BlueXP Klassifizierung nutzen

BlueXP classification

NetApp
April 03, 2024

Inhalt

BlueXP Klassifizierung nutzen

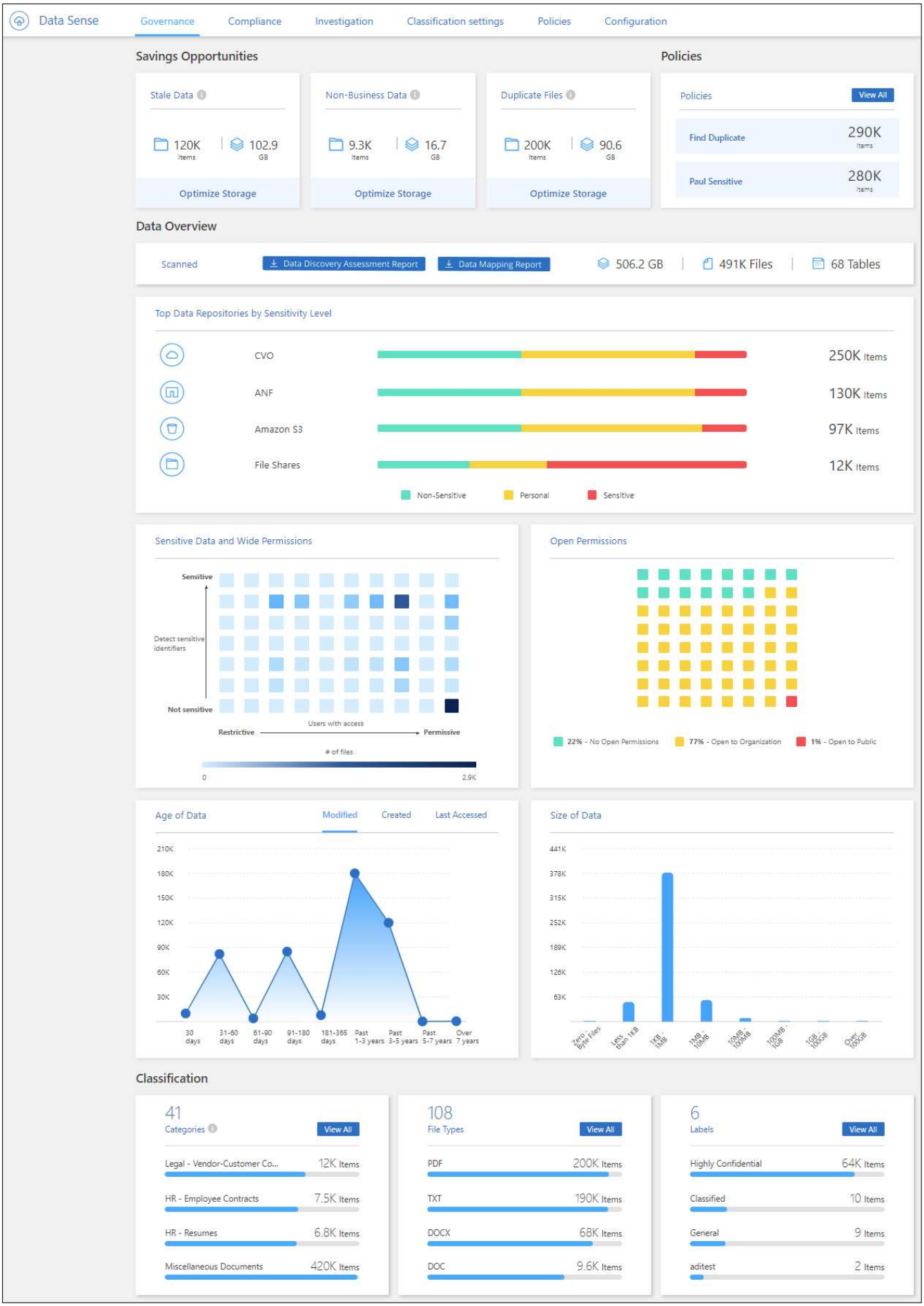
Zeigen Sie Governance-Details zu den in Ihrer Organisation gespeicherten Daten an

Behalten Sie die Kontrolle über die Kosten im Zusammenhang mit Daten auf den Storage-Ressourcen Ihres Unternehmens. Die BlueXP Klassifizierung ermittelt die Menge veralteter Daten, nicht geschäftsferner Daten, mehrfach vorhandener Dateien und sehr großer Dateien auf Ihren Systemen. So können Sie entscheiden, ob Sie einige Dateien entfernen oder auf kostengünstigeren Objekt-Storage verschieben möchten.

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


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co... 12K Items
HR - Employee Contracts 7.5K Items
HR - Resumes 6.8K Items
Miscellaneous Documents 420K Items
108
File Types
View All
PDF 200K Items
TXT 190K Items
DOCX 68K Items
DOC 9.6K Items
6
Labels
View All
Highly Confidential 64K Items
Classified 10 Items
General 9 Items
aditest 2 Items

Speichern Sie Opportunitys

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".

  HINWEIS

  Wenn eine Ihrer Datenquellen Daten-Tiering implementiert, werden alte Daten, die sich bereits im Objektspeicher befinden, möglicherweise in der Kategorie „veraltete Daten“ identifiziert.

Politik mit der größten Anzahl von Ergebnissen

Im Bereich *Policies* werden die Richtlinien mit der größten Anzahl von Ergebnissen oben in der Liste angezeigt. Klicken Sie auf den Namen einer Richtlinie, 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

Der Abschnitt *Data Overview* bietet einen schnellen Überblick über alle zu scannenden Daten. Klicken Sie auf die Schaltfläche, um einen vollständigen Bericht zur Datenzuordnung herunterzuladen, der Nutzungskapazität, Alter der Daten, Datengröße und Dateitypen für alle Arbeitsumgebungen und Datenquellen enthält. Siehe Datenzuordnungsbericht Alle Details zu diesem Bericht.

Die wichtigsten Daten-Repositorys, die nach Sensibilität aufgeführt sind

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

- Nicht-sensible Daten
- Persönliche Daten
- Sensible personenbezogene Daten

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

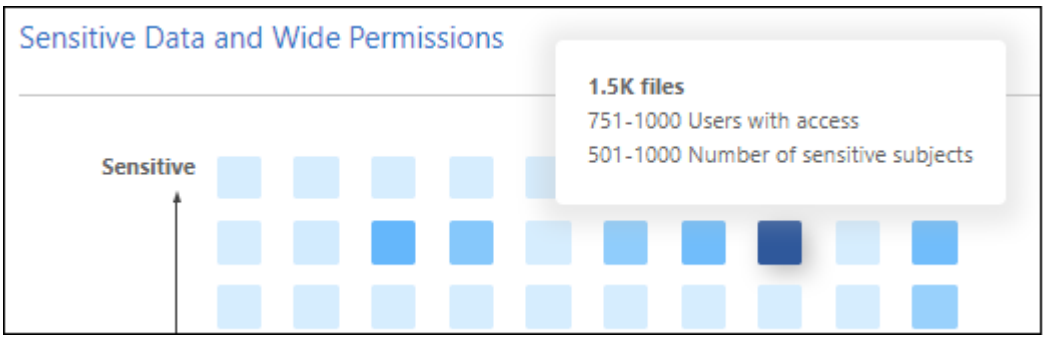
anzuzeigen.

