf die zugegriffen wurde und die geändert wurden.
Sie können mehrere Tags für eine einzelne Datei haben.	Sie können eine Bezeichnung auf einer einzelnen Datei haben.
Das Tag kann für interne Datensense-Aktion verwendet werden, z. B. Kopieren, Verschieben, Löschen, Ausführen einer Richtlinie, Usw.	Andere Systeme, die die Datei lesen können, können das Etikett sehen - welches für zusätzliche Automatisierung verwendet werden kann.
Nur ein einzelner API-Aufruf wird verwendet, um zu sehen, ob eine Datei ein Tag hat.	

Kategorisieren Sie Ihre Daten mit AIP-Etiketten

Sie können AIP-Etiketten in den Dateien verwalten, die Cloud Data Sense scannt, wenn Sie abonniert haben "Azure Information Protection (AIP)". Mit AIP können Sie Dokumente und Dateien klassifizieren und schützen, indem Sie Etiketten auf Inhalte anwenden. Mit „Data Sense“ können Sie die bereits zugewiesenen Beschriftungen anzeigen, Dateien Beschriftungen hinzufügen und Etiketten ändern, wenn bereits eine Bezeichnung vorhanden ist.

Cloud Data Sense unterstützt AIP-Etiketten in den folgenden Dateitypen: .DOC, .DOCX, .PDF, .PPTX, .XLS, .XLSX

- Sie können zurzeit keine Etiketten in Dateien ändern, die größer als 30 MB sind. Für OneDrive, SharePoint und Google Drive Konten die maximale Dateigröße beträgt 4 MB.
- Wenn eine Datei ein Label hat, das in AIP nicht mehr existiert, wird sie von Cloud Data Sense als Datei ohne Etikett betrachtet.
- Wenn Sie Data Sense in einer Regierungsregion oder an einem lokalen Standort bereitgestellt haben, der keinen Internetzugang hat (auch als dunkle Site bezeichnet), ist die AIP-Label-Funktion nicht verfügbar.

Integrieren von AIP-Etiketten in Ihren Arbeitsbereich

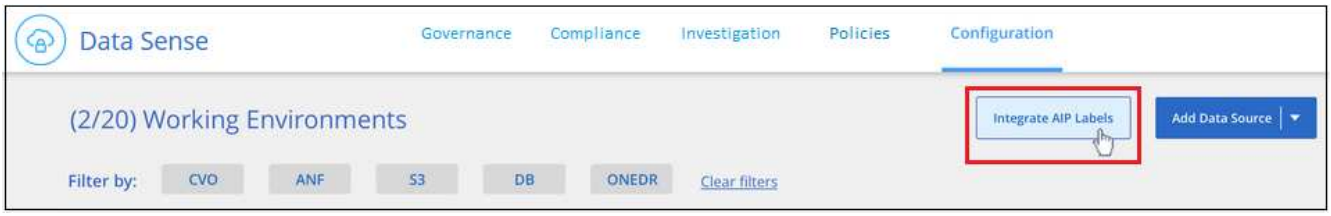
Bevor Sie AIP-Etiketten verwalten können, müssen Sie die AIP-Label-Funktion in Cloud Data Sense integrieren, indem Sie sich in Ihrem bestehenden Azure-Konto anmelden. Nach der Aktivierung können Sie AIP-Beschriftungen in Dateien für alle verwalten "Datenquellen" In Ihrem BlueXP Workspace.

Anforderungen

- Sie benötigen ein Konto und eine Azure Information Protection-Lizenz.
- Sie müssen die Anmeldedaten für das Azure-Konto besitzen.
- Wenn Sie Etiketten in Dateien ändern möchten, die in Amazon S3 Buckets gespeichert sind, stellen Sie die Berechtigung sicher `s3:PutObject` Ist in der IAM-Rolle enthalten. Siehe "Einrichten der IAM-Rolle".

Schritte

1. Klicken Sie auf der Seite Cloud Data Sense Configuration auf **AIP Labels integrieren**.



2. Klicken Sie im Dialogfeld AIP-Etiketten integrieren auf **in Azure anmelden**.
3. Wählen Sie auf der angezeigten Microsoft-Seite das Konto aus, und geben Sie die erforderlichen Anmeldedaten ein.
4. Kehren Sie zur Registerkarte Cloud Data Sense zurück, und Sie sehen die Meldung "*AIP-Labels wurden erfolgreich in das Konto <Account_Name>* integriert.
5. Klicken Sie auf **Schließen** und Sie sehen den Text *AIP Labels integriert* oben auf der Seite.

Ergebnis

Sie können AIP-Beschriftungen im Ergebnisbereich der Untersuchungsseite anzeigen und zuweisen. Außerdem können Sie Dateien mithilfe von Richtlinien AIP-Etiketten zuweisen.

Anzeigen von AIP-Etiketten in Ihren Dateien

Sie können die aktuelle AIP-Bezeichnung anzeigen, die einer Datei zugewiesen ist.

Klicken Sie im Bereich „Untersuchungsergebnisse“ auf Für die Datei zum erweitern der Dateimetadaten.

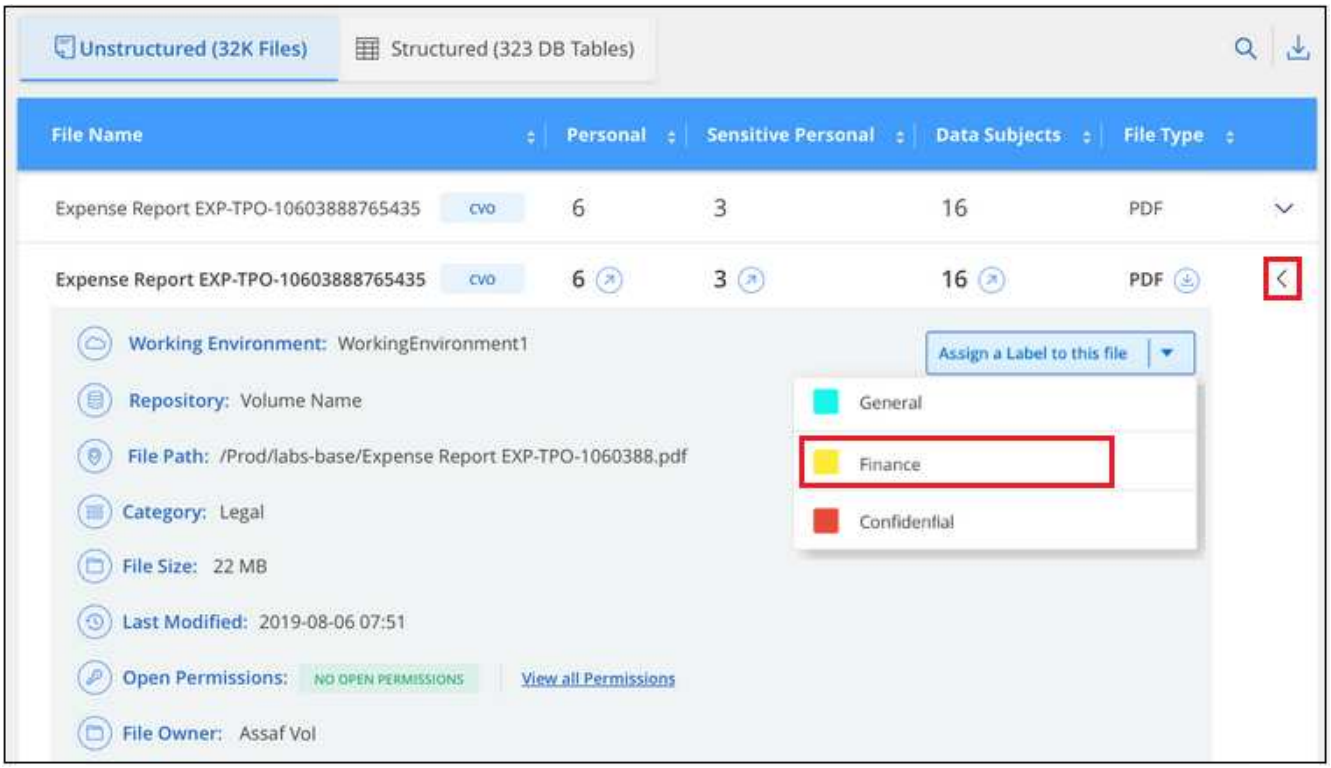
Manuelles Zuweisen von AIP-Beschriftungen

Mit Cloud Data Sense können Sie AIP-Etiketten aus Ihren Dateien hinzufügen, ändern und entfernen.

Führen Sie diese Schritte aus, um einer einzelnen Datei eine AIP-Bezeichnung zuzuweisen.

Schritte

1. Klicken Sie im Bereich „Untersuchungsergebnisse“ auf Für die Datei zum erweitern der Dateimetadaten.



2. Klicken Sie auf **Etikett dieser Datei zuweisen** und wählen Sie dann die Beschriftung aus.

   Die Beschriftung wird in den Dateimetadaten angezeigt.

So weisen Sie mehreren Dateien eine AIP-Bezeichnung zu:

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie beschriften möchten.

   - Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
   - Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).

2. Klicken Sie in der Symbolleiste auf **Etikett** und wählen Sie die AIP-Bezeichnung:

   Die AIP-Bezeichnung wird den Metadaten für alle ausgewählten Dateien hinzugefügt.

Automatisches Zuweisen von AIP-Etiketten mit Richtlinien

Sie können allen Dateien, die die Kriterien der Richtlinie erfüllen, eine AIP-Beschriftung zuweisen. Sie können beim Erstellen der Richtlinie das AIP-Etikett angeben oder die Beschriftung beim Bearbeiten einer Richtlinie hinzufügen.

Etiketten werden kontinuierlich in Dateien hinzugefügt oder aktualisiert, wenn Cloud Data Sense Ihre Dateien scannt.

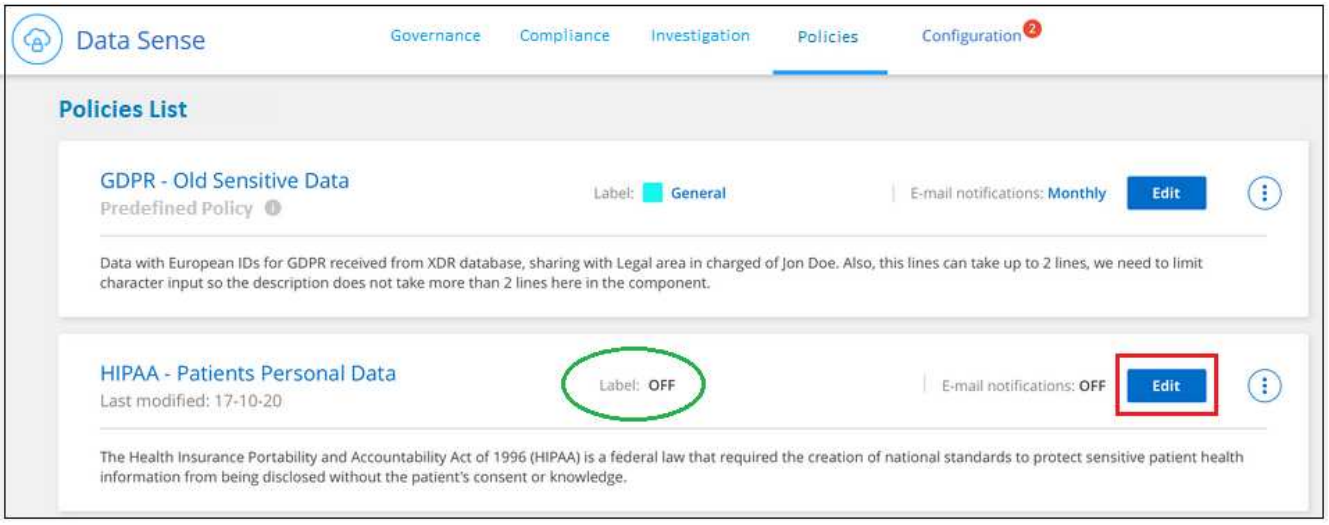
Je nachdem, ob bereits ein Label auf eine Datei und die Klassifizierungsstufe des Etiketts angewendet wurde, werden beim Ändern einer Bezeichnung folgende Aktionen ausgeführt:

Wenn die Datei…	Dann…
Hat kein Etikett	Die Beschriftung wird hinzugefügt
Verfügt über ein bereits vorhandenes Etikett mit einer niedrigeren Klassifizierungsstufe	Das Etikett der höheren Ebene wird hinzugefügt
Verfügt über ein bereits vorhandenes Etikett mit einer höheren Klassifizierungsstufe	Das Etikett der höheren Ebene bleibt erhalten
Wird eine Bezeichnung sowohl manuell als auch von einer Richtlinie zugewiesen	Das Etikett der höheren Ebene wird hinzugefügt
Ist zwei Richtlinien zugewiesen	Das Etikett der höheren Ebene wird hinzugefügt

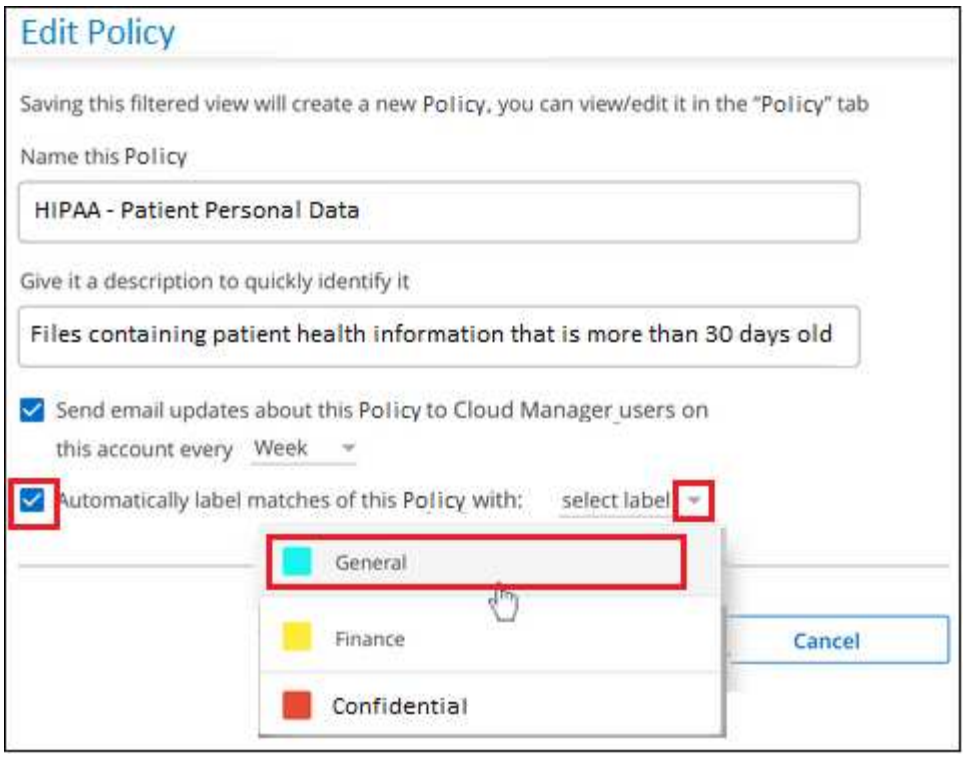
Führen Sie diese Schritte aus, um einer vorhandenen Richtlinie eine AIP-Beschriftung hinzuzufügen.

Schritte

1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, in der Sie die AIP-Bezeichnung hinzufügen (oder ändern) möchten.



2. Aktivieren Sie auf der Seite Richtlinie bearbeiten das Kontrollkästchen, um automatische Beschriftungen für Dateien zu aktivieren, die den Richtlinieparametern entsprechen, und wählen Sie die Beschriftung aus (z. B. **Allgemein**).



3. Klicken Sie auf **Save Policy** und das Etikett wird in der Policy description angezeigt.

Wenn eine Richtlinie mit einem Etikett konfiguriert wurde, die Bezeichnung aber seitdem von AIP entfernt wurde, wird der Name der Bezeichnung auf AUS gesetzt und die Bezeichnung nicht mehr zugewiesen.

Entfernen der AIP-Integration

Wenn Sie AIP-Beschriftungen in Dateien nicht mehr verwalten möchten, können Sie das AIP-Konto aus der Cloud Data Sense Schnittstelle entfernen.

Beachten Sie, dass die Etiketten, die Sie mit Data Sense hinzugefügt haben, nicht geändert werden. Die in Dateien vorhandenen Beschriftungen bleiben so, wie sie derzeit vorhanden sind.