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

Daten, die nach Sensitivität und breiten Berechtigungen aufgelistet sind

Der Bereich *sensible Daten und Wide Permissions* bietet eine Heatmap von Dateien, die sensible Daten (einschließlich sensibler und sensibler personenbezogener Daten) enthalten und zu permissiv sind. So erkennen Sie, wo Sie möglicherweise Risiken mit sensiblen Daten haben.

Die Dateien werden anhand der Anzahl der Benutzer bewertet, die berechtigt sind, auf die Dateien auf der X-Achse (niedrigste bis höchste) zuzugreifen, und die Anzahl der sensiblen Kennungen innerhalb der Dateien auf der Y-Achse (niedrigste bis höchste). Die Blöcke stellen die Anzahl der Dateien dar, die mit den Elementen der X- und Y-Achsen übereinstimmen. Der hellere Block ist gut, da weniger Benutzer auf die Dateien zugreifen können und weniger sensible Kennungen pro Datei. Die dunkleren Blöcke sind die Elemente, die Sie untersuchen möchten. Auf dem folgenden Bildschirm wird beispielsweise der Mauszeiger für den dunkelblauen Block angezeigt. Es zeigt, dass Sie 1,500 Dateien haben, auf die 751-100 Benutzer zugreifen können und wo es 501-100 sensible Kennungen pro Datei gibt.



Sie können auf den Block klicken, für den Sie sich interessieren, um die gefilterten Ergebnisse der betroffenen Dateien auf der Untersuchungsseite anzuzeigen, damit Sie weitere Untersuchungen durchführen können.

Wenn Sie keinen Identitätsdienst mit BlueXP-Klassifizierung integriert haben, werden in diesem Bereich keine Daten angezeigt. "Erfahren Sie, wie Sie Ihren Active Directory-Service in die BlueXP Klassifizierung integrieren".

> Dieses Fenster unterstützt Dateien in CIFS-Freigaben, OneDrive und SharePoint-Datenquellen. Derzeit werden Datenbanken, Google Drive, Amazon S3 und generischer Objektspeicher nicht unterstützt.

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:

- Keine Offenen Berechtigungen
- 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.

  HINWEIS

  Wenn eine Ihrer Datenquellen Daten-Tiering implementiert, können im Diagramm „_Age of Data“ alte Daten, die sich bereits im Objektspeicher befinden, identifiziert werden.

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 anzeigen, die Sie haben. 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.

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 eine Übersicht, in der alle Arbeitsumgebungen und Datenquellen zusammengefasst sind, und enthält dann eine Aufschlüsselung für jede Arbeitsumgebung.

Der Bericht enthält die folgenden Informationen:

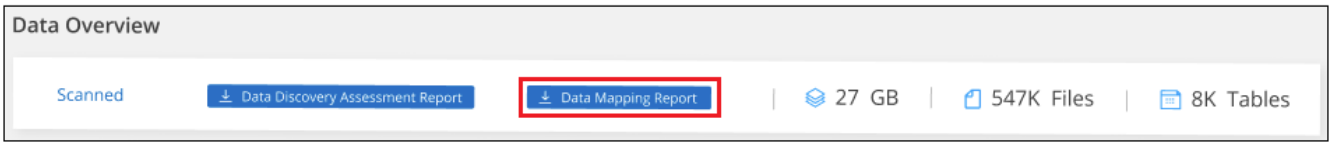
Kategorie	Beschreibung
Nutzung Von Kapazitäten	Für alle Arbeitsumgebungen: Listet die Anzahl der Dateien und die genutzte Kapazität für jede Arbeitsumgebung. Für einzelne Arbeitsumgebungen: Listet die Dateien auf, die die größte Kapazität nutzen.
Alter der Daten	Bietet drei Diagramme und Diagramme für 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.

Generieren Sie den Bericht zur Datenzuordnung

Sie generieren diesen Bericht über die Registerkarte Governance in der BlueXP Klassifizierung.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Governance** und dann auf die Schaltfläche **Data Mapping Report**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Wenn der Bericht größer als 1 MB ist, wird die PDF-Datei auf der BlueXP Klassifizierungsinstanz beibehalten, und es wird eine Popup-Nachricht über den genauen Speicherort angezeigt. Wenn die BlueXP Klassifizierung auf einer lokalen Linux-Maschine oder auf einer Linux-Maschine, die Sie in der Cloud implementiert haben, installiert ist, können Sie direkt zur PDF-Datei navigieren. Wenn die BlueXP Klassifizierung in der Cloud implementiert wird, müssen Sie SSH zur BlueXP Klassifizierungsinstanz verwenden, um eine PDF-Datei herunterzuladen. "Informationen zum Zugriff auf Daten auf der Klassifikationsinstanz finden Sie unter".

Beachten Sie, dass Sie den Unternehmensnamen, der auf der ersten Seite des Berichts angezeigt wird, oben auf der BlueXP Klassifizierungsseite anpassen können, indem Sie auf klicken ⋮ Und dann auf **Firmenname ändern** klicken. Wenn Sie den Bericht das nächste Mal generieren, wird er den neuen Namen enthalten.

Data Discovery Assessment-Bericht

Der Data Discovery Assessment Report bietet eine allgemeine Analyse der gescannten Umgebung, um die Ergebnisse des Systems hervorzuheben und Problembereiche und mögliche Schritte zur Problembehebung

aufzuzeigen. Die Ergebnisse basieren sowohl auf der Zuordnung als auch auf der Klassifizierung Ihrer Daten. Mit diesem Bericht soll das Bewusstsein für drei wesentliche Aspekte Ihres Datensatzes gestärkt werden:

Merkmal	Beschreibung
Bedenken hinsichtlich der Daten-Governance	Ein detaillierter Überblick über alle Daten, die Sie besitzen, und Bereiche, in denen Sie die Datenmenge möglicherweise reduzieren und Kosten einsparen können.
Risiken im Hinblick auf die Datensicherheit	Bereiche, in denen Daten aufgrund umfassender Zugriffsberechtigungen für interne oder externe Angriffe verfügbar sind.
Lücken in der Daten-Compliance	Ihre personenbezogenen oder sensiblen personenbezogenen Daten sind sowohl aus Sicherheitsgründen als auch für DSLR-Zwecke (Zugriffsanfragen von Betroffenen) gespeichert.

Nach der Bewertung enthält dieser Bericht Bereiche, in denen Sie:

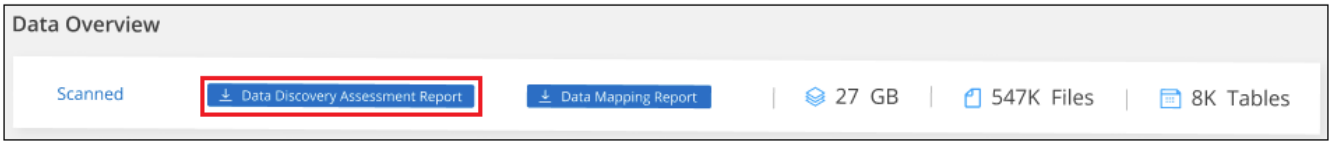
- Senkung der Storage-Kosten durch Ändern der Aufbewahrungsrichtlinie oder durch Verschieben oder Löschen bestimmter Daten (veraltete, doppelte oder nicht geschäftsfremde Daten)
- Schützen Sie Ihre berechtigen Daten durch eine Überarbeitung der globalen Richtlinien für das Gruppenmanagement
- Schützen Sie Ihre persönlichen oder sensiblen Daten, indem Sie personenbezogene Daten in sicherere Datenspeicher verlagern

Generieren Sie den Data Discovery Assessment Report

Sie generieren diesen Bericht über die Registerkarte Governance in der BlueXP Klassifizierung.

Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Klassifizierung**.
2. Klicken Sie auf **Governance** und dann auf die Schaltfläche **Data Discovery Assessment Report**.



Ergebnis

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Beachten Sie, dass Sie den Unternehmensnamen, der auf der ersten Seite des Berichts angezeigt wird, oben auf der BlueXP Klassifizierungsseite anpassen können, indem Sie auf klicken Und dann auf **Firmenname ändern** klicken. Wenn Sie den Bericht das nächste Mal generieren, wird er den neuen Namen enthalten.

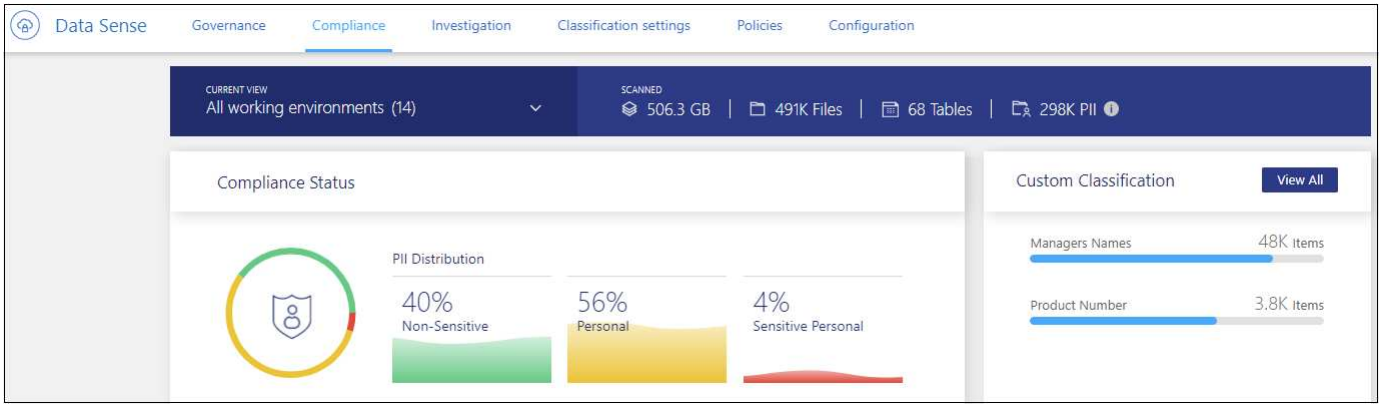
Zeigen Sie Compliance-Details zu den in Ihrem Unternehmen gespeicherten Daten an

Mehr Kontrolle über Ihre persönlichen Daten durch die Anzeige von Details zu den personenbezogenen Daten und vertraulichen personenbezogenen Daten in Ihrem

Unternehmen. Zusätzlich können Sie sich Sichtbarkeit verschaffen, indem Sie die Kategorien und Dateitypen überprüfen, die in Ihren Daten für die BlueXP Klassifizierung gefunden wurden.

> 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.

Im BlueXP Klassifizierungs-Dashboard werden standardmäßig 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.

Dateien anzeigen, die personenbezogene Daten enthalten

Durch die BlueXP Klassifizierung werden automatisch bestimmte Wörter, Strings und Muster (Regex) innerhalb der Daten identifiziert. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern, Kontonummern, Passwörter, Und vieles mehr. "Die vollständige Liste finden Sie hier". Durch die BlueXP Klassifizierung wird diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordner) oder in Datenbanktabellen identifiziert.

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 personenbezogenen Daten verwendet die BlueXP Klassifizierung *Proximity Validation*, um ihre Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. Beispielsweise identifiziert die BlueXP Klassifizierung eine US Sozialversicherungsnummer (SSN) als SSN, wenn sie neben ihr ein Näherungswort sieht - zum Beispiel *SSN* oder *Sozialversicherung*. "Der Tisch der personenbezogenen Daten" Zeigt an, wann die BlueXP Klassifizierung die Validierung der Nähe verwendet.

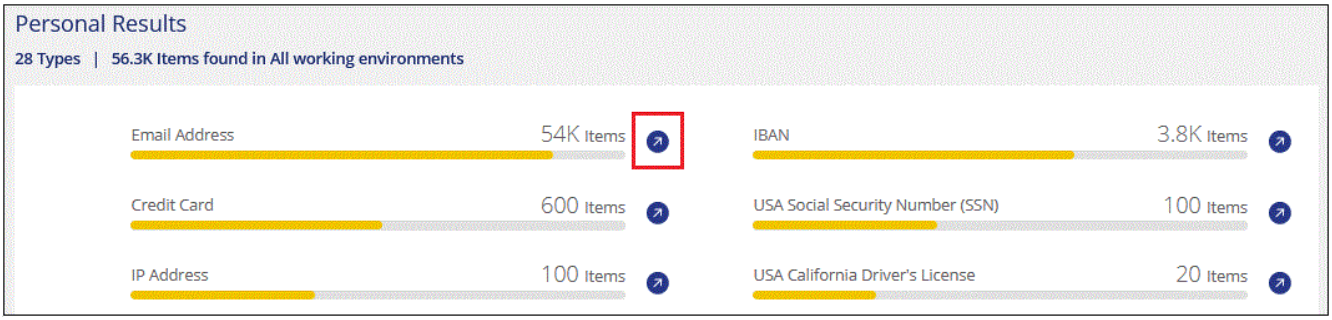
Schritte

1. Klicken Sie im Navigationsmenü von BlueXP links auf **Governance > Klassifizierung** und dann auf die

Registerkarte **Compliance**.

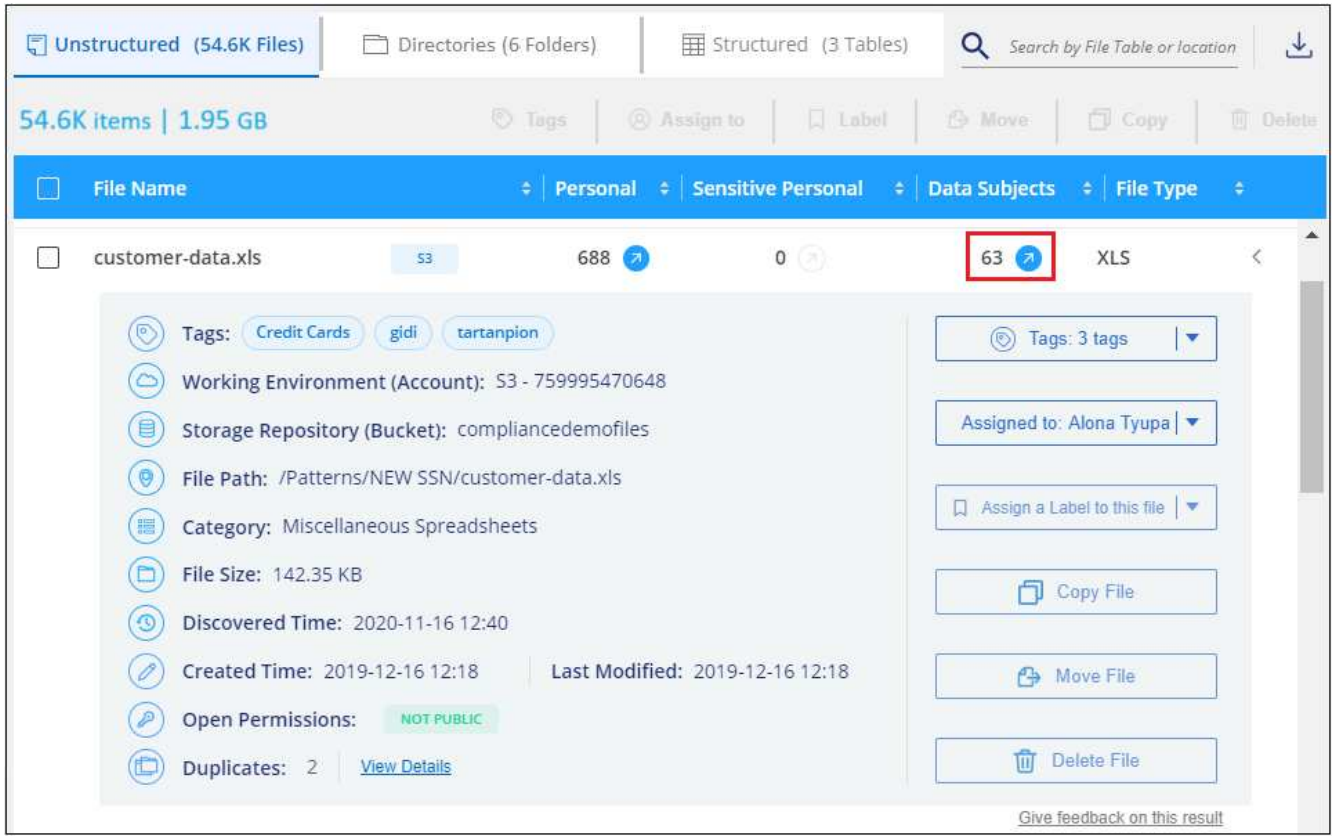
2. Um die Angaben zu allen personenbezogenen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz der persönlichen Daten.

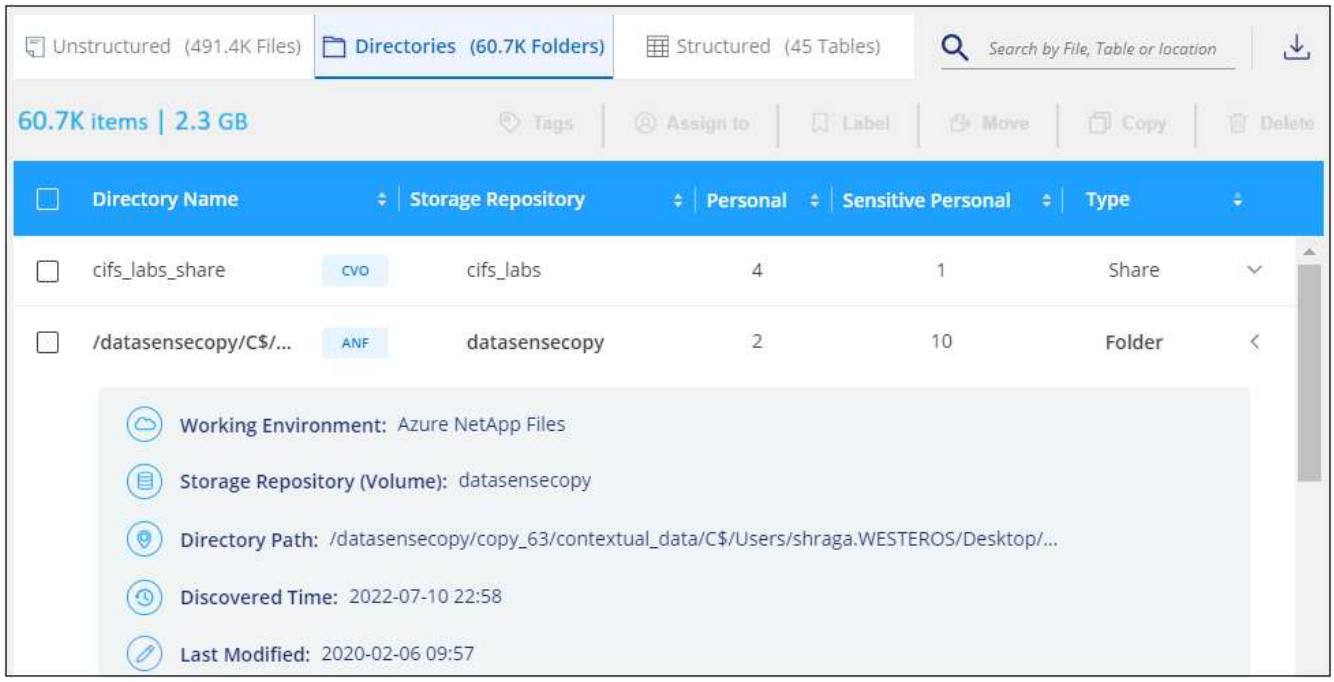
3. Um die Daten für eine bestimmte Art von personenbezogenen Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ von personenbezogenen Daten, z. B. E-Mail-Adressen.



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.





Dateien anzeigen, die sensible personenbezogene Daten enthalten

Die BlueXP Klassifizierung identifiziert automatisch besondere Arten von sensiblen personenbezogenen Daten, wie sie beispielsweise durch Datenschutzvorschriften 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". Durch die BlueXP Klassifizierung wird diese Art von Informationen in einzelnen Dateien, in Dateien innerhalb von Verzeichnissen (Freigaben und Ordner) oder in Datenbanktabellen identifiziert.

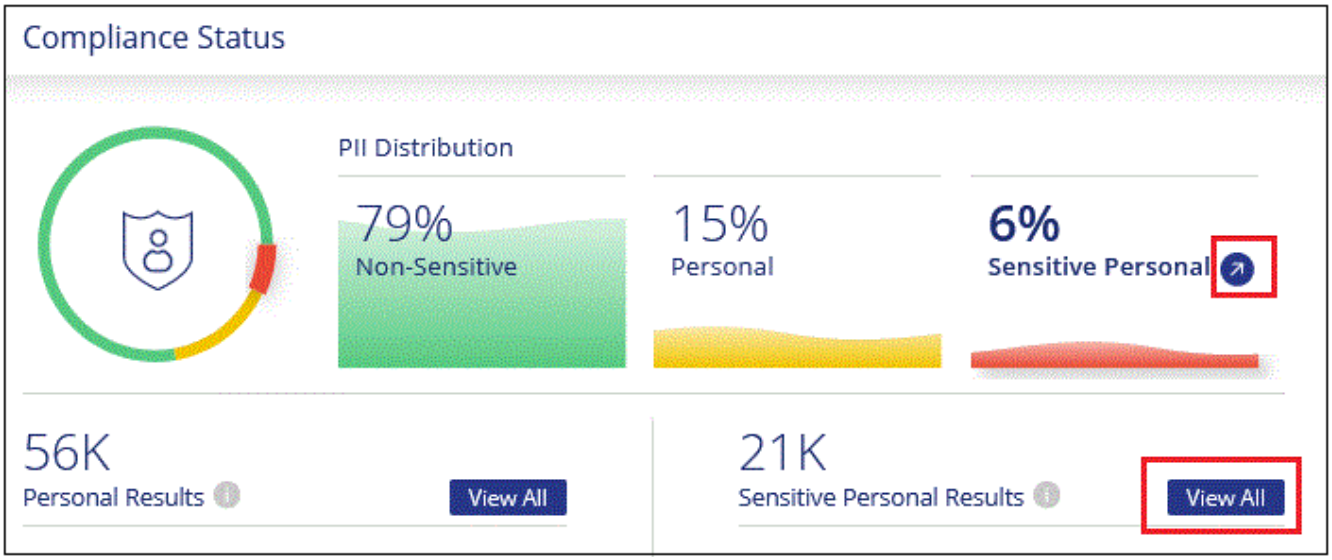
Die BlueXP Klassifizierung verwendet künstliche Intelligenz (KI), Natural Language Processing (NLP), Machine Learning (ML) und Cognitive Computing (CC), um die Bedeutung des gescannten Inhalts zu verstehen. Anhand dessen werden Entitäten extrahiert und entsprechend kategorisiert.