Schritte

1. Klicken Sie auf der Seite *Configuration* auf **AIP Labels integriert > Integration entfernen**.

2. Klicken Sie im Bestätigungsdialogfeld auf **Integration entfernen**.

Anwenden von Tags zur Verwaltung der gescannten Dateien

Sie können Dateien, die Sie für eine Art von Follow-up markieren möchten, ein Tag hinzufügen. Sie haben z. B. einige doppelte Dateien gefunden und möchten eine davon löschen, müssen aber überprüfen, welche Dateien gelöscht werden sollen. Sie könnten der Datei einen Tag mit "Prüfen zum Löschen" hinzufügen, damit Sie wissen, dass diese Datei eine Recherche und eine Art von zukünftigen Aktionen erfordert.

Mit „Data Sense“ können Sie die Tags anzeigen, die Dateien zugewiesen sind, Tags hinzufügen oder aus Dateien entfernen und den Namen ändern oder ein vorhandenes Tag löschen.

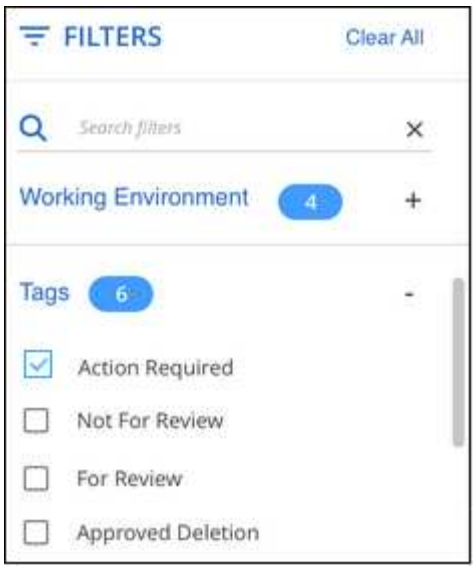
Beachten Sie, dass das Tag der Datei nicht auf die gleiche Weise hinzugefügt wird wie AIP-Etiketten Teil der Dateimetadaten sind. Das Tag wird gerade von BlueXP-Benutzern mit Cloud Data Sense angezeigt, so dass Sie sehen können, ob eine Datei gelöscht oder für eine Art von Follow-up überprüft werden muss.

Tags, die Dateien in Cloud Data Sense zugewiesen wurden, stehen nicht in Verbindung mit den Tags, die Sie Ressourcen hinzufügen können, wie Volumes oder Instanzen von virtuellen Maschinen. Auf Dateiebene werden Daten-SENSE-Tags angewendet.

Anzeigen von Dateien, auf die bestimmte Tags angewendet wurden

Sie können alle Dateien anzeigen, denen bestimmte Tags zugewiesen sind.

1. Klicken Sie in Cloud Data Sense auf die Registerkarte **Untersuchung**.
2. Klicken Sie auf der Seite Datenuntersuchung im Bereich Filter auf **Tags** und wählen Sie die gewünschten Tags aus.



Im Bereich Untersuchungsergebnisse werden alle Dateien angezeigt, denen diese Tags zugewiesen sind.

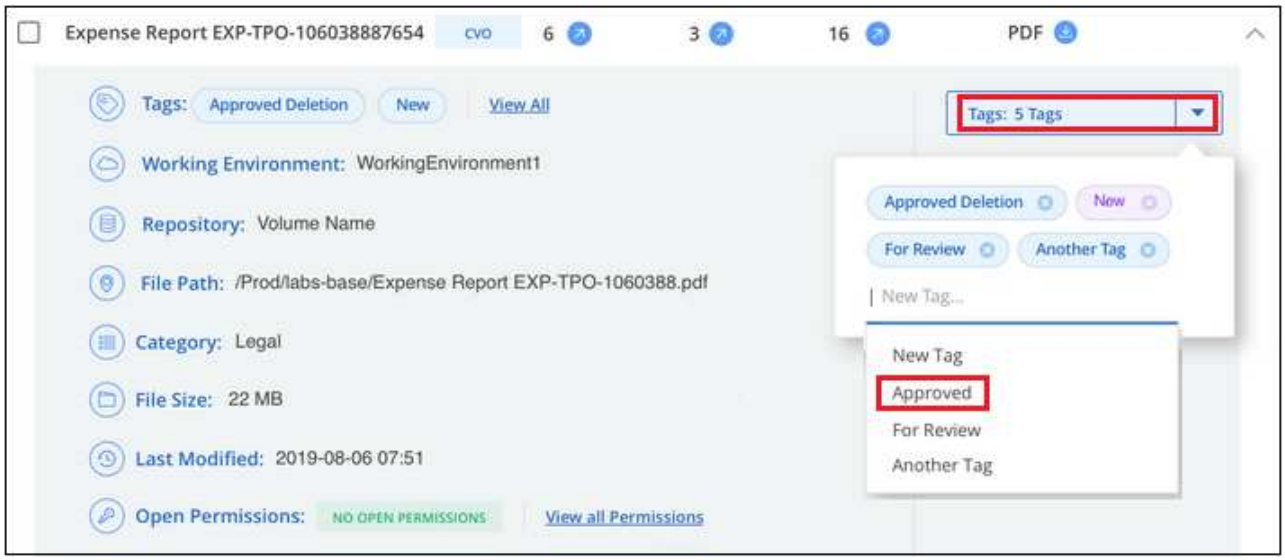
Tags zu Dateien werden zugewiesen

Sie können Tags zu einer einzelnen Datei oder zu einer Gruppe von Dateien hinzufügen.

So fügen Sie einer einzelnen Datei ein Tag hinzu:

Schritte

1. Klicken Sie im Bereich „Untersuchungsergebnisse“ auf ⌄ Für die Datei zum erweitern der Dateimetadaten.
2. Klicken Sie auf das Feld **Tags** und die aktuell zugewiesenen Tags werden angezeigt.
3. Tag oder Tags hinzufügen:
   - Um ein vorhandenes Tag zuzuweisen, klicken Sie in das Feld **Neues Tag…** und geben den Namen des Tags ein. Wenn das gesuchte Tag angezeigt wird, wählen Sie es aus, und drücken Sie **Enter**.
   - Um ein neues Tag zu erstellen und es der Datei zuzuweisen, klicken Sie in das Feld **New Tag…**, geben Sie den Namen des neuen Tags ein und drücken Sie **Enter**.



Das Tag wird in den Dateimetadaten angezeigt.

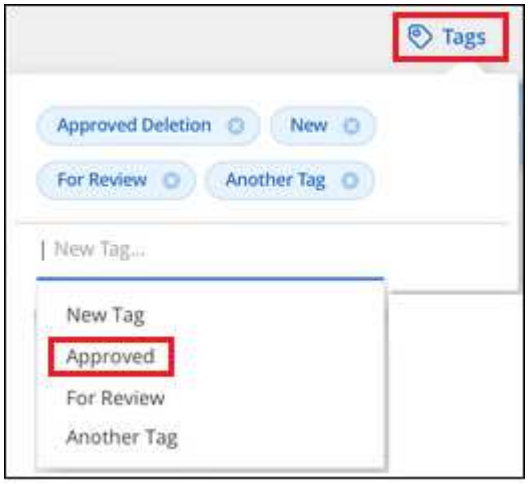
So fügen Sie einem mehrere Dateien ein Tag hinzu:

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die markiert werden sollen.

   - Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
   - Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).

2. Klicken Sie in der Buttonleiste auf **Tags** und die aktuell zugewiesenen Tags werden angezeigt.
3. Tag oder Tags hinzufügen:
    - Um ein vorhandenes Tag zuzuweisen, klicken Sie in das Feld **Neues Tag…** und geben den Namen des Tags ein. Wenn das gesuchte Tag angezeigt wird, wählen Sie es aus, und drücken Sie **Enter**.
    - Um ein neues Tag zu erstellen und es der Datei zuzuweisen, klicken Sie in das Feld **New Tag…**, geben Sie den Namen des neuen Tags ein und drücken Sie **Enter**.



4. Genehmigen Sie das Hinzufügen der Tags im Bestätigungsdialogfeld, und die Tags werden den Metadaten für alle ausgewählten Dateien hinzugefügt.

Tags aus Dateien werden gelöscht

Sie können ein Tag löschen, wenn Sie es nicht mehr verwenden müssen.

Klicken Sie einfach auf das **x** für ein vorhandenes Tag.

Wenn Sie mehrere Dateien ausgewählt haben, wird das Tag aus allen Dateien entfernt.

Zuweisen von Benutzern zum Verwalten bestimmter Dateien

Sie können einen BlueXP-Benutzer einer bestimmten Datei oder mehreren Dateien zuweisen, so dass diese Person für alle Follow-up-Aktionen verantwortlich sein kann, die in der Datei ausgeführt werden müssen. Diese Funktion wird häufig zusammen mit der Funktion verwendet, um einer Datei benutzerdefinierte Status-Tags hinzuzufügen.

Sie können beispielsweise eine Datei mit bestimmten personenbezogenen Daten haben, die zu vielen Benutzern Lese- und Schreibzugriff (offene Berechtigungen) ermöglicht. Sie können also das Status-Tag "Berechtigungen ändern" zuweisen und diese Datei dem Benutzer "Joan Smith" zuweisen, damit er entscheiden kann, wie das Problem behoben werden kann. Wenn sie das Problem behoben haben, könnten sie die Status-Tag-Nummer auf „Abgeschlossen“ ändern.

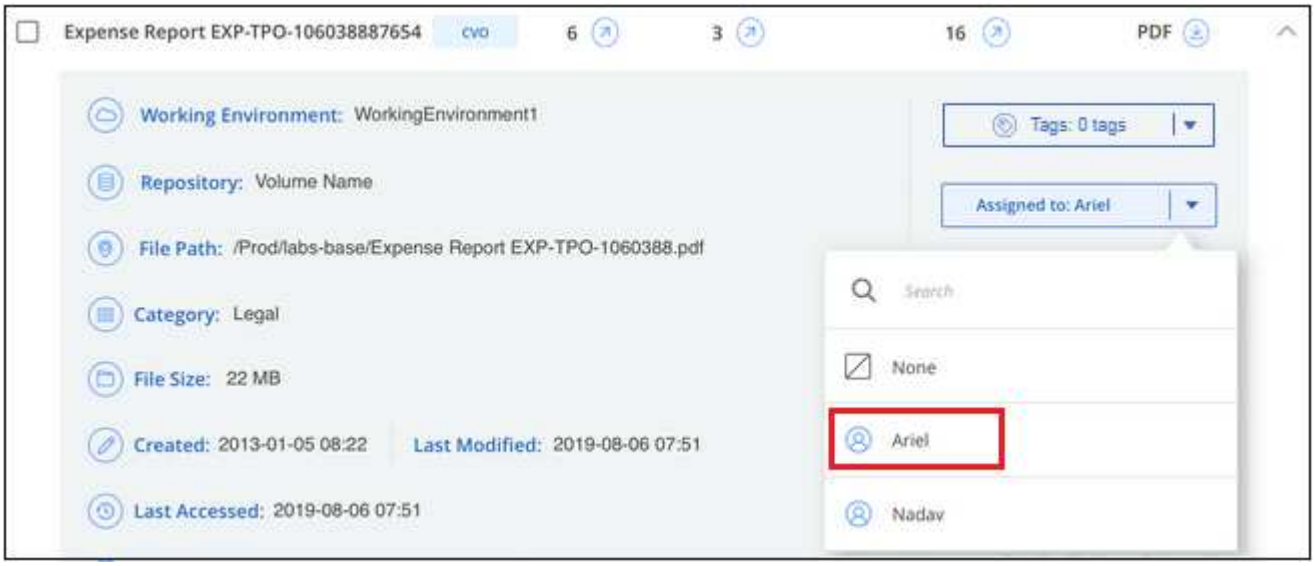
Beachten Sie, dass der Benutzername der Datei nicht als Teil der Dateimetadaten hinzugefügt wird - er wird gerade von BlueXP Benutzern bei der Verwendung von Cloud Data Sense angezeigt.

Mit einem neuen Filter auf der Untersuchungsseite können Sie problemlos alle Dateien anzeigen, die dieselbe Person im Feld „Assigned to“ haben.

So weisen Sie einen Benutzer einer einzelnen Datei zu:

Schritte

1. Klicken Sie im Bereich „Untersuchungsergebnisse“ auf Für die Datei zum erweitern der Dateimetadaten.
2. Klicken Sie auf das Feld **Assigned to** und wählen Sie den Benutzernamen aus.



Der Benutzername wird in den Dateimetadaten angezeigt.

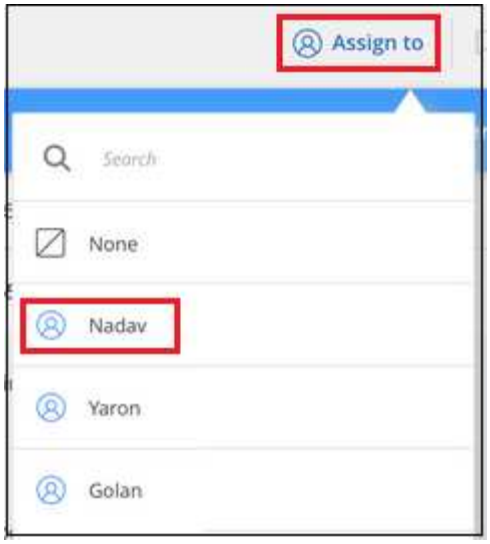
So weisen Sie einen Benutzer mehreren Dateien zu:

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie einem Benutzer zuweisen möchten.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).

2. Klicken Sie in der Symbolleiste auf **Zuweisen zu** und wählen Sie den Benutzernamen aus:



Der Benutzer wird den Metadaten für alle ausgewählten Dateien hinzugefügt.

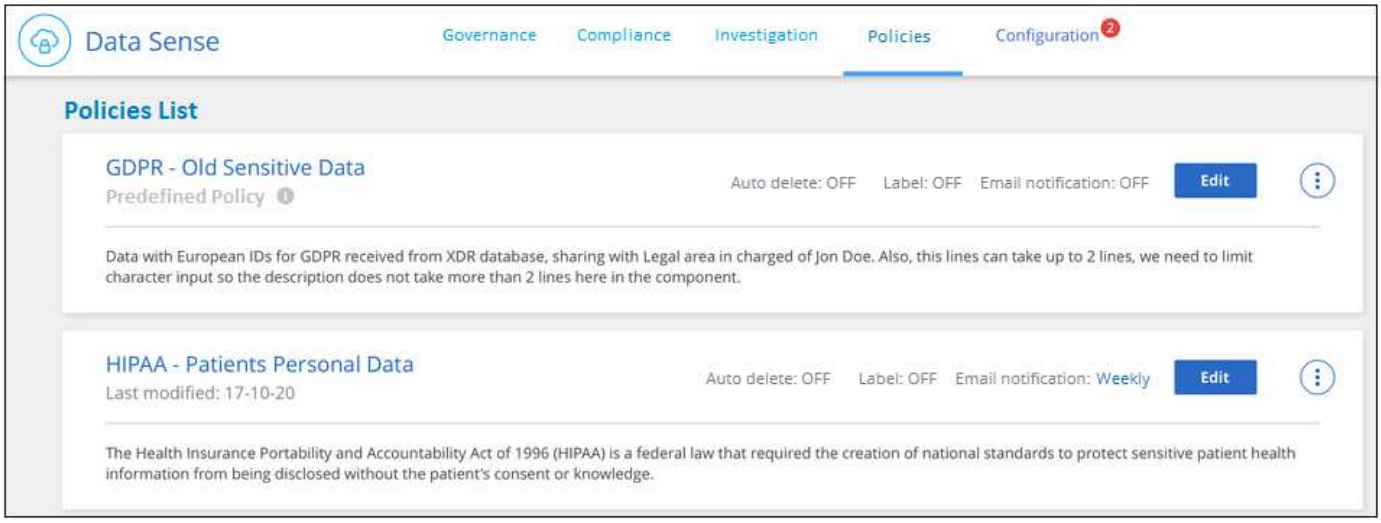
Kontrolle Ihrer Daten mithilfe von Richtlinien

Richtlinien sind wie eine Favoritenliste mit benutzerdefinierten Filtern, die Suchergebnisse auf der Untersuchungsseite für häufig angeforderte Compliance-Abfragen liefern. Cloud Data Sense bietet einen Satz vordefinierter Richtlinien, die auf gängigen Kundenanfragen basieren. Sie können benutzerdefinierte Richtlinien erstellen, die Ergebnisse für die Suche liefern, die speziell auf Ihr Unternehmen zugeschnitten sind.

Richtlinien bieten folgende Funktionen:

- Vordefinierte Richtlinien Von NetApp basierend auf Benutzeranfragen
- Möglichkeit, eigene benutzerdefinierte Richtlinien zu erstellen
- Starten Sie die Untersuchungsseite mit den Ergebnissen Ihrer Richtlinien mit nur einem Klick
- Senden Sie E-Mail-Benachrichtigungen an BlueXP-Benutzer, wenn bestimmte kritische Richtlinien Ergebnisse zurückgeben, damit Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten können
- Weisen Sie AIP-Etiketten (Azure Information Protection) automatisch allen Dateien zu, die den in einer Richtlinie definierten Kriterien entsprechen
- Löschen Sie Dateien automatisch (einmal pro Tag), wenn bestimmte Richtlinien Ergebnisse zurückgeben, damit Sie Ihre Daten automatisch schützen können

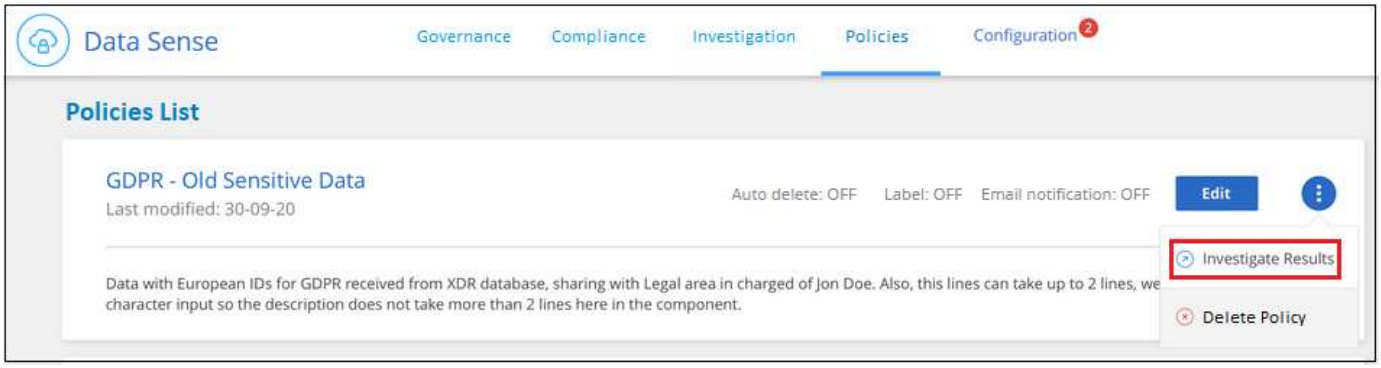
Auf der Registerkarte **Richtlinien** im Compliance Dashboard werden alle vordefinierten und benutzerdefinierten Richtlinien aufgelistet, die auf dieser Instanz von Cloud Data Sense verfügbar sind.



Darüber hinaus werden Richtlinien in der Liste der Filter auf der Untersuchungsseite angezeigt.

Anzeigen von Policy-Ergebnissen auf der Untersuchungsseite

Um die Ergebnisse für eine Richtlinie auf der Untersuchungsseite anzuzeigen, klicken Sie auf die Klicken Sie für eine bestimmte Richtlinie, und wählen Sie dann **Ergebnisse untersuchen**.



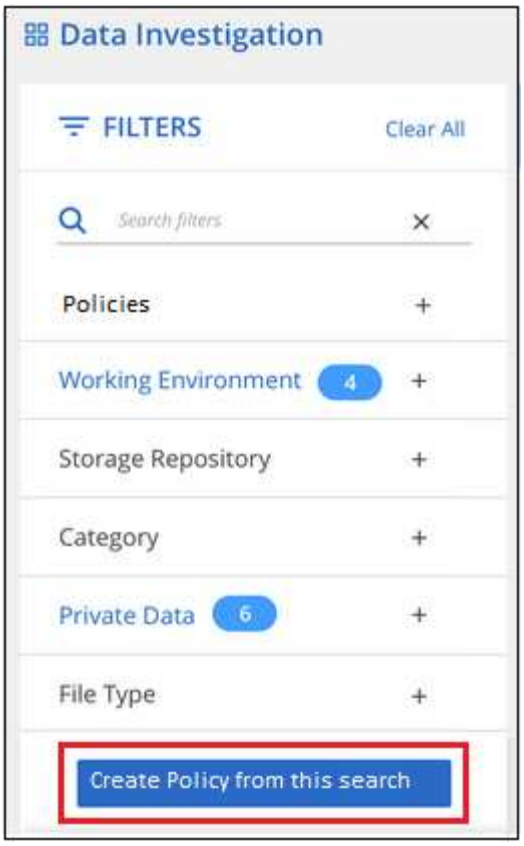
Erstellen benutzerdefinierter Richtlinien

Sie können eigene benutzerdefinierte Richtlinien erstellen, die Ergebnisse für spezifische Suchen in Ihrem Unternehmen liefern. Die Ergebnisse werden für alle Dateien und Verzeichnisse (Freigaben und Ordner) zurückgegeben, die den Suchkriterien entsprechen.

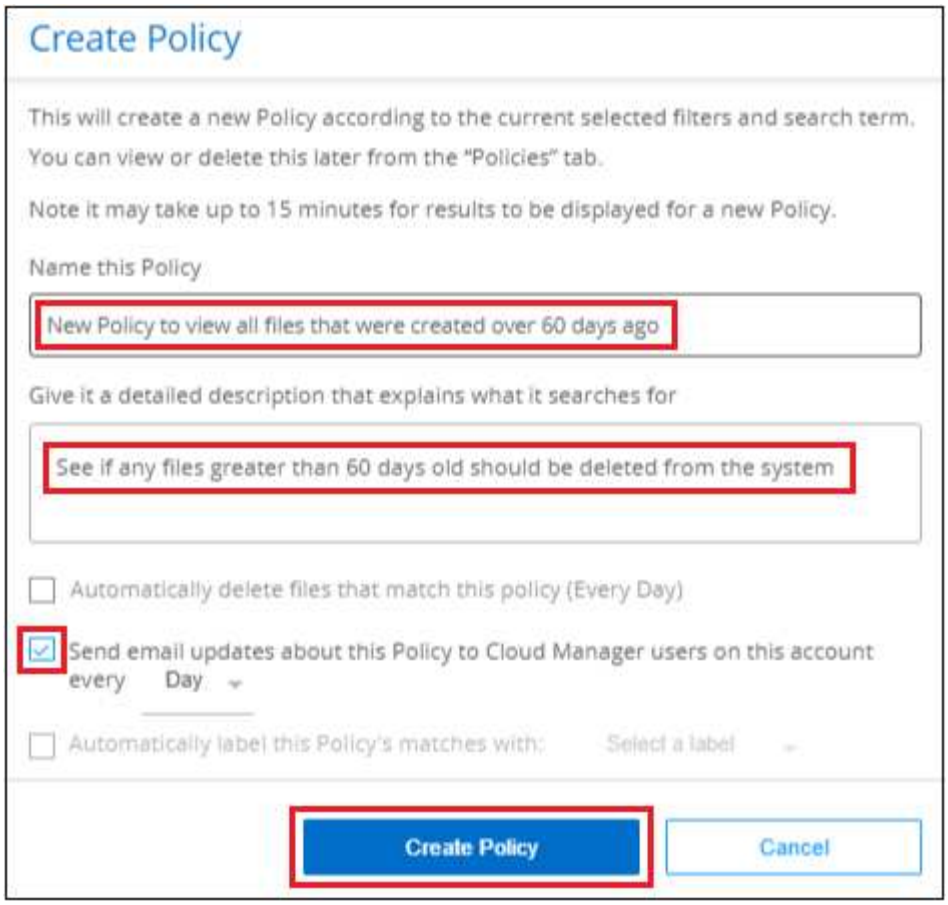
Beachten Sie, dass die Aktionen zum Löschen von Daten und zum Zuweisen von AIP-Etiketten auf der Grundlage der Richtlinienergebnisse nur für Dateien gültig sind. Verzeichnisse, die den Suchkriterien entsprechen, können nicht automatisch gelöscht oder AIP-Bezeichnungen zugewiesen werden.

Schritte

1. Definieren Sie auf der Seite „Untersuchung von Daten“ die Suche, indem Sie alle Filter auswählen, die Sie verwenden möchten. Siehe "Filtern von Daten auf der Seite „Datenuntersuchung“" Entsprechende Details.
2. Wenn Sie alle Filtereigenschaften genau so haben, wie Sie sie wollen, klicken Sie auf **Create Policy von dieser Suche**.



3. Benennen Sie die Richtlinie, und wählen Sie andere Aktionen aus, die von der Richtlinie ausgeführt werden können:
   a. Geben Sie einen eindeutigen Namen und eine eindeutige Beschreibung ein.
   b. Aktivieren Sie optional das Kontrollkästchen, um Dateien automatisch zu löschen, die mit den Richtlinieparametern übereinstimmen. Weitere Informationen zu "Quelldateien mit einer Richtlinie löschen".
   c. Aktivieren Sie optional das Kontrollkästchen, wenn Benachrichtigungen an BlueXP-Benutzer gesendet werden sollen, und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird. Weitere Informationen zu "Senden von E-Mail-Warnmeldungen anhand von Richtlinienergebnissen".
   d. Aktivieren Sie optional das Kontrollkästchen, um Dateien, die den Richtlinieparametern entsprechen, automatisch AIP-Etiketten zuzuweisen, und wählen Sie die Beschriftung aus. (Nur wenn Sie bereits AIP-Etiketten integriert haben. Weitere Informationen zu "AIP-Etiketten".)
   e. Klicken Sie Auf **Create Policy**.



Ergebnis

Die neue Richtlinie wird auf der Registerkarte Richtlinien angezeigt.

Senden von E-Mail-Warnungen, wenn nicht konforme Daten gefunden werden

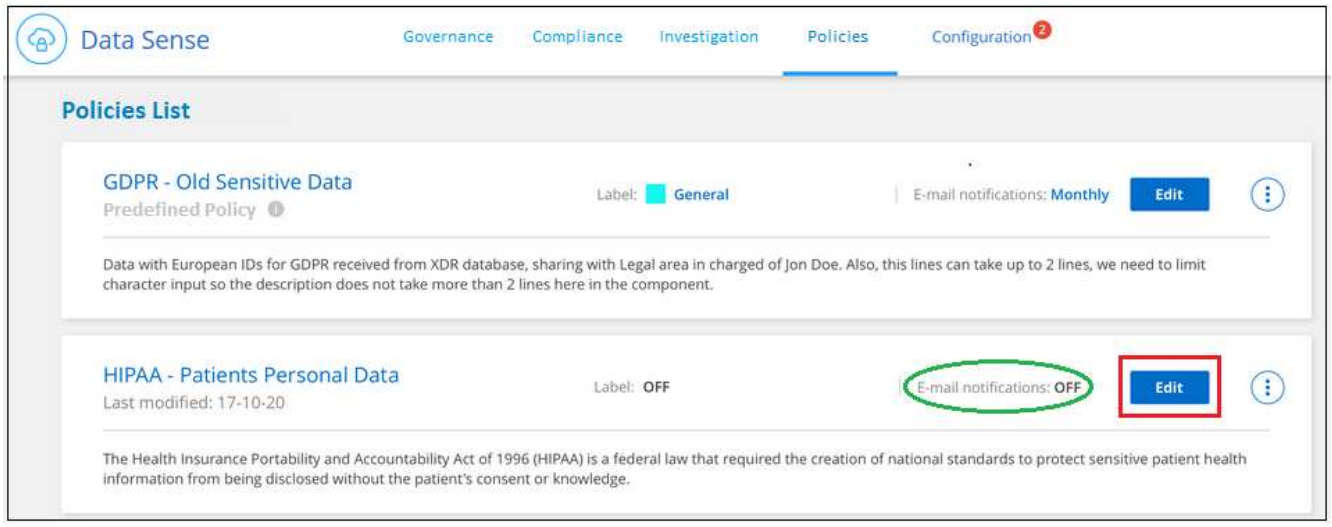
Cloud Data Sense kann E-Mail-Benachrichtigungen an BlueXP-Benutzer senden, wenn bestimmte kritische Richtlinien Ergebnisse liefern, damit Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten können. Sie können die E-Mail-Benachrichtigungen täglich, wöchentlich oder monatlich versenden.

Sie können diese Einstellung beim Erstellen der Richtlinie oder beim Bearbeiten einer Richtlinie konfigurieren.

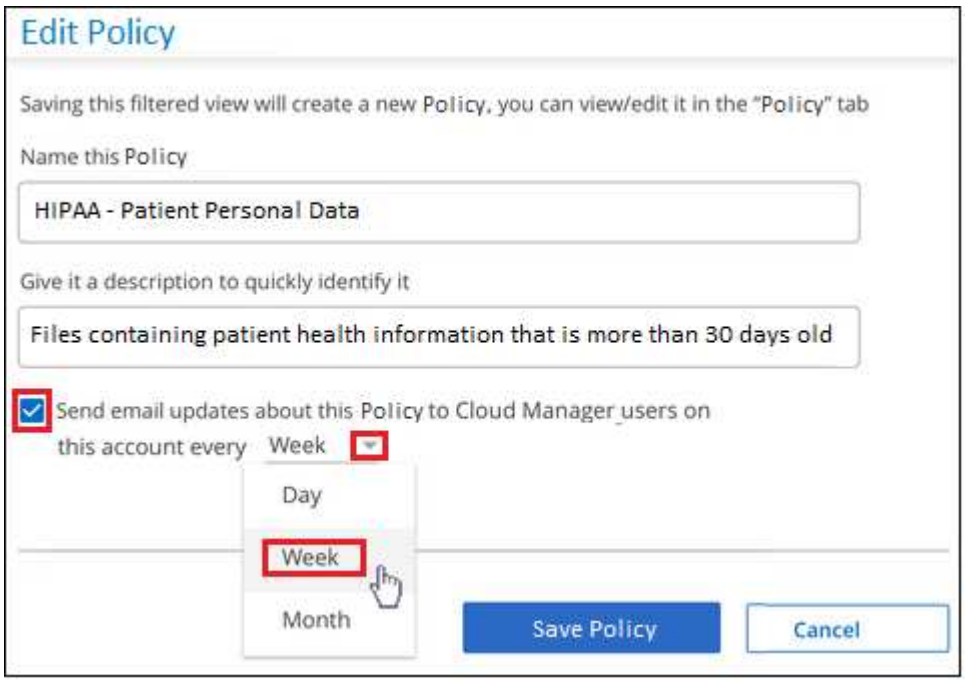
Befolgen Sie diese Schritte, um E-Mail-Updates zu einer bestehenden Richtlinie hinzuzufügen.

Schritte

1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, in der Sie die E-Mail-Einstellung hinzufügen (oder ändern) möchten.



2. Aktivieren Sie auf der Seite „Edit Policy“ das Kontrollkästchen, wenn Sie Benachrichtigungs-E-Mails an BlueXP-Benutzer senden möchten, und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird (z. B. jede **Woche**).



3. Klicken Sie auf **Save Policy** und das Intervall, in dem die E-Mail gesendet wird, wird in der Policy description angezeigt.

Ergebnis

Die erste E-Mail wird jetzt gesendet, wenn Ergebnisse aus der Richtlinie vorliegen - aber nur, wenn Dateien die Kriterien der Richtlinie erfüllen. Es werden keine personenbezogenen Daten in die Benachrichtigungs-E-Mails gesendet. Die E-Mail zeigt an, dass es Dateien gibt, die den Kriterien der Richtlinie entsprechen, und sie enthält einen Link zu den Ergebnissen der Richtlinie.

Richtlinien Werden Bearbeitet

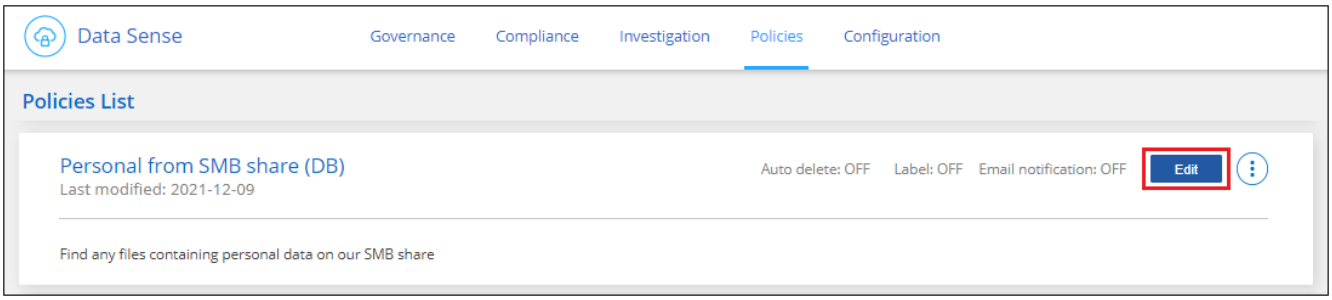
Sie können alle Kriterien für eine vorhandene Richtlinie ändern, die Sie zuvor erstellt haben. Dies kann besonders nützlich sein, wenn Sie die Abfrage (die Elemente, die Sie mit Filtern definiert haben) ändern

möchten, um bestimmte Parameter hinzuzufügen oder zu entfernen.