Beispielsweise ist eine sensitive DSGVO-Datenkategorie ethnisch Ursprungs. Aufgrund der NLP-Fähigkeiten kann die BlueXP Klassifizierung den Unterschied zwischen einem Satz unterscheiden: „George ist Mexikaner“ (sensible sensible sensible Daten gemäß DSGVO, Artikel 9) und „George isst Mexikanisch“.

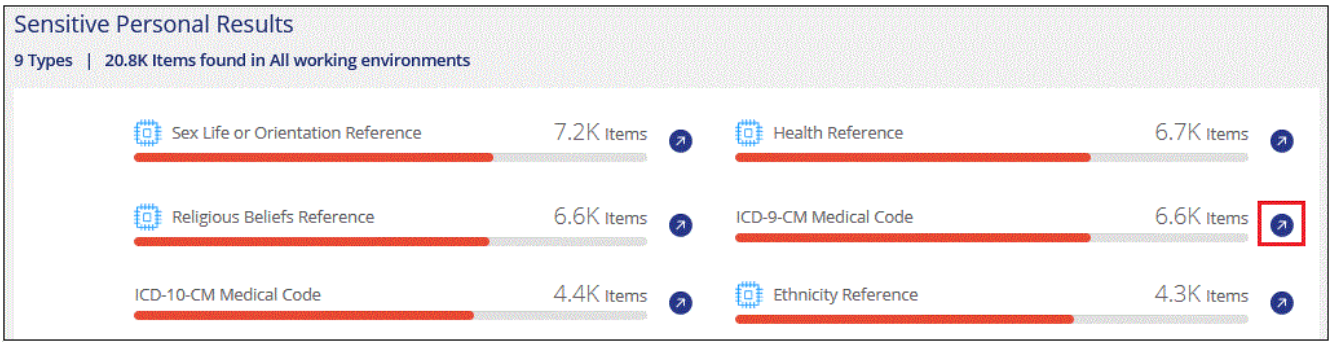
> Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

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.

Dateien nach Kategorien anzeigen

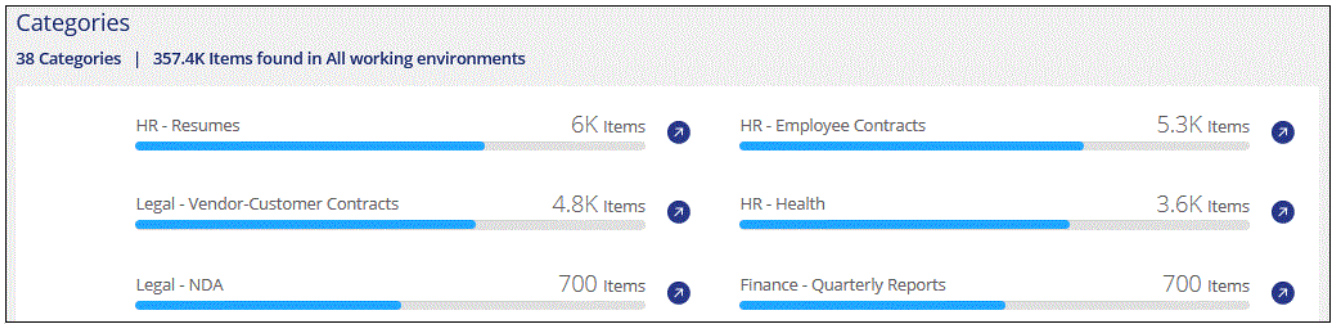
Die BlueXP Klassifizierung unterteilt die gescannten Daten in unterschiedliche Kategorien. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Siehe die Liste der Kategorien".

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.

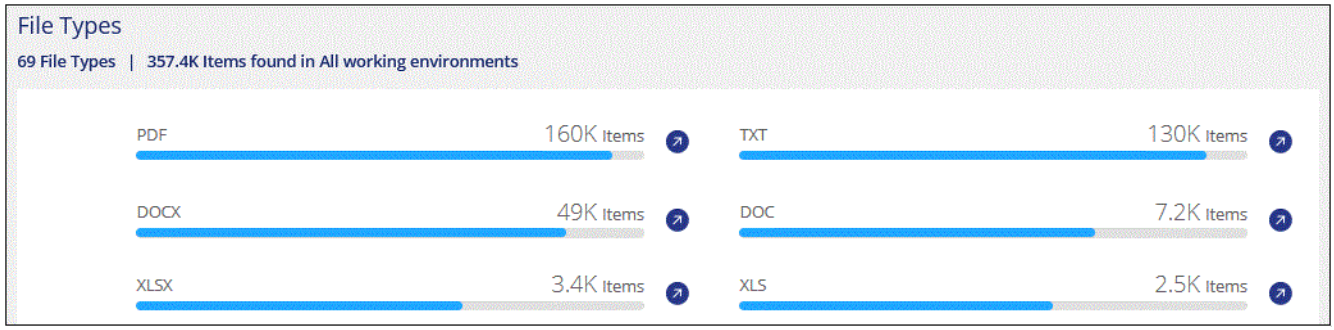
Dateien nach Dateitypen anzeigen

Die BlueXP Klassifizierung unterteilt die gescannten Daten nach Dateityp. 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.