Beachten Sie, dass Sie für vordefinierte Richtlinien nur ändern können, ob E-Mail-Benachrichtigungen gesendet werden und ob AIP-Beschriftungen hinzugefügt werden. Andere Werte können nicht geändert werden.

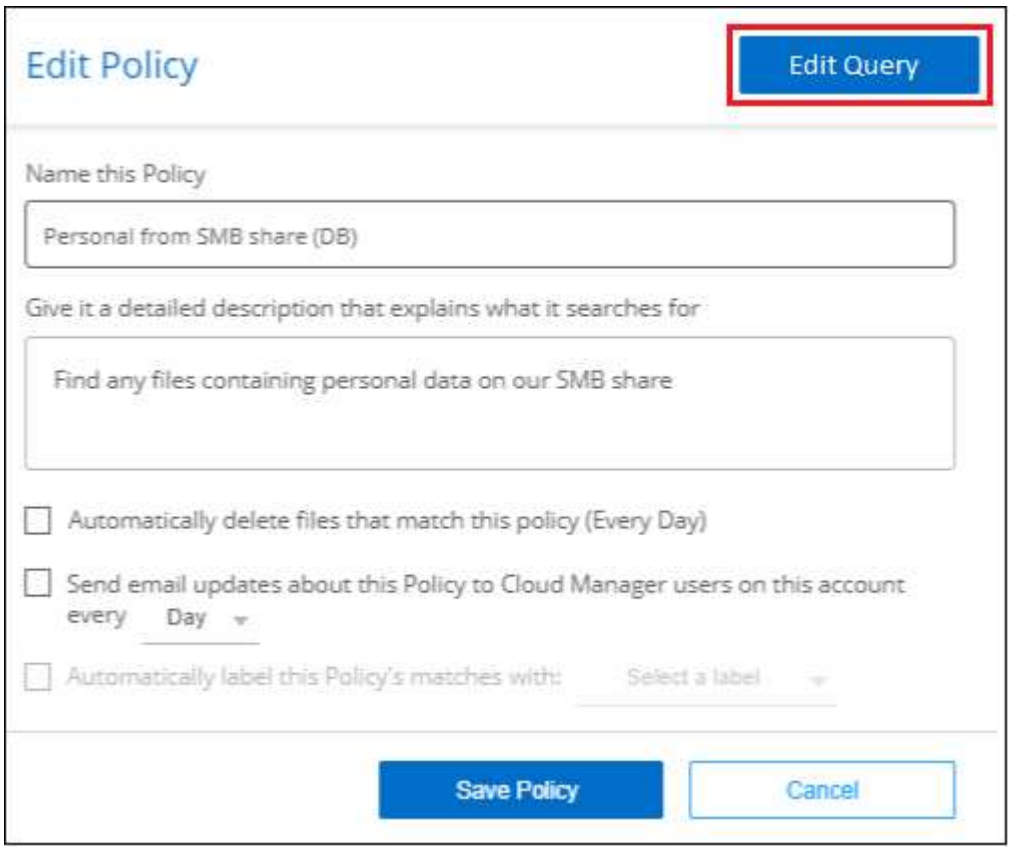
Schritte

1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, die Sie ändern möchten.

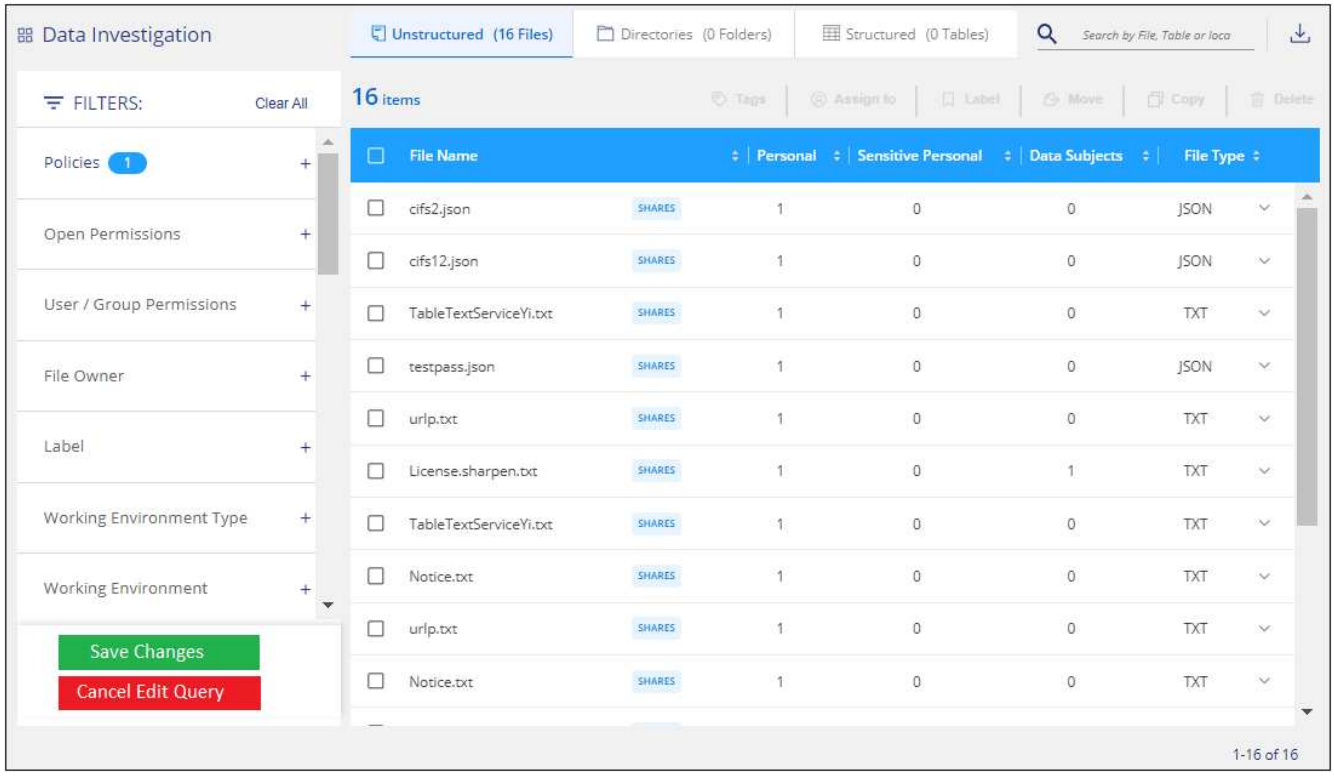


2. Wenn Sie nur die Elemente auf dieser Seite ändern möchten (Name, Beschreibung, ob E-Mail-Benachrichtigungen gesendet werden, und ob AIP-Beschriftungen hinzugefügt werden), ändern Sie die Änderung und klicken Sie auf **Richtlinie speichern**.

   Wenn Sie die Filter für die gespeicherte Abfrage ändern möchten, klicken Sie auf **Abfrage bearbeiten**.



3. Bearbeiten Sie auf der Untersuchungsseite, die diese Abfrage definiert, die Abfrage durch Hinzufügen, Entfernen oder Anpassen der Filter und klicken Sie auf **Änderungen speichern** .



Ergebnis

Die Richtlinie wird sofort geändert. Alle Aktionen, die für diese Richtlinie zum Senden einer E-Mail, Hinzufügen von AIP-Etiketten oder Löschen von Dateien definiert sind, werden im nächsten internen ausgeführt.

Richtlinien Werden Gelöscht

Sie können alle benutzerdefinierten Richtlinien löschen, die Sie erstellt haben, wenn Sie sie nicht mehr benötigen. Sie können keine der vordefinierten Richtlinien löschen.

Zum Löschen einer Richtlinie klicken Sie auf das Klicken Sie für eine bestimmte Richtlinie auf **Richtlinie löschen**, und klicken Sie dann im Bestätigungsdialogfeld erneut auf **Richtlinie löschen**.

Liste der vordefinierten Richtlinien

Cloud Data Sense bietet die folgenden systemdefinierten Richtlinien:

Name	Beschreibung	Logik
S3 öffentlich zugängliche private Daten	S3 Objekte mit persönlichen oder sensiblen persönlichen Daten, mit offenem öffentlichen Lesezugriff.	S3 Public ENTHÄLT persönliche ODER sensible persönliche Informationen
PCI DSS – veraltete Daten über 30 Tage	Dateien mit Kreditkarteninformationen, zuletzt geändert vor mehr als 30 Tagen.	Enthält Kreditkarte UND zuletzt geändert über 30 Tage
HIPAA – veraltete Daten über 30 Tage	Dateien mit Gesundheitsinformationen, zuletzt geändert vor mehr als 30 Tagen.	Enthält Gesundheitsdaten (wie in HIPAA-Berichten definiert) UND die letzte Änderung über 30 Tage

Name	Beschreibung	Logik
Private Daten – veraltet über 7 Jahre	Dateien mit persönlichen oder sensiblen persönlichen Daten, zuletzt geändert vor über 7 Jahren.	Dateien mit persönlichen oder sensiblen persönlichen Daten, zuletzt geändert vor über 7 Jahren
DSGVO – europäische Bürger	Dateien mit mehr als 5 Kennungen von EU-Bürgern oder DB-Tabellen, die Kennungen von EU-Bürgern enthalten.	Dateien, die mehr als 5 Kennungen von (einem) EU-Bürgern oder DB-Tabellen enthalten, die Zeilen mit mehr als 15 % der Spalten mit den EU-Kennungen eines Landes enthalten. (Eine der nationalen Kennungen der europäischen Länder. Beinhaltet keine Brasilien, Kalifornien, USA SSN, Israel, Südafrika)
CCPA – Einwohner Kaliforniens	Dateien, die über 10 California Driver's License Identifier oder DB-Tabellen mit dieser Kennung enthalten.	Dateien, die über 10 California Driver's License Identifier ODER DB-Tabellen enthalten, die California Driver's License enthalten
Namen der Betroffenen – hohes Risiko	Dateien mit mehr als 50 Namen des Betroffenen.	Dateien mit mehr als 50 Namen des Betroffenen
E-Mail-Adressen – hohes Risiko	Dateien mit über 50 E-Mail-Adressen oder DB-Spalten mit über 50 % ihrer Zeilen, die E-Mail-Adressen enthalten	Dateien mit über 50 E-Mail-Adressen oder DB-Spalten mit über 50 % ihrer Zeilen, die E-Mail-Adressen enthalten
Personenbezogene Daten – hohes Risiko	Dateien mit mehr als 20 Identifikatoren für persönliche Daten oder Datenbankspalten mit über 50 % ihrer Zeilen, die Identifikatoren für persönliche Daten enthalten.	Dateien mit über 20 persönlichen oder DB-Spalten mit über 50% ihrer Zeilen, die persönliche enthalten
Sensible personenbezogene Daten – hohes Risiko	Dateien mit über 20 vertraulichen personenbezogenen Daten-IDs oder DB-Spalten mit über 50 % ihrer Zeilen, die vertrauliche personenbezogene Daten enthalten.	Dateien mit über 20 sensiblen persönlichen oder DB-Spalten mit über 50% ihrer Zeilen, die sensible persönliche Daten enthalten

Management privater Daten

Cloud Data Sense bietet viele Möglichkeiten für das Management von privaten Daten. Einige Funktionen erleichtern die Vorbereitung auf die Migration Ihrer Daten, während andere Funktionen können Sie Änderungen an den Daten.

- Sie können Dateien in eine Ziel-NFS-Freigabe kopieren, wenn Sie eine Kopie bestimmter Daten erstellen und sie an einen anderen NFS-Speicherort verschieben möchten.
- Sie können ein ONTAP Volume auf einem neuen Volume klonen und dabei nur ausgewählte Dateien aus dem Quell-Volume im neuen geklonten Volume eingeschlossen. Dies ist nützlich für Situationen, in denen Sie Daten migrieren und Sie bestimmte Dateien vom ursprünglichen Volume ausschließen möchten.
- Sie können Dateien aus einem Quell-Repository in ein Verzeichnis an einem bestimmten Zielspeicherort kopieren und synchronisieren. Dies ist nützlich für Situationen, in denen Sie Daten von einem Quellsystem zu einem anderen migrieren, während es noch einige letzte Aktivität auf den Quelldateien gibt.
- Sie können Quelldateien verschieben, die Data Sense auf jede NFS-Freigabe scannt.

- Sie können Dateien löschen, die als unsicher oder zu riskant erscheinen, um in Ihrem Speichersystem zu verbleiben, oder die Sie als Duplikat identifiziert haben.

- Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.
- Daten von Google Drive-Konten können derzeit keine dieser Funktionen nutzen.

Quelldateien werden kopiert

Sie können alle Quelldateien kopieren, die von Data Sense gescannt werden. Es gibt drei Arten von Kopiervorgängen, je nachdem, was Sie erreichen möchten:

- **Kopieren Sie Dateien** aus den gleichen oder anderen Volumes oder Datenquellen in eine Ziel-NFS-Freigabe.

  Dies ist nützlich, wenn Sie eine Kopie bestimmter Daten erstellen und sie an einen anderen NFS-Speicherort verschieben möchten.

- **Ein ONTAP-Volume** zu einem neuen Volume im selben Aggregat klonen, aber nur ausgewählte Dateien aus dem Quell-Volume in das neue geklonte Volume einbeziehen.

  Dies ist nützlich für Situationen, in denen Sie Daten migrieren und bestimmte Dateien vom ursprünglichen Volume ausschließen möchten. Diese Aktion verwendet das "NetApp FlexClone" Funktionalität zum schnellen Duplizieren des Volumes und dann entfernen Sie die Dateien, die Sie **nicht** ausgewählt haben.

- **Kopieren und Synchronisieren von Dateien** aus einem Quell-Repository (ONTAP-Volume, S3-Bucket, NFS-Freigabe usw.) zu einem Verzeichnis in einem bestimmten Ziel-Speicherort (Ziel).

  Dies ist besonders nützlich, wenn Sie Daten von einem Quellsystem zu einem anderen migrieren. Nach der ersten Kopie synchronisiert der Service alle geänderten Daten auf der Grundlage des von Ihnen festgelegten Zeitplans. Diese Aktion verwendet das "NetApp Cloud Sync" Funktion zum Kopieren und Synchronisieren von Daten von einer Quelle an ein Ziel

Quelldateien werden in eine NFS-Freigabe kopiert

Sie können Quelldateien kopieren, die Data Sense auf jede NFS-Freigabe scannt. Die NFS-Freigabe muss nicht in Data Sense integriert werden, Sie müssen nur den Namen der NFS-Freigabe kennen, wo alle ausgewählten Dateien in das Format kopiert werden `<host_name>:/<share_path>`.

Sie können keine Dateien kopieren, die sich in Datenbanken befinden.

Anforderungen

- Sie müssen über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen, um Dateien zu kopieren.
- Das Kopieren von Dateien erfordert, dass die Ziel-NFS-Freigabe den Zugriff aus der Data Sense Instanz ermöglicht.
- Sie können maximal 100,000 Dateien gleichzeitig kopieren.

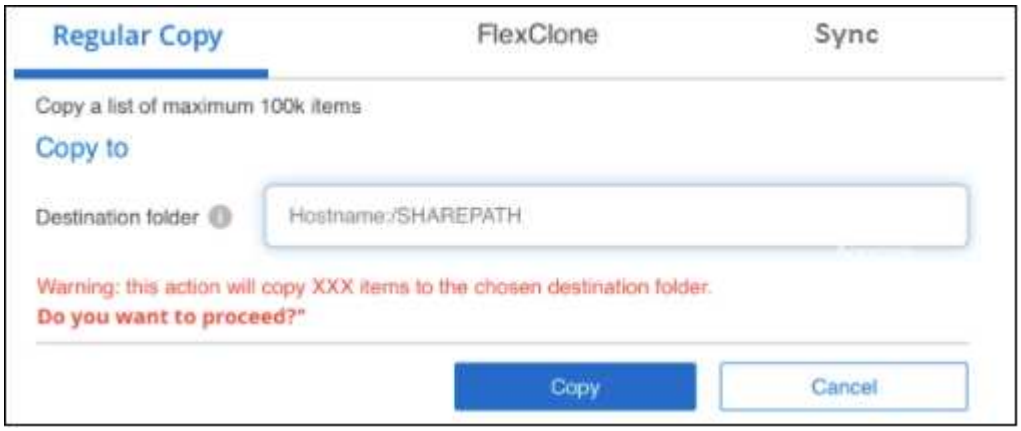
Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie

kopieren möchten, und klicken Sie auf **Kopieren**.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht
  All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

2. Wählen Sie im Dialogfeld „ Dateien kopieren “ die Registerkarte **normale Kopie** aus.



3. Geben Sie den Namen der NFS-Freigabe ein, auf die alle ausgewählten Dateien in das Format kopiert werden sollen `<host_name>:/<share_path>`, Und klicken Sie auf **Kopieren**.

   Ein Dialogfeld mit dem Status des Kopiervorgangs wird angezeigt.

Sie können den Fortschritt des Kopiervorgangs in anzeigen "Statusbereich Aktionen".

Beachten Sie, dass Sie bei der Anzeige der Metadatendetails für eine Datei auch eine einzelne Datei kopieren können. Klicken Sie einfach auf **Datei kopieren**.

Klonen von Volume-Daten auf einem neuen Volume

Sie können ein vorhandenes ONTAP Volume klonen, das Data Sense mithilfe der NetApp *FlexClone* Funktion scannt. So können Sie das Volume schnell duplizieren, während nur die von Ihnen ausgewählten Dateien enthalten sind. Dies ist nützlich, wenn Sie Daten migrieren und bestimmte Dateien vom ursprünglichen Volume ausschließen möchten oder wenn Sie eine Kopie eines Volumes zu Testzwecken erstellen möchten.

Das neue Volume wird im selben Aggregat erstellt wie das Quell-Volume. Stellen Sie vor Beginn dieser Aufgabe sicher, dass genügend Platz für dieses neue Volume im Aggregat vorhanden ist. Wenden Sie sich bei Bedarf an Ihren Storage-Administrator.

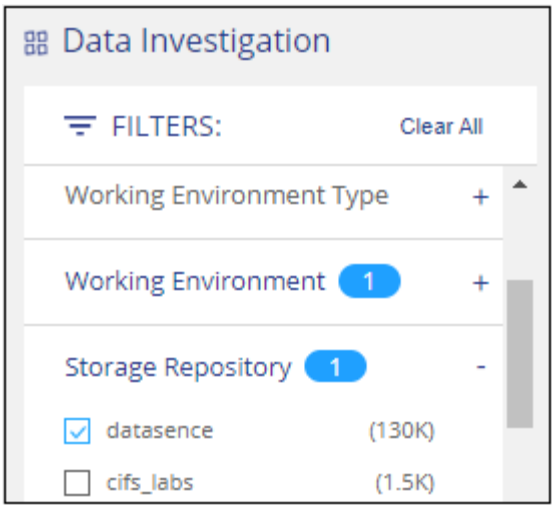
Hinweis: FlexGroup Volumes können nicht geklont werden, da sie nicht von FlexClone unterstützt werden.

Anforderungen

- Sie müssen über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen, um Dateien zu kopieren.
- Alle ausgewählten Dateien müssen sich vom selben Volume befinden, und das Volume muss online sein.
- Das Volume muss aus einem Cloud Volumes ONTAP oder einem lokalen ONTAP System stammen. Derzeit werden keine anderen Datenquellen unterstützt.
- Die FlexClone Lizenz muss auf dem Cluster installiert sein. Diese Lizenz wird standardmäßig auf Cloud Volumes ONTAP-Systemen installiert.

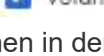
Schritte

1. Erstellen Sie im Bereich Datenuntersuchung einen Filter, indem Sie eine einzige **Arbeitsumgebung** und ein einziges **Speicher-Repository** auswählen, um sicherzustellen, dass alle Dateien vom selben ONTAP-Volume stammen.



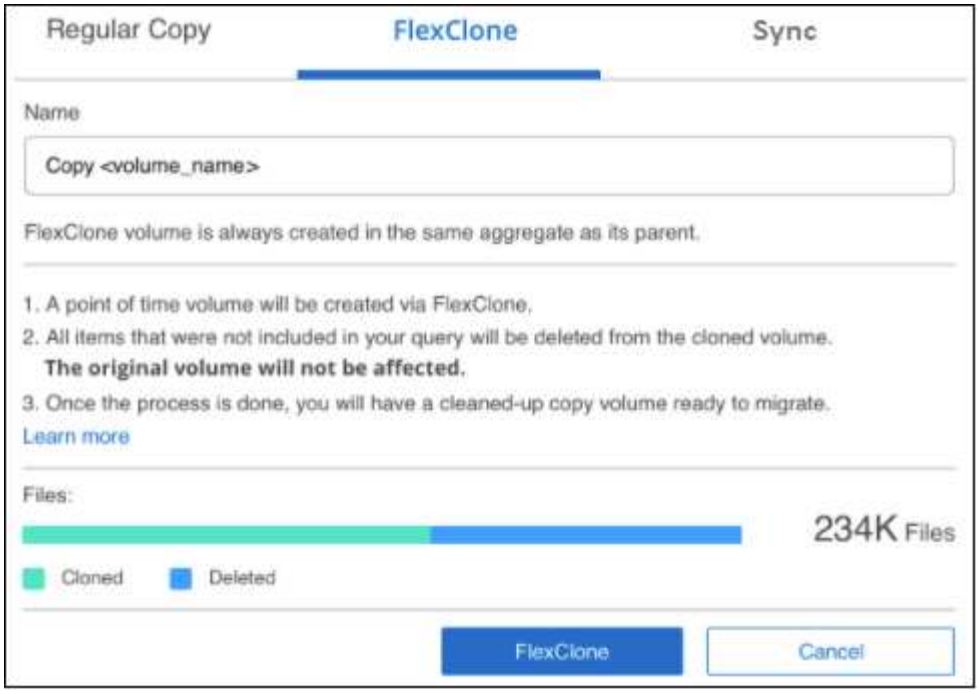
Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie auf dem neuen Volume klonen möchten.

2. Wählen Sie im Bereich Untersuchungsergebnisse die Dateien aus, die Sie klonen möchten, und klicken Sie auf **Kopieren**.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei ().
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile ().
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (), und dann in der Pop-up-Nachricht


Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

3. Wählen Sie im Dialogfeld *Dateien kopieren* die Registerkarte **FlexClone** aus. Diese Seite zeigt die Gesamtzahl der Dateien, die aus dem Volume geklont werden (die von Ihnen ausgewählten Dateien) und die Anzahl der Dateien, die nicht enthalten bzw. gelöscht sind (die Dateien, die Sie nicht ausgewählt haben), aus dem geklonten Volume.



4. Geben Sie den Namen des neuen Volume ein und klicken Sie auf **FlexClone**.

   Ein Dialogfeld mit dem Status des Klonvorgangs wird angezeigt.

Ergebnis

Das neue geklonte Volume wird in demselben Aggregat erstellt wie das Quell-Volume.

Sie können den Status des Klonvorgangs in anzeigen "Statusbereich Aktionen".

Wenn Sie ursprünglich **Alle Volumes** oder **Karte & Klassifizieren alle Volumen** ausgewählt haben, wenn Sie Data Sense für die Arbeitsumgebung aktiviert haben, in der sich das Quellvolume befindet, wird Data Sense das neue geklonte Volume automatisch scannen. Wenn Sie eine dieser Optionen zunächst nicht verwendet haben, müssen Sie dieses neue Volume scannen "Aktivieren Sie manuell das Scannen auf dem Volumen".

Kopieren und Synchronisieren von Quelldateien auf ein Zielsystem

Sie können Quelldateien kopieren, die Data Sense von jeder unterstützten unstrukturierten Datenquelle in ein Verzeichnis an einem bestimmten Zielspeicherort scannt ("Zielorte, die von Cloud Sync unterstützt werden"). Nach der ersten Kopie werden alle geänderten Daten in den Dateien gemäß dem von Ihnen konfigurierten Zeitplan synchronisiert.

Dies ist besonders nützlich, wenn Sie Daten von einem Quellsystem zu einem anderen migrieren. Diese Aktion verwendet das "NetApp Cloud Sync" Funktion zum Kopieren und Synchronisieren von Daten von einer Quelle an ein Ziel

Dateien, die sich in Datenbanken, OneDrive-Konten oder SharePoint Konten befinden, können nicht kopiert und synchronisiert werden.

Anforderungen

- Zum Kopieren und Synchronisieren von Dateien müssen Sie über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen.
- Alle ausgewählten Dateien müssen aus demselben Quell-Repository stammen (ONTAP Volume, S3

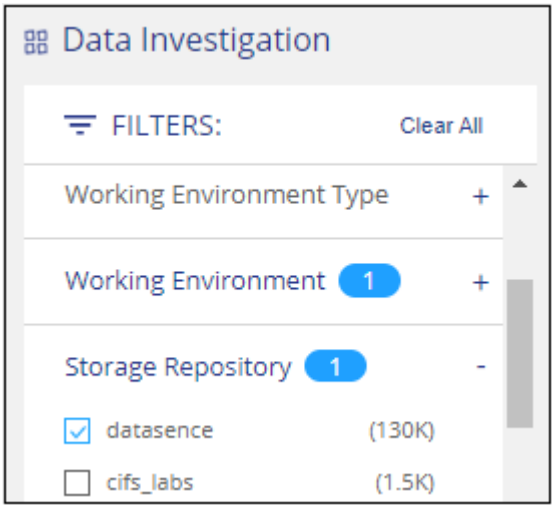
Bucket, NFS oder CIFS-Freigabe usw.).

- Sie müssen den Cloud Sync Service aktivieren und mindestens einen Daten-Broker konfigurieren, der zur Übertragung von Dateien zwischen Quell- und Zielsystemen genutzt werden kann. Prüfen Sie die Cloud Sync-Anforderungen, die mit dem beginnen "Kurzanleitung".

  Beachten Cloud Sync Sie, dass für Ihre Synchronisierungsbeziehungen separate Servicegebühren anfallen und bei der Bereitstellung des Daten-Brokers in der Cloud Gebühren anfallen.

Schritte

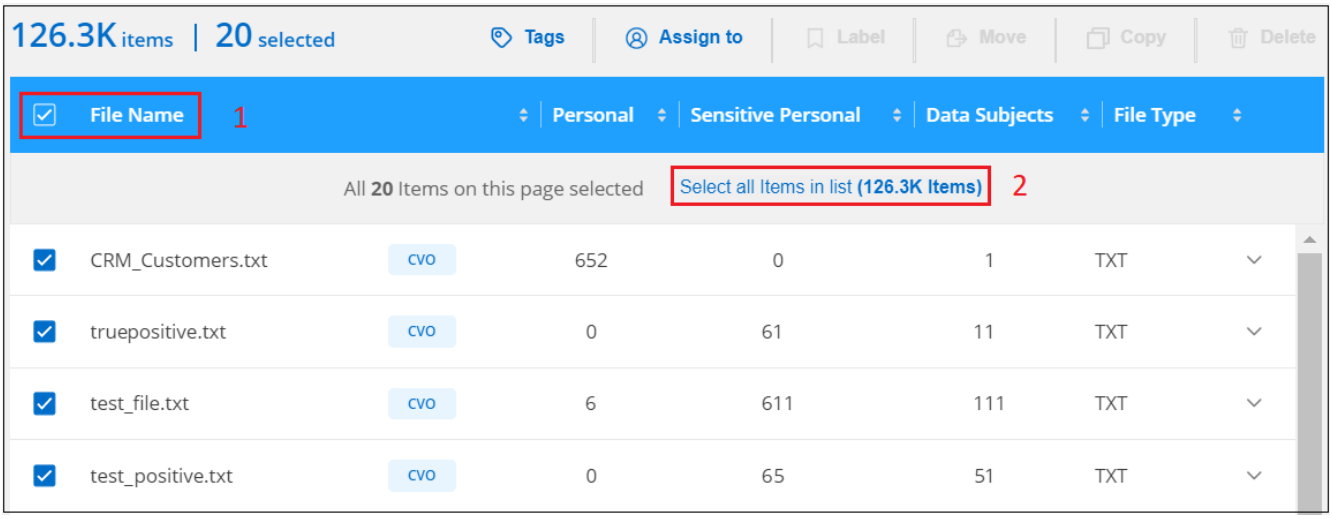
1. Erstellen Sie im Bereich Datenuntersuchung einen Filter, indem Sie eine einzige * Arbeitsumgebung* und ein einziges **Speicher-Repository** auswählen, um sicherzustellen, dass alle Dateien aus demselben Repository stammen.



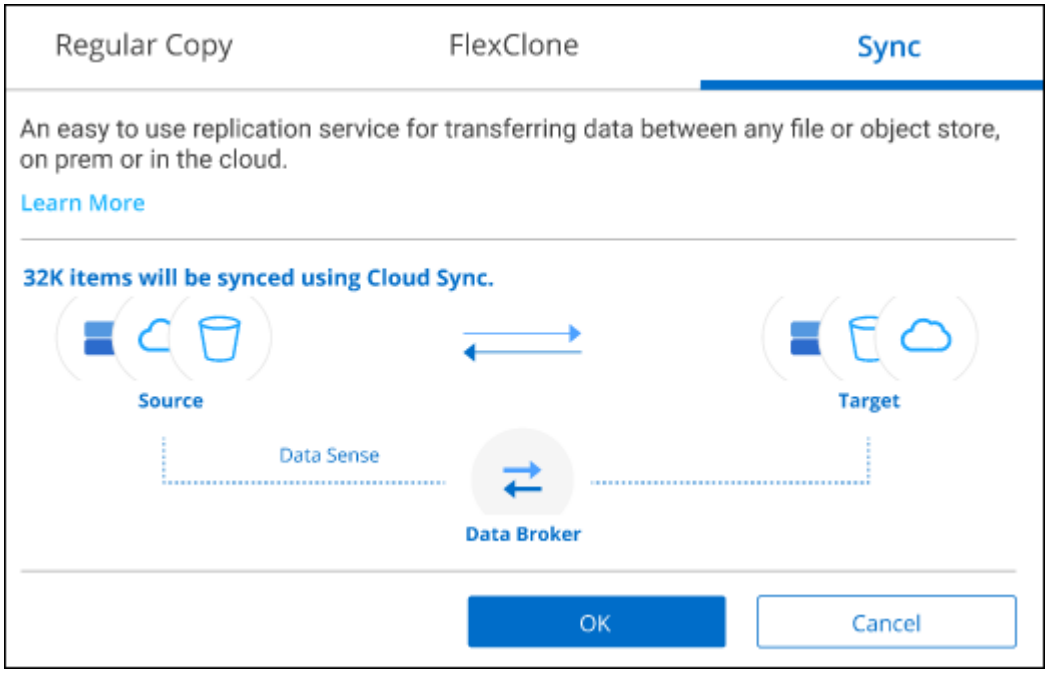
   Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie kopieren und mit dem Zielsystem synchronisieren möchten.

2. Wählen Sie im Bereich Untersuchungsergebnisse alle Dateien auf allen Seiten aus, indem Sie das Kästchen in der Titelzeile (aktivieren 

), dann in der Pop-up-Nachricht All 20 Items on this page selected Select all Items in list (63K Items) Klicken Sie auf **Wählen Sie alle Elemente aus der Liste aus (xxx Elemente)**, und klicken Sie dann auf **Kopieren**.



3. Wählen Sie im Dialogfeld „ Dateien kopieren “ die Registerkarte **Sync** aus.



4. Wenn Sie sicher sind, dass Sie die ausgewählten Dateien mit einem Zielort synchronisieren möchten, klicken Sie auf **OK**.

   Die Cloud Sync-Benutzeroberfläche wird in BlueXP geöffnet.

   Sie werden aufgefordert, die Synchronisierungsbeziehung zu definieren. Das Quellsystem ist auf der Grundlage des Repositorys und der Dateien, die Sie bereits in Data Sense ausgewählt haben, vorbelegt.

5. Sie müssen das Zielsystem auswählen und dann den zu verwendenden Daten-Broker (oder erstellen) auswählen. Prüfen Sie die Cloud Sync-Anforderungen, die mit dem beginnen "Kurzanleitung".