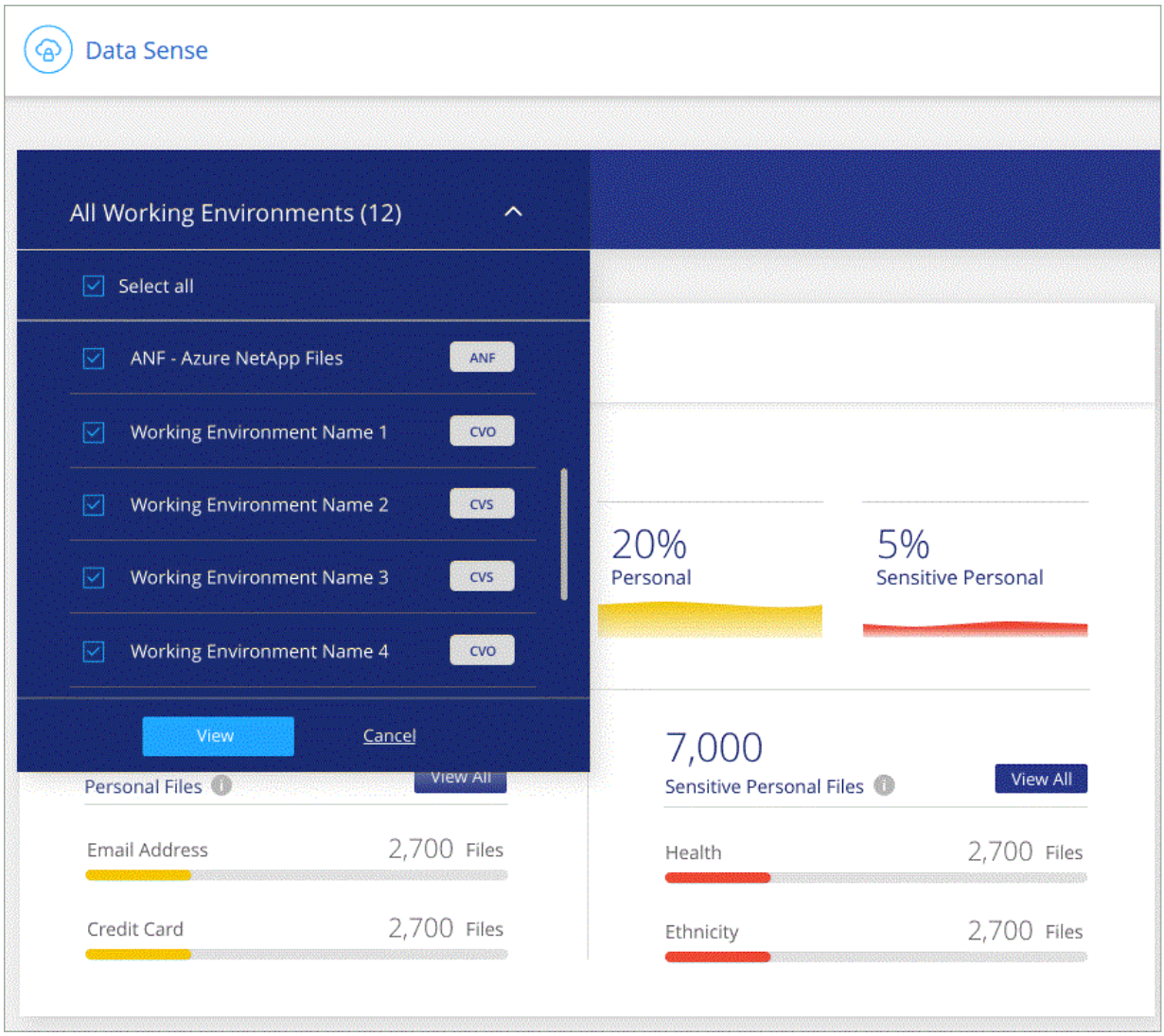
Anzeigen von Dashboard-Daten für bestimmte Arbeitsumgebungen

Sie können die Inhalte des BlueXP Klassifizierungs-Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen einzusehen.

Wenn Sie das Dashboard filtern, erfasst die BlueXP Klassifizierung die Compliance-Daten und Berichte nur an die von Ihnen ausgewählten Applikationsumgebungen.

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**.



Kategorien von privaten Daten

Es gibt viele Arten von privaten Daten, die durch die BlueXP Klassifizierung in Ihren Volumes, Amazon S3 Buckets, Datenbanken, OneDrive-Ordnern, SharePoint-Konten identifiziert werden können. Und Google Drive-Konten. Sehen Sie sich die folgenden Kategorien an.

> Wenn Sie zur Identifizierung anderer privater Datentypen die Klassifizierung von BlueXP benötigen, z. B. zusätzliche nationale ID-Nummern oder Identifikatoren in Ihrem Gesundheitswesen, senden Sie eine E-Mail an ng-contact-data-sense@netapp.com.

Arten personenbezogener Daten

Die in Dateien gefundenen personenbezogenen Daten können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte der Tabelle unten wird angegeben, ob die BlueXP Klassifizierung verwendet "Prüfung der Nähe" Zum Validieren seiner Ergebnisse für die Kennung.

Die Sprachen, in denen diese Elemente erkannt werden können, sind in der Tabelle aufgeführt.

Beachten Sie, dass Sie der Liste der persönlichen Daten, die in Ihren Dateien gefunden werden, hinzufügen können. Wenn Sie einen Datenbankserver scannen, können Sie mit der Funktion *Data Fusion* zusätzliche Kennungen auswählen, nach denen die BlueXP-Klassifizierung in ihren Scans suchen wird, indem Sie Spalten in einer Datenbanktabelle auswählen. Sie können auch benutzerdefinierte Schlüsselwörter aus einer Textdatei oder benutzerdefinierte Muster mit einem regulären Ausdruck hinzufügen. Siehe "Hinzufügen persönlicher Daten-IDs zu Ihren BlueXP Klassifizierungs-Scans" Entsprechende Details.

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
Allgemein	Kreditkartennummer	Nein	✓	✓	✓		✓
	Betroffenen	Nein	✓	✓	✓		
	E-Mail-Adresse	Nein	✓	✓	✓		✓
	IBAN-Nummer (internationale Bankkontonummer)	Nein	✓	✓	✓		✓
	IP-Adresse	Nein	✓	✓	✓		✓
	Passwort	Ja.	✓	✓	✓		✓

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
Nationale Kennungen							

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
	Sozialversicherungsnummer	Ja.	✓	✓	✓		
	Steuernummer (Steuerliche Identifikationsnummer)	Ja.	✓	✓	✓		
	Griechische ID	Ja.	✓	✓	✓		
	Ungarische Steuernummer	Ja.	✓	✓	✓		
	Irish ID (PPS)	Ja.	✓	✓	✓		
	Israelische ID	Ja.	✓	✓	✓		
	Italienische Steuernummer	Ja.	✓	✓	✓		
	Japanische Personal Identification Number (Privat- und Firmennummer)	Ja.	✓	✓	✓		✓
	Lettischer Ausweis	Ja.	✓	✓	✓		
	Litauische ID	Ja.	✓	✓	✓		
	Luxemburg-ID	Ja.	✓	✓	✓		
	Maltesische ID	Ja.	✓	✓	✓		
	NHS-Nummer (National Health Service)	Ja.	✓	✓	✓		
	Konto Einer Neuseeländischen Bank	Ja.	✓	✓	✓		
	Führerschein in Neuseeland	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.	✓	✓	✓		
	Personalausweis für die nationale Registrierung in Singapur (NRIC)	Ja.	✓	✓	✓		
	Slowenische ID (EMSO)	Ja.	✓	✓	✓		
	Südafrikanischer Ausweis	Ja.	✓	✓	✓		
	Spanische Steuernummer	Ja.	✓	✓	✓		
	Schwedische ID	Ja.	✓	✓	✓		
	Texas Driver’s License	Ja.	✓	✓	✓		
	GROSSBRITANNIEN ID (NINO)	Ja.	✓	✓	✓		
	USA California Driver’s License	Ja.	✓	✓	✓		
	USA Indiana Führerschein	Ja.	✓	✓	✓		
	USA New York Führerschein	Ja.	✓	✓	✓		
	USA Sozialversicherungsnummer (SSN)	Ja.	✓	✓	✓		

Arten sensibler personenbezogener Daten

Die sensiblen personenbezogenen Daten, die die BlueXP Klassifizierung in Dateien finden kann, enthalten 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

Die BlueXP Klassifizierung 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	✓	✓	✓

Kategorie	Typ	Englisch	Deutsch	Spanisch
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
- BlueXP Klassifizierungs-Breadcrumbs
- Design-Dateien
- E-Mail-Anwendungsdaten
- Verschlüsselt (Dateien mit hohem Entropie-Wert)
- Ausführbare Dateien
- Daten Aus Finanzapplikationen

- Daten Der Integritätsanwendungen
- Bilder
- Protokolle
- Verschiedene Dokumente
- Diverse Präsentationen
- Verschiedene Tabellenkalkulationen
- Verschiedenes „Unbekannt“
- Passwortgeschützte Dateien
- Strukturierte Daten
- Videos
- Zero-Byte-Dateien

Dateitypen

Die BlueXP Klassifizierung scannt alle Dateien nach Kategorien- und Metadaten und zeigt alle Dateitypen im Abschnitt „Dateitypen“ des Dashboards an.