Ergebnis

Die Dateien werden in das Zielsystem kopiert und auf der Grundlage des von Ihnen definierten Zeitplans synchronisiert. Wenn Sie eine einmalige Synchronisierung auswählen, werden die Dateien nur einmal kopiert und synchronisiert. Wenn Sie eine regelmäßige Synchronisierung auswählen, werden die Dateien auf Grundlage des Zeitplans synchronisiert. Beachten Sie, dass wenn das Quellsystem neue Dateien hinzufügt, die mit der Abfrage übereinstimmen, die Sie mit Filtern erstellt haben, diese *neuen*-Dateien in das Ziel kopiert und in Zukunft synchronisiert werden.

Beachten Sie, dass einige der üblichen Cloud Sync-Vorgänge beim Aufruf von Data Sense deaktiviert sind:

- Sie können die Schaltflächen **Dateien auf Quelle löschen** oder **Dateien auf Ziel** löschen nicht verwenden.
- Ausführen eines Berichts ist deaktiviert.

Quelldateien werden in eine NFS-Freigabe verschoben

Sie können Quelldateien verschieben, die Data Sense auf jede NFS-Freigabe scannt. Die NFS-Freigabe muss nicht mit Data Sense integriert werden (siehe "Scannen von Dateifreigaben").

Optional können Sie eine Breadcrumb-Datei am Speicherort der verschobenen Datei belassen. Eine Breadcrumb-Datei hilft Ihren Benutzern zu verstehen, warum eine Datei vom ursprünglichen Speicherort

verschoben wurde. Für jede verschobene Datei erstellt das System eine Breadcrumb-Datei im Quellspeicherort mit dem Namen `<filename>-breadcrumb-<date>.txt`. Sie können Text in das Dialogfeld einfügen, das der Breadcrumb-Datei hinzugefügt wird, um den Speicherort anzugeben, an dem die Datei verschoben wurde, und den Benutzer, der die Datei verschoben hat.

Wenn eine Datei mit dem gleichen Namen am Zielspeicherort vorhanden ist, wird die Datei nicht verschoben.

Sie können keine Dateien verschieben, die sich in Datenbanken befinden.

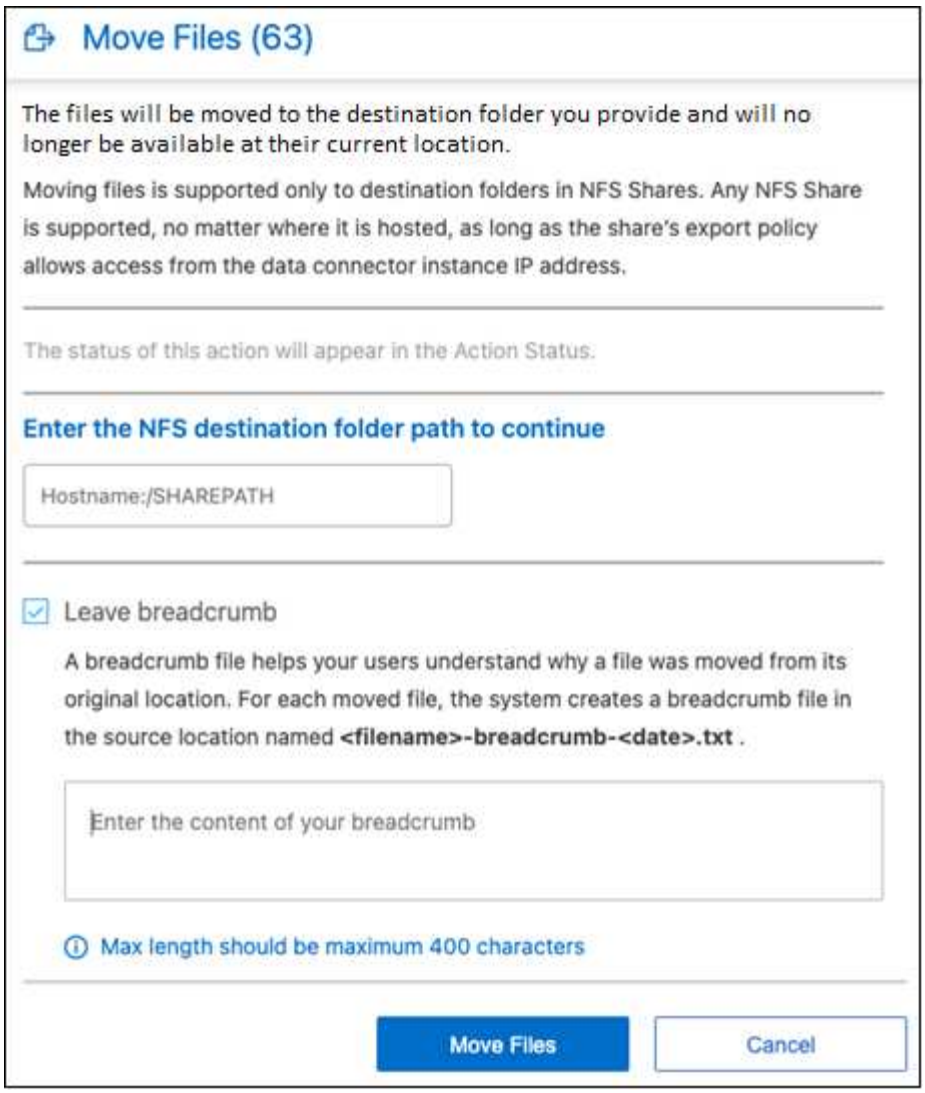
Anforderungen

- Sie müssen über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen, um Dateien zu verschieben.
- Die Quelldateien lassen sich in den folgenden Datenquellen befinden: On-Premises ONTAP, Cloud Volumes ONTAP, Azure NetApp Files, File Shares und SharePoint Online.
- Beim Verschieben von Dateien muss die NFS-Freigabe den Zugriff über die IP-Adresse der Datensense-Instanz ermöglichen.
- Sie können maximal 100,000 Dateien gleichzeitig verschieben.

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie verschieben möchten.

   - Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
   - Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
   - Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.
2. Klicken Sie in der Tastenleiste auf **Move**.



3. Geben Sie im Dialogfeld „ Dateien verschieben “ den Namen der NFS-Freigabe ein, bei der alle ausgewählten Dateien im Format verschoben werden `<host_name>:/<share_path>`.
4. Wenn Sie eine Breadcrumb-Datei verlassen möchten, aktivieren Sie das Kontrollkästchen *Breadcrumb* verlassen. Sie können Text in das Dialogfeld eingeben, um den Speicherort anzugeben, an dem die Datei verschoben wurde, sowie den Benutzer, der die Datei verschoben hat, und weitere Informationen, z. B. den Grund, aus dem die Datei verschoben wurde.
5. Klicken Sie Auf **Dateien Verschieben**.

Beachten Sie, dass Sie auch eine einzelne Datei verschieben können, wenn Sie sich die Metadatendetails für eine Datei ansehen. Klicken Sie einfach auf **Datei verschieben**.

Quelldateien werden gelöscht

Sie können Quelldateien dauerhaft entfernen, die unsicher oder zu riskant erscheinen, um in Ihrem Speichersystem zu verbleiben, oder dass Sie als Duplikat identifiziert haben. Diese Aktion ist permanent und es gibt kein Rückgängigmachen oder Wiederherstellen.

Sie können Dateien manuell aus dem Untersuchungsbereich oder automatisch mit Richtlinien löschen.

Sie können keine Dateien löschen, die sich in Datenbanken befinden.

Das Löschen von Dateien erfordert die folgenden Berechtigungen:

- Für NFS-Daten: Die Exportrichtlinie muss mit Schreibberechtigungen definiert werden.
- Für CIFS-Daten - die CIFS-Anmeldeinformationen benötigen Schreibberechtigungen.
- Für S3-Daten muss die IAM-Rolle die folgende Berechtigung enthalten: `s3:DeleteObject`.

Quelldateien werden manuell gelöscht

Anforderungen

- Zum Löschen von Dateien müssen Sie über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen.
- Sie können maximal 100,000 Dateien gleichzeitig löschen.

Schritte

1. Wählen Sie im Bereich Ergebnisse der Datenuntersuchung die Datei oder die Dateien aus, die Sie löschen möchten.

- Um einzelne Dateien auszuwählen, aktivieren Sie das Kontrollkästchen für jede Datei (Volume_1).
- Um alle Dateien auf der aktuellen Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name).
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (File Name), und dann in der Pop-up-Nachricht
  All **20** Items on this page selected Select all Items in list (63K Items)Klicken Sie auf **Wählen Sie alle Einträge aus der Liste (xxx Elemente)**.

2. Klicken Sie in der Tastenleiste auf **Löschen**.
3. Da der Löschvorgang dauerhaft ist, müssen Sie "**permanent delete**" in das folgende Dialogfeld *Datei löschen* eingeben und auf **Datei löschen** klicken.

Sie können den Fortschritt des Löschvorgangs in der anzeigen "Statusbereich Aktionen".

Beachten Sie, dass Sie auch eine einzelne Datei löschen können, wenn Sie sich die Metadatendetails für eine Datei ansehen. Klicken Sie einfach auf **Datei löschen**.

Quelldateien werden automatisch mithilfe von Richtlinien gelöscht

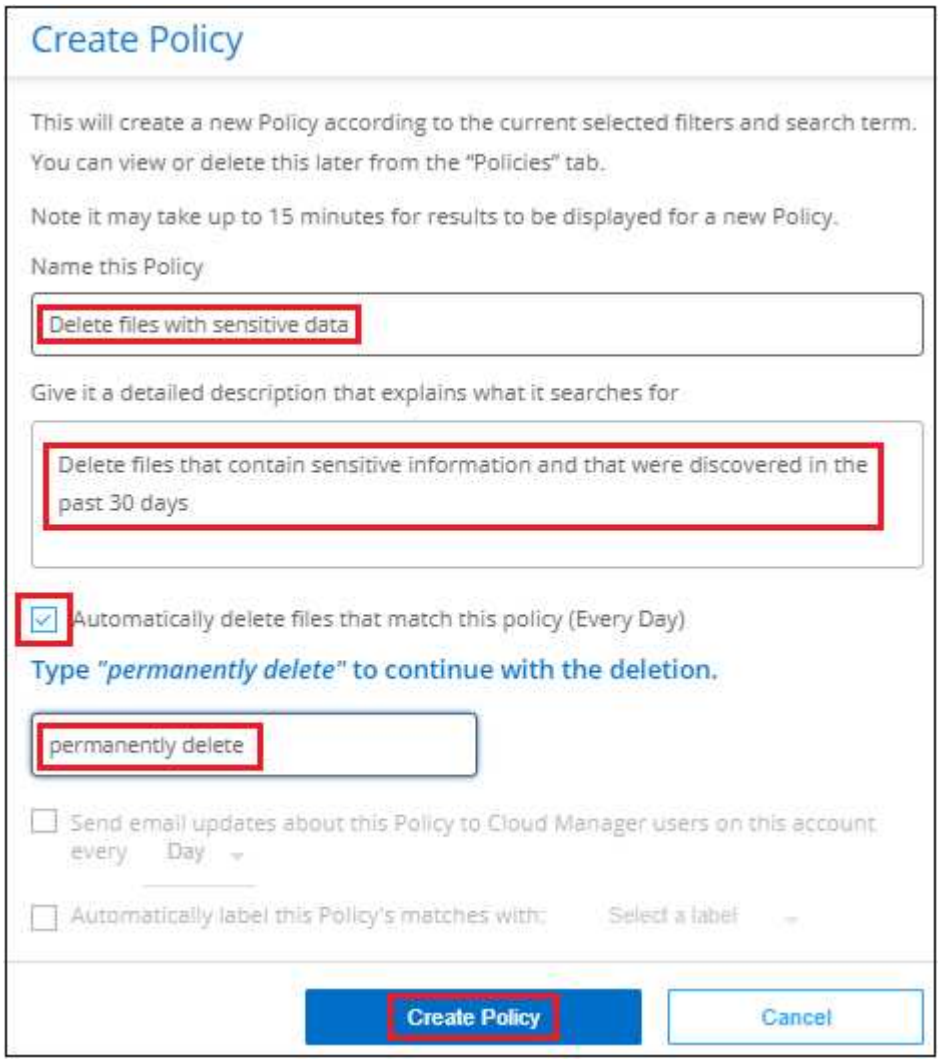
Sie können eine benutzerdefinierte Richtlinie erstellen, um Dateien zu löschen, die der Richtlinie entsprechen. Sie können beispielsweise Dateien löschen, die vertrauliche Informationen enthalten und von Data Sense in den letzten 30 Tagen entdeckt wurden.

Nur Kontoadministratoren können eine Richtlinie zum automatischen Löschen von Dateien erstellen.

Alle Dateien, die der Richtlinie entsprechen, werden einmal am Tag dauerhaft gelöscht.

Schritte

1. Definieren Sie auf der Seite „Untersuchung von Daten“ die Suche, indem Sie alle Filter auswählen, die Sie verwenden möchten. Siehe "Filtern von Daten auf der Seite „Datenuntersuchung“" Entsprechende Details.
2. Wenn Sie alle Filtereigenschaften genau so haben, wie Sie sie wollen, klicken Sie auf **Create Policy von dieser Suche**.
3. Benennen Sie die Richtlinie, und wählen Sie andere Aktionen aus, die von der Richtlinie ausgeführt werden können:
   a. Geben Sie einen eindeutigen Namen und eine eindeutige Beschreibung ein.
   b. Aktivieren Sie das Kontrollkästchen "Dateien, die dieser Richtlinie entsprechen automatisch löschen" und geben Sie **dauerhaft löschen** ein, um zu bestätigen, dass Dateien dauerhaft von dieser Richtlinie gelöscht werden sollen.
   c. Klicken Sie Auf **Create Policy**.



Ergebnis

Die neue Richtlinie wird auf der Registerkarte Richtlinien angezeigt. Dateien, die der Richtlinie entsprechen, werden einmal pro Tag gelöscht, wenn die Richtlinie ausgeführt wird.

Sie können die Liste der Dateien anzeigen, die im gelöscht wurden "Statusbereich Aktionen".

Anzeigen von Compliance-Berichten

Cloud Data Sense bietet Berichte, anhand deren Sie den Status des Datenschutzprogramms Ihres Unternehmens besser verstehen können.

Standardmäßig zeigen die Cloud Data Sense Dashboards Compliance- und Governance-Daten für alle Arbeitsumgebungen, Datenbanken und Datenquellen an. Wenn Sie Berichte anzeigen möchten, die Daten nur für einige Arbeitsumgebungen enthalten, Wählen Sie diese Arbeitsumgebungen aus.

- Die in diesem Abschnitt beschriebenen Berichte sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan durchgeführt wurde, können nur den Daten-Mapping-Bericht generieren.
- NetApp kann keine Garantie für 100 % der Genauigkeit persönlicher Daten und sensibler personenbezogener Daten, die Cloud Data Sense identifiziert. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Datenschutzrisiko-Assessment-Bericht

Der Datenschutzrisiko-Assessment-Bericht bietet einen Überblick über den Datenschutzrisikostatus Ihres Unternehmens, wie dies durch Datenschutzvorschriften wie DSGVO und CCPA erforderlich ist. Der Bericht enthält die folgenden Informationen:

Compliance-Status

A Schweregrad Und die Verteilung von Daten, ganz gleich, ob es sich um unempfindliche, personenbezogene oder sensible Daten handelt.

Assessment-Übersicht

Eine Aufschlüsselung der gefundenen Arten von personenbezogenen Daten sowie der Kategorien von Daten.

Betroffene in dieser Beurteilung

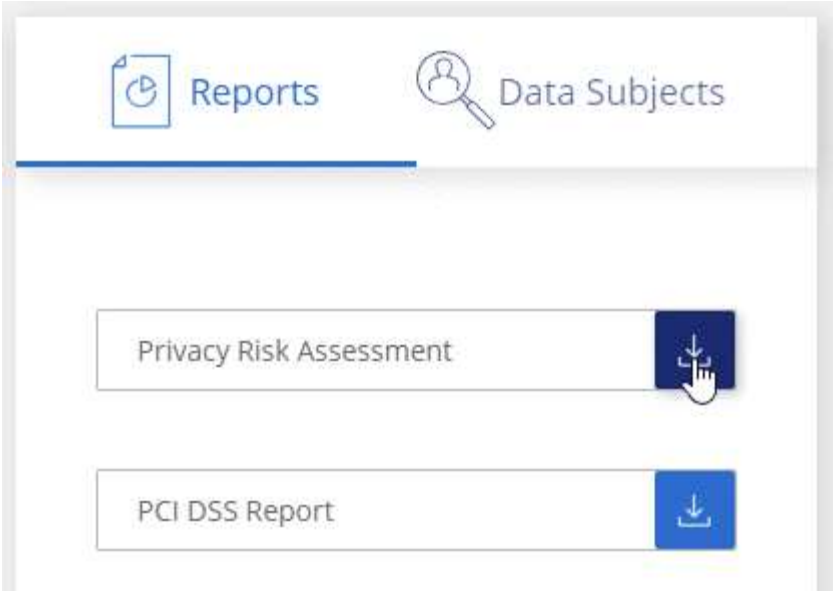
Die Anzahl der Personen, nach Ort, für die nationale Kennungen gefunden wurden.

Generieren des Datenschutzrisikobewertungsberichts

Rufen Sie die Registerkarte „Data Sense“ auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Compliance** und dann auf das Download-Symbol neben **Privacy Risk Assessment** unter **Reports**.



Ergebnis

Cloud Data Sense erstellt einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Schweregrad

Cloud Data Sense berechnet den Schweregrad für den Privacy Risk Assessment-Bericht auf der Grundlage von drei Variablen:

- Der Prozentsatz der personenbezogenen Daten aus allen Daten.
- Der Prozentsatz sensibler personenbezogener Daten aus allen Daten.
- Der Prozentsatz der Dateien, die betroffene Daten enthalten, die durch nationale Kennungen wie nationale IDs, Sozialversicherungsnummern und Steuerkennzahlen bestimmt werden.

Die folgende Logik dient zur Ermittlung der Punktzahl:

Schweregrad	Logik
0	Alle drei Variablen sind genau 0%
1	Eine der Variablen ist größer als 0 %
2	Eine der Variablen ist größer als 3%
3	Zwei der Variablen sind größer als 3%
4	Drei der Variablen sind größer als 3 %
5	Eine der Variablen ist größer als 6%
6	Zwei der Variablen sind größer als 6%
7	Drei der Variablen sind größer als 6 %
8	Eine der Variablen ist größer als 15%
9	Zwei der Variablen sind größer als 15%
10	Drei der Variablen sind größer als 15 %

PCI DSS-Bericht

Der PCI DSS-Bericht (Payment Card Industry Data Security Standard) hilft Ihnen bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien hinweg. Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Kreditkarteninformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Kreditkartendaten in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Kreditkarteninformationen, die in Arbeitsumgebungen gespeichert sind, für die der Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Ihre Kreditkartendaten nicht länger aufbewahren sollten, als Sie sie bearbeiten müssen.

Verteilung der Kreditkarteninformationen

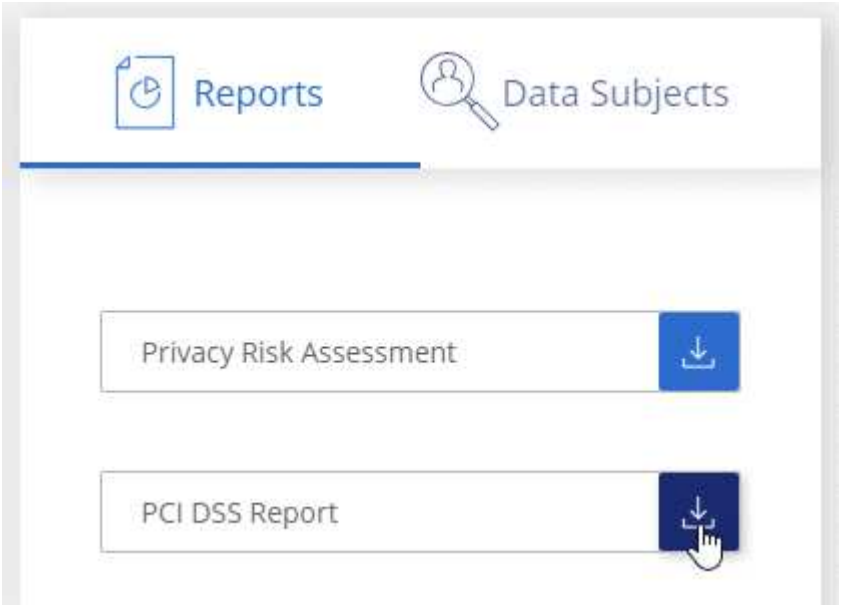
Die Arbeitsumgebungen, in denen Kreditkartendaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

PCI DSS-Bericht wird erstellt

Rufen Sie die Registerkarte „Data Sense“ auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Compliance** und dann auf das Download-Symbol neben **PCI DSS Report** unter **Reports**.



Ergebnis

Cloud Data Sense erstellt einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

HIPAA-Bericht

Der HIPAA-Bericht (Health Insurance Portability and Accountability Act) hilft Ihnen bei der Identifizierung von Dateien, die Gesundheitsdaten enthalten. Es wurde entwickelt, um die Anforderung Ihres Unternehmens zu unterstützen, die HIPAA-Datenschutzgesetze einzuhalten. Die Information Cloud Data Sense Looks umfasst:

- Zustandsreferenzmuster
- ICD-10 CM medizinischer Code
- ICD-9 CM medizinischer Code
- HR – Kategorie Gesundheit
- Datenkategorie für Gesundheitsanwendungen

Der Bericht enthält die folgenden Informationen:

Überblick
: Wie viele Dateien enthalten Gesundheitsinformationen und in welchen Arbeitsumgebungen.

Verschlüsselung
: Der Prozentsatz der Dateien, die Gesundheitsinformationen in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware
: Der Prozentsatz von Dateien mit Gesundheitsinformationen in Arbeitsumgebungen, in denen Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung
: Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Gesundheitsinformationen nicht länger aufbewahren sollten, als Sie sie verarbeiten müssen.

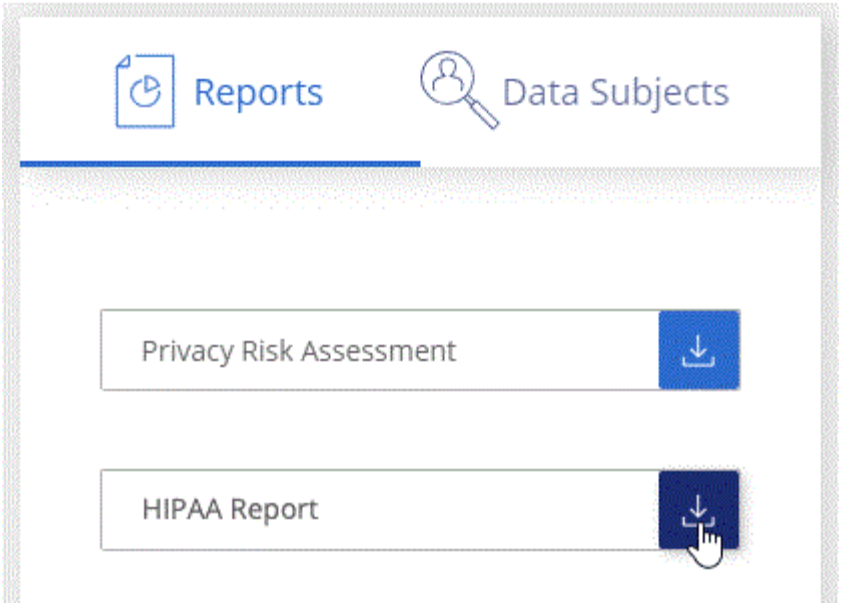
Verteilung von Gesundheitsinformationen
: In den Arbeitsumgebungen, in denen die Gesundheitsdaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

HIPAA-Bericht wird erstellt

Rufen Sie die Registerkarte „Data Sense“ auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Compliance** und dann auf das Download-Symbol neben **HIPAA Report** unter **Reports**.



Ergebnis

Cloud Data Sense erstellt einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Datenzuordnungsbericht

Der Daten-Mapping-Bericht bietet einen Überblick über die Daten, die in Ihren Datenquellen gespeichert werden, um Sie bei Entscheidungen zu Migrations-, Backup-, Sicherheits- und Compliance-Prozessen zu unterstützen. Der Bericht enthält zunächst einen Übersichtsbericht, der alle Arbeitsumgebungen und Datenquellen zusammenfasst und dann eine Aufschlüsselung der einzelnen Arbeitsumgebungen enthält.

Der Bericht enthält die folgenden Informationen:

Nutzung Von Kapazitäten

Für alle Arbeitsumgebungen: Listet die Anzahl der Dateien und die genutzte Kapazität für jede Arbeitsumgebung. Für einzelne Arbeitsumgebungen: Listet die Dateien auf, die die größte Kapazität nutzen.

Alter der Daten

Bietet drei Diagramme und Diagramme für den Zeitpunkt, an dem Dateien erstellt, zuletzt geändert oder zuletzt aufgerufen wurden. Listet die Anzahl der Dateien und deren verwendete Kapazität auf der Grundlage bestimmter Datumsbereiche auf.

Größe von Daten

Führt die Anzahl der Dateien auf, die in bestimmten Größenbereichen in Ihren Arbeitsumgebungen vorhanden sind.

Dateitypen

Listet die Gesamtzahl der Dateien und die genutzte Kapazität für jeden Dateityp auf, der in Ihren Arbeitsumgebungen gespeichert ist.

Datenzuordnungsbericht wird erstellt

Rufen Sie die Registerkarte „Data Sense“ auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Governance**, und klicken Sie dann im Governance Dashboard auf die Schaltfläche **Bericht zur Übersicht über die vollständige Datenzuordnung**.

Ergebnis

Cloud Data Sense erstellt einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Bericht Zur Datenuntersuchung

Der Datenuntersuchungs-Bericht ist ein Download der Inhalte der Seite Datenuntersuchung. "Erfahren Sie mehr über die Seite zur Untersuchung von Daten".

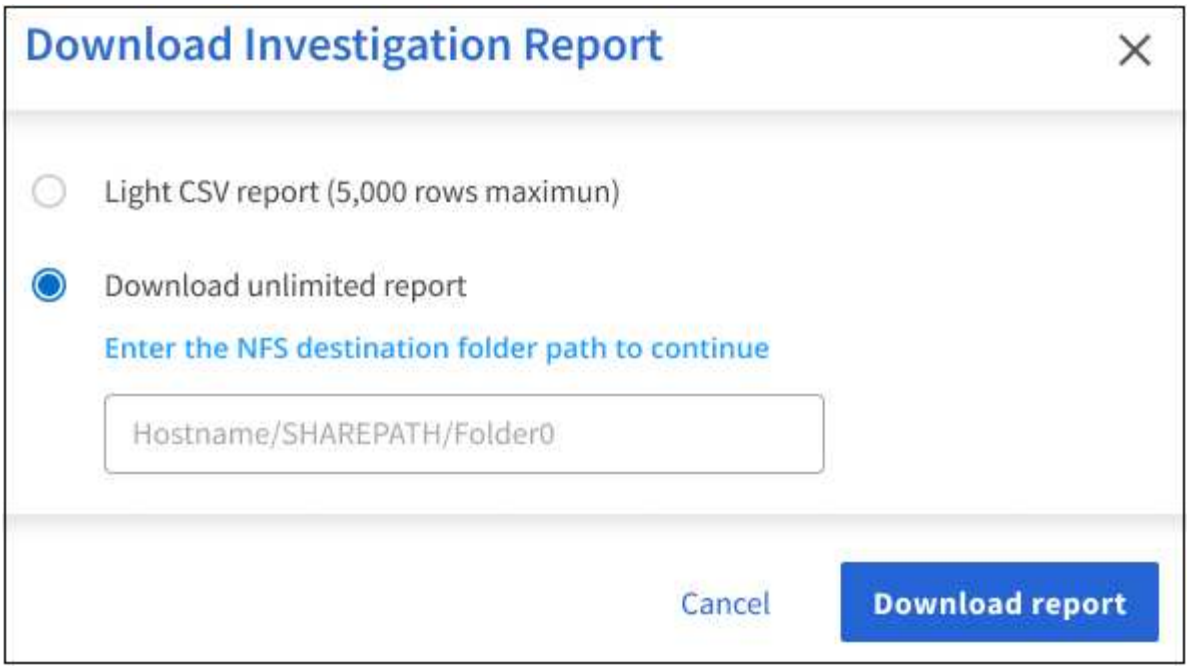
Sie können den Bericht als CSV-Datei (die bis zu 5,000 Datenzeilen enthalten kann) auf dem lokalen Rechner speichern oder als JSON-Datei, die Sie in eine NFS-Freigabe exportieren (die eine unbegrenzte Anzahl von Zeilen enthalten kann). Wenn Data Sense Dateien (unstrukturierte Daten), Verzeichnisse (Ordner und Dateifreigaben) oder Datenbanken (strukturierte Daten) scannt, können bis zu drei Berichtsdateien heruntergeladen werden.

Beim Exportieren in eine Dateifreigabe stellen Sie sicher, dass Data Sense über die entsprechenden Berechtigungen für den Exportzugriff verfügt.

Generieren des Datenuntersuchungsberichts

Schritte

1. Klicken Sie auf der Seite „Untersuchung von Daten“ auf Oben rechts auf der Seite klicken.
2. Wählen Sie aus, ob Sie einen .CSV-Bericht oder einen JSON-Bericht der Daten herunterladen möchten, und klicken Sie auf **Bericht herunterladen**.



Geben Sie bei Auswahl eines JSON-Berichts den Namen der NFS-Freigabe ein, auf die der Bericht im Format heruntergeladen werden soll `<host_name>:/<share_path>`.

Ergebnis

Ein Dialogfeld zeigt eine Meldung an, dass die Berichte heruntergeladen werden.

Sie können den Fortschritt der JSON-Berichterstellung in anzeigen "Statusbereich Aktionen".

Was ist in jedem Datenuntersuchungs-Bericht enthalten

Der Datenbericht **unstrukturierte Dateien** enthält folgende Informationen zu Ihren Dateien:

- Dateiname
- Positionstyp
- Name der Arbeitsumgebung
- Storage-Repository (z. B. Volume, Bucket, Shares)
- Art der Arbeitsumgebung
- Dateipfad
- Dateityp
- Dateigröße
- Erstellungszeit
- Zuletzt geändert
- Zuletzt aufgerufen
- Dateibesitzer
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten

- Löscherkennung Datum

  Ein Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. So können Sie feststellen, wann sensible Dateien verschoben wurden. Gelöschte Dateien sind nicht Teil der Anzahl der Dateinummern, die im Dashboard oder auf der Untersuchungsseite angezeigt wird. Die Dateien werden nur in den CSV-Berichten angezeigt.