Wenn jedoch die BlueXP Klassifizierung personenbezogene Daten 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 die Genauigkeit der personenbezogenen Daten und sensiblen personenbezogenen Daten, die durch die BlueXP Klassifizierung identifiziert werden, nicht zu 100 % garantieren. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Basierend auf unseren Tests zeigt die folgende Tabelle die Genauigkeit der Informationen, die bei der BlueXP Klassifizierung als Ergebnis zu finden sind. Wir brechen es durch *Precision* und *Recall* ab:

Präzision

Die Wahrscheinlichkeit, dass die gefundenen Elemente der BlueXP Klassifizierung korrekt identifiziert wurden. 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 die BlueXP Klassifizierung ihre Inhalte findet. Beispielsweise bedeutet eine Rückrufrate von 70 % für personenbezogene Daten, dass die BlueXP Klassifizierung 7 von 10 Dateien identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Die BlueXP Klassifizierung würde 30 % der Daten verfehlen und wird dann nicht im Dashboard angezeigt.

Wir verbessern die Genauigkeit unserer Ergebnisse ständig. Diese Verbesserungen werden in zukünftigen BlueXP Klassifizierungs-Releases automatisch zur Verfügung stehen.

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 %

Untersuchen Sie die in Ihrem Unternehmen gespeicherten Daten

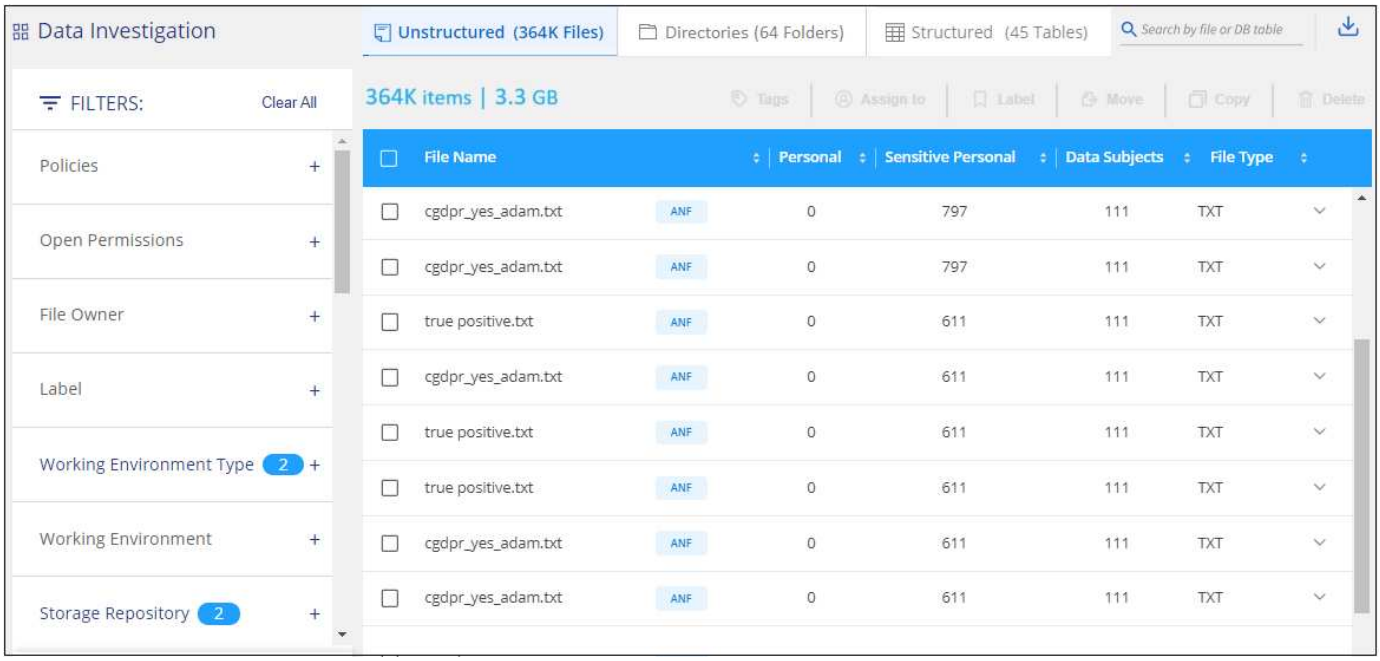
Sie können die Daten Ihres Unternehmens untersuchen, indem Sie Details auf der Seite „Datenuntersuchung“ anzeigen. Sie können diese Seite aus vielen Bereichen der BlueXP Klassifizierungs-UI aufrufen, einschließlich der Governance- und Compliance-Dashboards.

> 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.

Filtern Sie die 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. Einzelheiten zum Untersuchungsbericht zu Daten finden Sie hier.



- Auf den Registerkarten der obersten Ebene können Sie Daten aus Dateien (unstrukturierte Daten), Verzeichnissen (Ordner und Dateifreigaben) oder 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 die in den nächsten Abschnitten beschriebenen Attribute auswählen.

Filtern von Daten nach Sensitivität und Inhalt

Mithilfe der folgenden Filter können Sie anzeigen, wie viele vertrauliche Informationen in Ihren Daten enthalten sind.

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 ergibt die BlueXP Klassifizierung insgesamt die Treffer aus allen Dateien in jedem Ordner (und in Unterordnern). HINWEIS: Die Veröffentlichung von Dezember 2023 (Version 1.26.6) hat die Möglichkeit, die Anzahl der personenbezogenen Daten (PII) nach Verzeichnissen zu berechnen, vorübergehend entfernt.
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. "Weitere Informationen zu Datensubjekten finden Sie hier".

Filtern Sie Daten nach Benutzereigern und Benutzerberechtigungen

Verwenden Sie die folgenden Filter, um Dateibesitzer und Berechtigungen für den Zugriff auf Ihre Daten anzuzeigen.

Filtern	Details
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.
Anzahl der Benutzer mit Zugriff	Wählen Sie einen oder mehrere Kategoriebereiche aus, um anzuzeigen, welche Dateien und Ordner für eine bestimmte Anzahl von Benutzern geöffnet sind.

Filtern Sie Daten nach Zeit

Verwenden Sie die folgenden Filter, um Daten basierend auf den Zeitkriterien anzuzeigen.

Filtern	Details
Erstellungszeit	Wählen Sie einen Zeitbereich aus, in dem die Datei erstellt wurde. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern.
Entdeckte Zeit	Wählen Sie einen Zeitraum aus, in dem die BlueXP Klassifizierung die Datei erkannt hat. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern.
Zuletzt Geändert	Wählen Sie einen Zeitbereich aus, in dem die Datei zuletzt geändert wurde. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern.
Zuletzt Aufgerufen	Wählen Sie einen Zeitraum aus, in dem zuletzt auf die Datei oder das Verzeichnis (nur CIFS oder NFS) zugegriffen wurde. Sie können auch einen benutzerdefinierten Zeitbereich angeben, um die Suchergebnisse weiter zu verfeinern. Für die Dateitypen, die die BlueXP Klassifizierung scannt, wurde die Datei zuletzt durch die BlueXP Klassifizierung gescannt. Beachten Sie, dass die Klassifizierung durch BlueXP nicht zur Zeit des letzten Zugriffs aus den folgenden Datenquellen herangezogen wird: SharePoint Online, SharePoint On-Premises (SharePoint Server), OneDrive, Google Drive und Amazon S3.