Der Datenbericht für unstrukturierte Verzeichnisse* enthält die folgenden Informationen zu Ihren Ordnern und Dateifreigaben:

- Name der Arbeitsumgebung
- Storage-Repository (beispielsweise ein Ordner oder Dateifreigaben)
- Art der Arbeitsumgebung
- Dateipfad (Verzeichnisname)
- Dateibesitzer
- Erstellungszeit
- Entdeckte Zeit
- Zuletzt geändert
- Zuletzt aufgerufen
- Berechtigungen öffnen
- Verzeichnistyp

Der **Structured Data Report** enthält die folgenden Informationen zu Ihren Datenbanktabellen:

- DB-Tabellenname
- Positionstyp
- Name der Arbeitsumgebung
- Storage-Repository (z. B. ein Schema)
- Anzahl der Spalten
- Zeilenanzahl
- Persönliche Angaben
- Sensible persönliche Daten

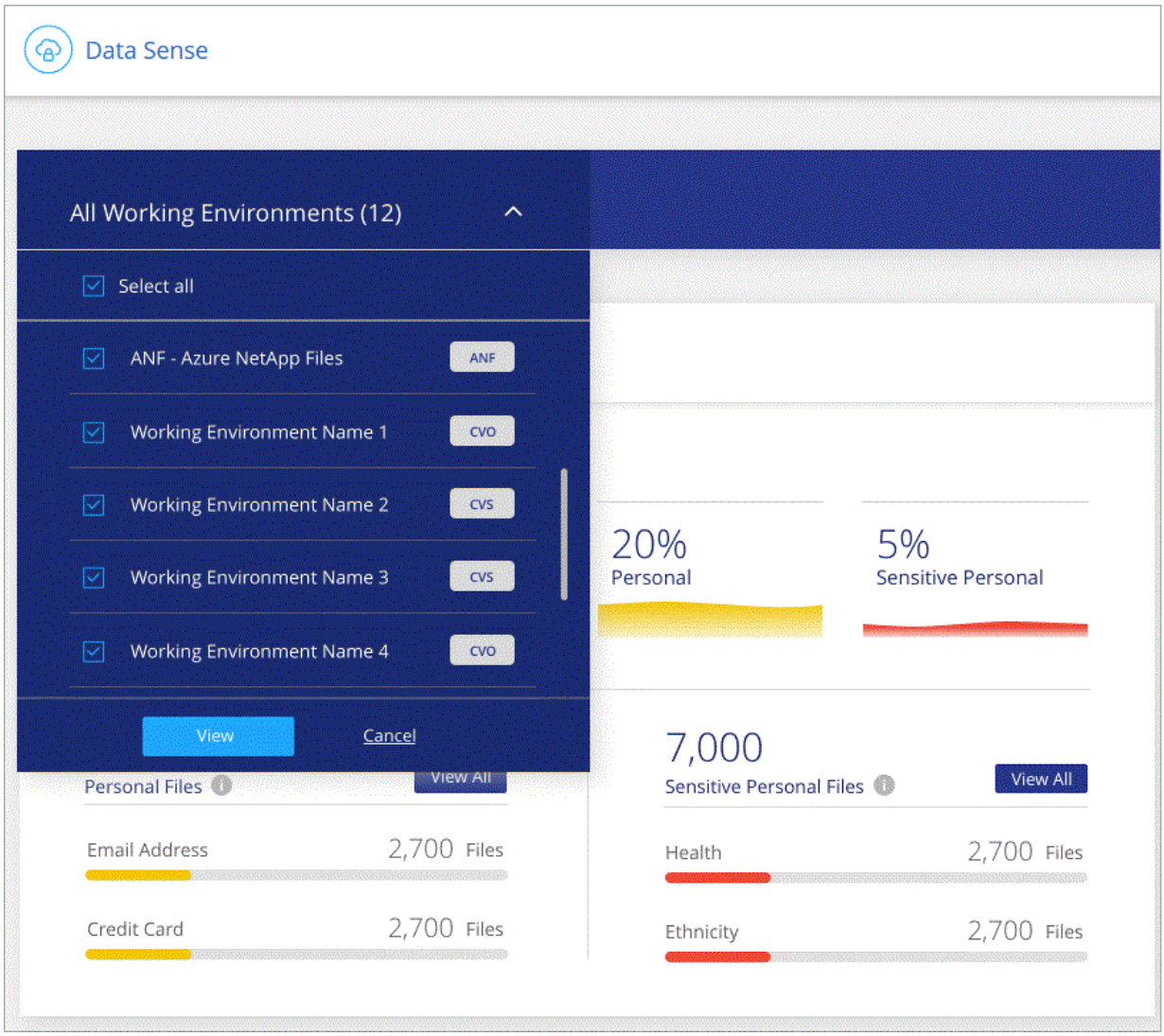
Auswählen der Arbeitsumgebungen für Berichte

Sie können die Inhalte des Cloud Data Sense Compliance Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur bestimmte Arbeitsumgebungen anzuzeigen.

Wenn Sie das Dashboard filtern, können Sie mit Data Sense die Compliance-Daten und -Berichte genau auf die von Ihnen ausgewählten Arbeitsumgebungen anwenden.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.



Reaktion auf eine Zugriffsanfrage für betroffene Person

Reagieren Sie auf eine DSAR (Data Subject Access Request), indem Sie nach dem vollständigen Namen oder der bekannten Kennung (z. B. einer E-Mail-Adresse) eines Studienteilnehmers suchen und dann einen Bericht herunterladen. Der Bericht soll Ihrem Unternehmen helfen, die Vorgaben der DSGVO oder ähnlicher Datenschutzgesetze einzuhalten.

Die DSAR-Funktionen stehen nur zur Verfügung, wenn Sie sich für eine vollständige Klassifizierungsprüfung Ihrer Datenquellen entschieden haben. Datenquellen, bei denen ein Scan nur für die Zuordnung durchgeführt wurde, bieten keine Details auf Dateiebene.

NetApp kann keine Garantie für 100 % der Genauigkeit persönlicher Daten und sensibler personenbezogener Daten, die Cloud Data Sense identifiziert. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Was ist ein Antrag auf Zugang für betroffene Person?

Datenschutzvorschriften wie die Europäische DSGVO erteilen Betroffenen (wie Kunden oder Mitarbeitern) das Recht, auf ihre personenbezogenen Daten zuzugreifen. Wenn eine betroffene Person diese Informationen anfordert, wird dies als DSAR (Zugriffsanfrage für betroffene Person) bezeichnet. Unternehmen sind verpflichtet, auf diese Anfragen „ohne übermäßige Verzögerung“ und spätestens innerhalb eines Monats nach Eingang zu reagieren.

Wie kann Cloud Data Sense Ihnen dabei helfen, auf einen DSAR zu reagieren?

Wenn Sie eine Suche für den Betroffenen durchführen, findet Cloud Data Sense alle Dateien, Buckets, OneDrive und SharePoint Konten, die darin ihren Namen oder ihr Kennung enthalten. Data Sense prüft die neuesten vorindizierten Daten auf den Namen oder die Kennung. Es wird kein neuer Scan gestartet.

Nachdem die Suche abgeschlossen ist, können Sie die Liste der Dateien für einen Bericht für die Anforderung von Datensubjekten herunterladen. Der Bericht sammelt Erkenntnisse aus den Daten und stellt die Daten zu rechtlichen Bedingungen bereit, die Sie an die Person zurücksenden können.

Die Suche nach Betroffenen wird derzeit in Datenbanken nicht unterstützt.

Suchen nach Betroffenen und Herunterladen von Berichten

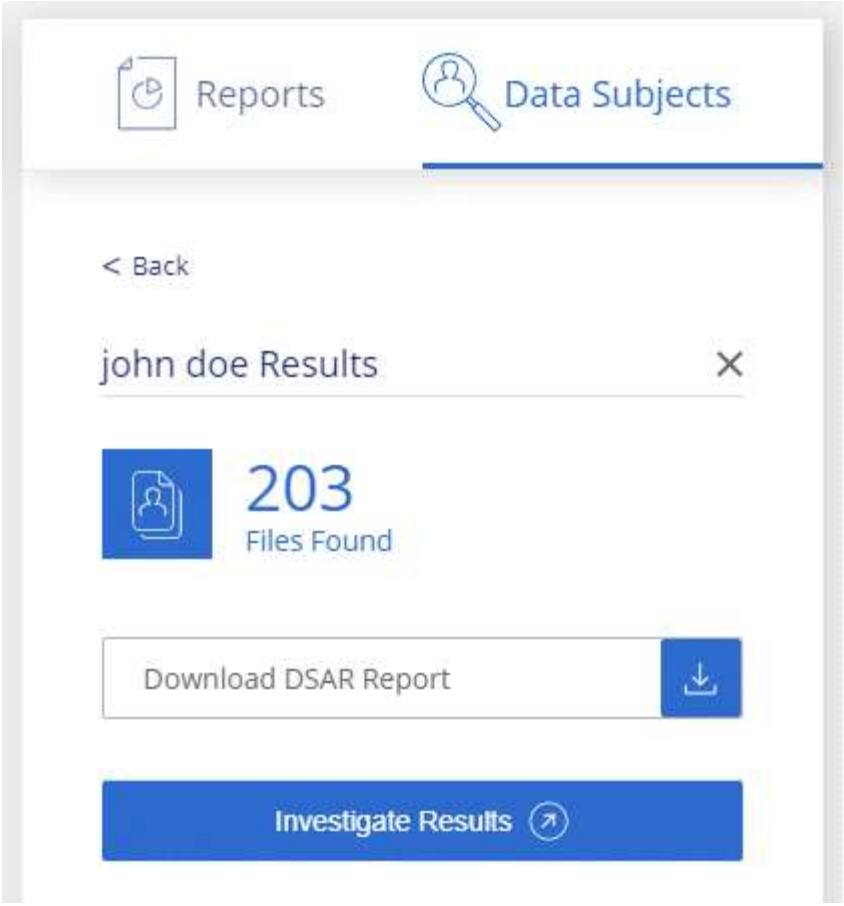
Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Suchen Sie nach "Alle persönlichen Informationstypen".

Englisch, Deutsch und Spanisch werden bei der Suche nach den Namen der Betroffenen unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie Auf **Data Subjects**.
3. Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen.

   Hier ein Beispiel, das eine Suche nach dem Namen *john doe* zeigt:



4. Wählen Sie eine der folgenden Optionen:
   - **Download DSAR Report**: Eine formelle Antwort auf die Zugriffsanfrage, die Sie an den Betroffenen senden können. Dieser Bericht enthält automatisch generierte Informationen auf der Grundlage von Daten, die Cloud Data Sense auf der betroffenen Person gefunden hat und als Vorlage verwendet werden können. Füllen Sie das Formular aus und überprüfen Sie es intern, bevor Sie es an den Betroffenen senden.
   - **Ergebnisse untersuchen**: Eine Seite, auf der Sie die Daten untersuchen können, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern und die Dateiliste herunterladen.

     Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die Top 10,000 in der Dateiliste angezeigt.

Kategorien von privaten Daten

Es gibt viele Arten von privaten Daten, die Cloud Data Sense in Ihren Volumes, Amazon S3 Buckets, Datenbanken, OneDrive Ordnern, SharePoint Konten, Und Google Drive Konten. Sehen Sie sich die folgenden Kategorien an.

Wenn Sie Cloud Data Sense zur Identifizierung anderer privater Datentypen benötigen, z. B. zusätzliche nationale ID-Nummern oder Kennungen des Gesundheitswesens, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com mit Ihrer Anfrage.

Arten personenbezogener Daten

Die in Dateien gefundenen personenbezogenen Daten können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte wird bestimmt, ob Cloud Data Sense verwendet wird "Prüfung der Nähe" Zum Validieren seiner Ergebnisse für die Kennung.

Die Artikel in dieser Kategorie können in jeder Sprache erkannt werden.

Beachten Sie, dass Sie der Liste der persönlichen Daten, die in Ihren Dateien gefunden werden, hinzufügen können, wenn Sie einen Datenbank-Server scannen. Mit der Funktion *Data Fusion* können Sie die zusätzlichen Kennungen auswählen, die Cloud Data Sense bei seinen Scans sucht, indem Sie Spalten in einer Datenbanktabelle auswählen. Siehe "Hinzufügen von ID-Kennungen unter Verwendung von Data Fusion" Entsprechende Details.

Typ	Kennung	Näherungsvalidierung?
Allgemein	E-Mail-Adresse	Nein
	Kreditkartennummer	Nein
	Betroffenen	Nein
	IBAN-Nummer (International Bank Account Number)	Nein
	IP-Adresse	Nein
	Passwort	Ja.

Typ	Kennung	Näherungsvalidierung?
Nationale Kennungen		

Typ	Kennung	Näherungsvalidierung?
	Lettischer Ausweis	Ja.
	Litauische ID	Ja.
	Luxemburg-ID	Ja.
	Maltesische ID	Ja.
	NHS-Nummer (National Health Service)	Ja.
	New York Führerschein	Ja.
	Konto Einer Neuseeländischen Bank	Ja.
	Neuseeländische Führerschein	Ja.
	Neuseeland-IRD-Nummer (Steuernummer)	Ja.
	Neuseeland NHI (National Health Index) Nummer	Ja.
	Neuseeländische Passnummer	Ja.
	Polish ID (PESEL)	Ja.
	Portugiesische Steuernummer (NIF)	Ja.
	Rumänische ID (CNP)	Ja.
	Slowenische ID (EMSO)	Ja.
	Südafrikanischer Ausweis	Ja.
	Spanische Steuernummer	Ja.
	Schwedische ID	Ja.
	Texas Driver’s License	Ja.
	GROSSBRITANNIEN ID (NINO)	Ja.
	USA Sozialversicherungsnummer (SSN)	Ja.

Arten sensibler personenbezogener Daten

Die sensiblen personenbezogenen Daten, die Cloud Data Sense in Dateien finden kann, umfassen die folgende Liste: Die Artikel in dieser Kategorie können derzeit nur auf Englisch erkannt werden.

Referenz Für Kriminelle Verfahren
: Daten zu strafrechtlichen Überzeugungen und Straftaten einer natürlichen Person.

Ethnische Referenz
: Daten über die rassische oder ethnische Herkunft einer natürlichen Person.

Systemzustand
: Daten über die Gesundheit einer natürlichen Person.

ICD-9-CM-Ärztliche Codes
: Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

ICD-10-CM-Ärztliche Codes
: Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

Philosophische Überzeugungen Referenz

Daten über die philosophischen Überzeugungen einer natürlichen Person.

Politische Meinungen Referenz

Daten über die politischen Meinungen einer natürlichen Person.

Religiöse Überzeugungen Referenz

Daten über die religiösen Überzeugungen einer natürlichen Person.

Sexualleben oder Orientierung Referenz

Daten über das Sexualleben einer natürlichen Person oder die sexuelle Orientierung.

Arten von Kategorien

Cloud Data Sense kategorisiert Ihre Daten wie folgt. Die meisten dieser Kategorien können in Englisch, Deutsch und Spanisch anerkannt werden.

Kategorie	Typ	Englisch	Deutsch	Spanisch
Finanzen	Bilanz	✓	✓	✓
	Bestellungen	✓	✓	✓
	Rechnungen	✓	✓	✓
	Vierteljährliche Berichte	✓	✓	✓
HR	Background-Checks	✓		✓
	Vergütungspläne	✓	✓	✓
	Mitarbeiterverträge	✓		✓
	Mitarbeiterbewertung	✓		✓
	Systemzustand	✓		✓
	Wird Fortgesetzt	✓	✓	✓
Legal	NDAs	✓	✓	✓
	Verträge zwischen Anbietern und Kunden	✓	✓	✓
Marketing	Kampagnen	✓	✓	✓
	Konferenzen	✓	✓	✓
Betrieb	Audit-Berichte	✓	✓	✓
Vertrieb	Aufträge	✓	✓	
Services	RFI	✓		✓
	AUSSCHREIBUNG	✓		✓
	SOW	✓	✓	✓
	Schulung	✓	✓	✓
Unterstützung	Reklamationen und Tickets	✓	✓	✓

Die folgenden Metadaten werden ebenfalls kategorisiert und in den gleichen unterstützten Sprachen identifiziert:

- Applikationsdaten
- Archivdateien
- Audio
- Daten Von Business-Applikationen
- CAD-Dateien
- Codieren
- Beschädigt
- Datenbank- und Indexdateien
- Daten Spüren Breadcrumbs
- Design-Dateien
- E-Mail-Anwendungsdaten
- Verschlüsselt
- Ausführbare Dateien
- Daten Aus Finanzapplikationen
- Daten Der Integritätsanwendungen
- Bilder
- Protokolle
- Verschiedene Dokumente
- Diverse Präsentationen
- Verschiedene Tabellenkalkulationen
- Verschiedenes „Unbekannt“
- Strukturierte Daten
- Videos
- Zero-Byte-Dateien

Dateitypen

Cloud Data Sense scannt alle Dateien nach Informationen zu Kategorie und Metadaten und zeigt alle Dateitypen im Abschnitt Dateitypen des Dashboards an.

Wenn Data Sense jedoch personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt:

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

Genauigkeit der gefundenen Informationen

NetApp kann keine Garantie für 100 % der Genauigkeit persönlicher Daten und sensibler personenbezogener Daten, die Cloud Data Sense identifiziert. Überprüfen Sie die Informationen immer, indem Sie die Daten

überprüfen.

Auf der Grundlage unserer Tests zeigt die folgende Tabelle die Genauigkeit der Informationen, die Data Sense findet. Wir brechen es durch *Precision* und *Recall* ab:

Präzision

Die Wahrscheinlichkeit, dass das, was Data Sense findet, korrekt identifiziert wurde. Beispielsweise bedeutet eine Datengenauigkeit von 90% für personenbezogene Daten, dass 9 von 10 Dateien, die als personenbezogene Daten identifiziert werden, tatsächlich personenbezogene Daten enthalten. 1 von 10 Dateien wäre falsch positiv.

Rückruf

Die Wahrscheinlichkeit, dass Daten sinnvoll zu finden, was sie sollten. Beispielsweise bedeutet eine Rückrufquote von 70 % für personenbezogene Daten, dass Data Sense 7 von 10 Dateien identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Data Sense würde 30% der Daten vermissen und es wird nicht im Dashboard erscheinen.

Wir verbessern die Genauigkeit unserer Ergebnisse ständig. Diese Verbesserungen werden in zukünftigen Data Sense Versionen automatisch verfügbar sein.

Typ	Präzision	Rückruf
Personenbezogene Daten - Allgemeines	90 % - 95 %	60 % - 80 %
Persönliche Daten – Länderkennungen	30 % - 60 %	40 % - 60 %
Sensible persönliche Daten	80 % - 95 %	20 % - 30 %
Kategorien	90 % - 97 %	60 % - 80 %