Filtern Sie Daten nach Metadaten

Verwenden Sie die folgenden Filter, um Daten auf der Grundlage von Speicherort, Größe und Verzeichnis oder Dateityp anzuzeigen.

Filtern	Details
Dateipfad	Geben Sie bis zu 20 Teilpfade oder vollständige Pfade ein, die in die Abfrage einbezogen oder ausgeschlossen werden sollen. Wenn Sie beide Einschlusspfade eingeben und Pfade ausschließen, werden bei der BlueXP Klassifizierung zuerst alle Dateien in den eingeschlossenen Pfaden gefunden. Anschließend werden Dateien aus ausgeschlossenen Pfaden entfernt, und die Ergebnisse werden angezeigt. Beachten Sie, dass die Verwendung von "*" in diesem Filter keine Wirkung hat und dass Sie bestimmte Ordner nicht aus dem Scan ausschließen können - alle Verzeichnisse und Dateien unter einer konfigurierten Freigabe werden gescannt.
Verzeichnistyp	Wählen Sie den Verzeichnistyp aus, entweder „Share“ oder „Folder“.
Dateityp	Wählen Sie die aus "Dateitypen".
Dateigröße	Wählen Sie den Dateigrößenbereich aus.
Datei-Hash	Geben Sie den Hash der Datei ein, um eine bestimmte Datei zu finden, selbst wenn der Name anders ist.

Filtern Sie Ihre Daten nach Storage-Typ

Verwenden Sie die folgenden Filter, um Daten nach Speichertyp anzuzeigen.

Filtern	Details
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.

Filtern Sie Daten nach Tags, Labels, zugewiesenen Benutzern und Richtlinien

Verwenden Sie die folgenden Filter, um Daten nach AIP-Etiketten oder -Tags anzuzeigen.

Filtern	Details
Richtlinien	Wählen Sie eine Richtlinie oder Richtlinien aus. Los "Hier" Um die Liste der vorhandenen Richtlinien anzuzeigen und eigene Richtlinien zu erstellen.
Etikett	Wählen Sie "AIP-Etiketten" Die Ihren Dateien zugewiesen sind.
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.

Filtern Sie Daten nach Analysestatus

Verwenden Sie den folgenden Filter, um Daten nach dem BlueXP Klassifizierungs-Scan-Status anzuzeigen.

Filtern	Details
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.
Analyseereignis Scannen	Wählen Sie aus, ob Dateien angezeigt werden sollen, die nicht klassifiziert wurden, weil die BlueXP-Klassifizierung die Uhrzeit des letzten Zugriffs nicht rückgängig machen konnte, oder Dateien, die klassifiziert wurden, obwohl die BlueXP-Klassifizierung die Zeit des letzten Zugriffs nicht rückgängig machen konnte.

"Weitere Informationen zum Zeitstempel des letzten Zugriffs" Weitere Informationen zu den Elementen, die beim Filtern mit dem Ereignis Scananalyse auf der Seite Untersuchung angezeigt werden.

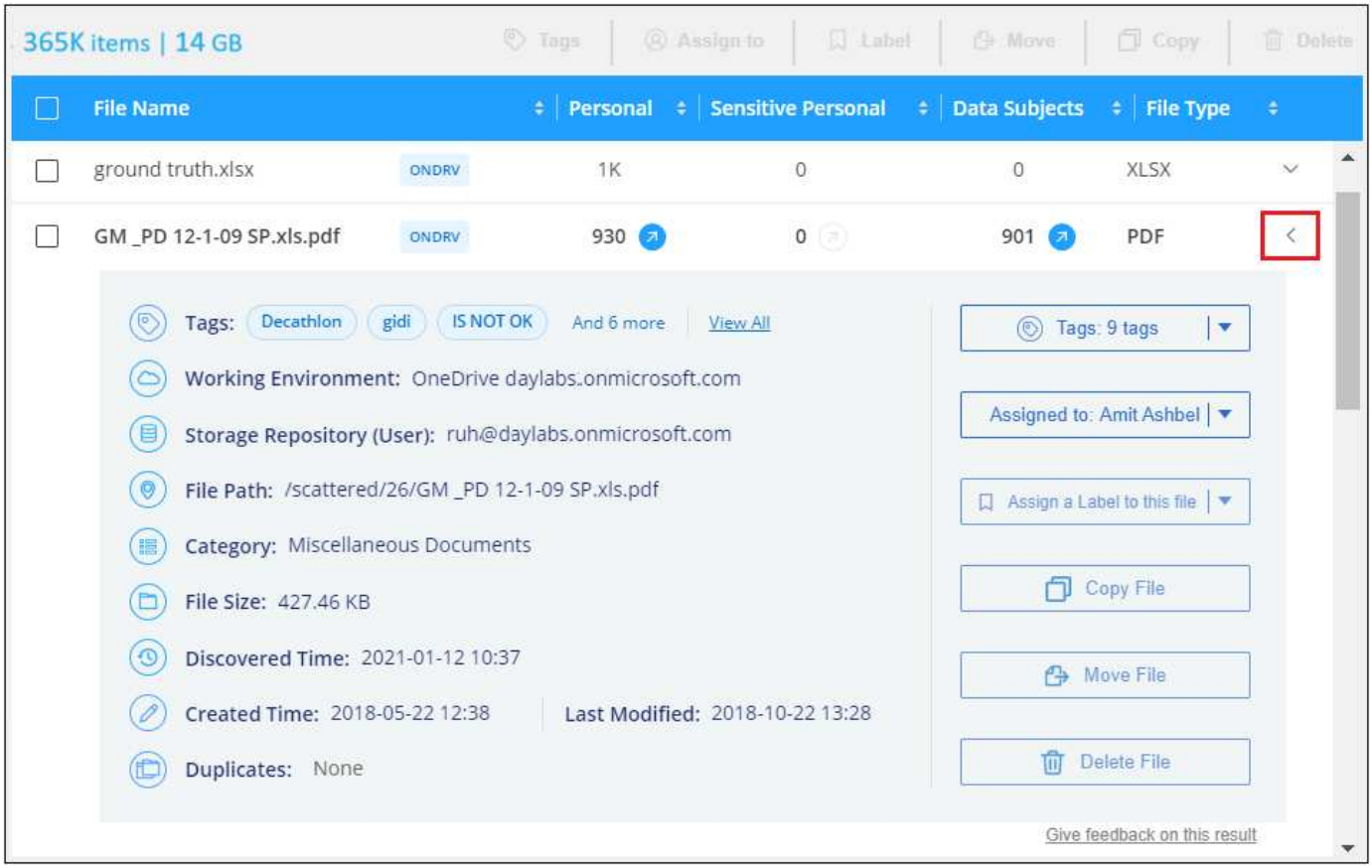
Daten nach Duplikaten filtern

Verwenden Sie den folgenden Filter, um Dateien anzuzeigen, die im Speicher dupliziert wurden.

Filtern	Details
Duplikate	Wählen Sie aus, ob die Datei in den Repositorys dupliziert wird.

Anzeigen von Datei-Metadaten

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 BlueXP Klassifizierung"). 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"

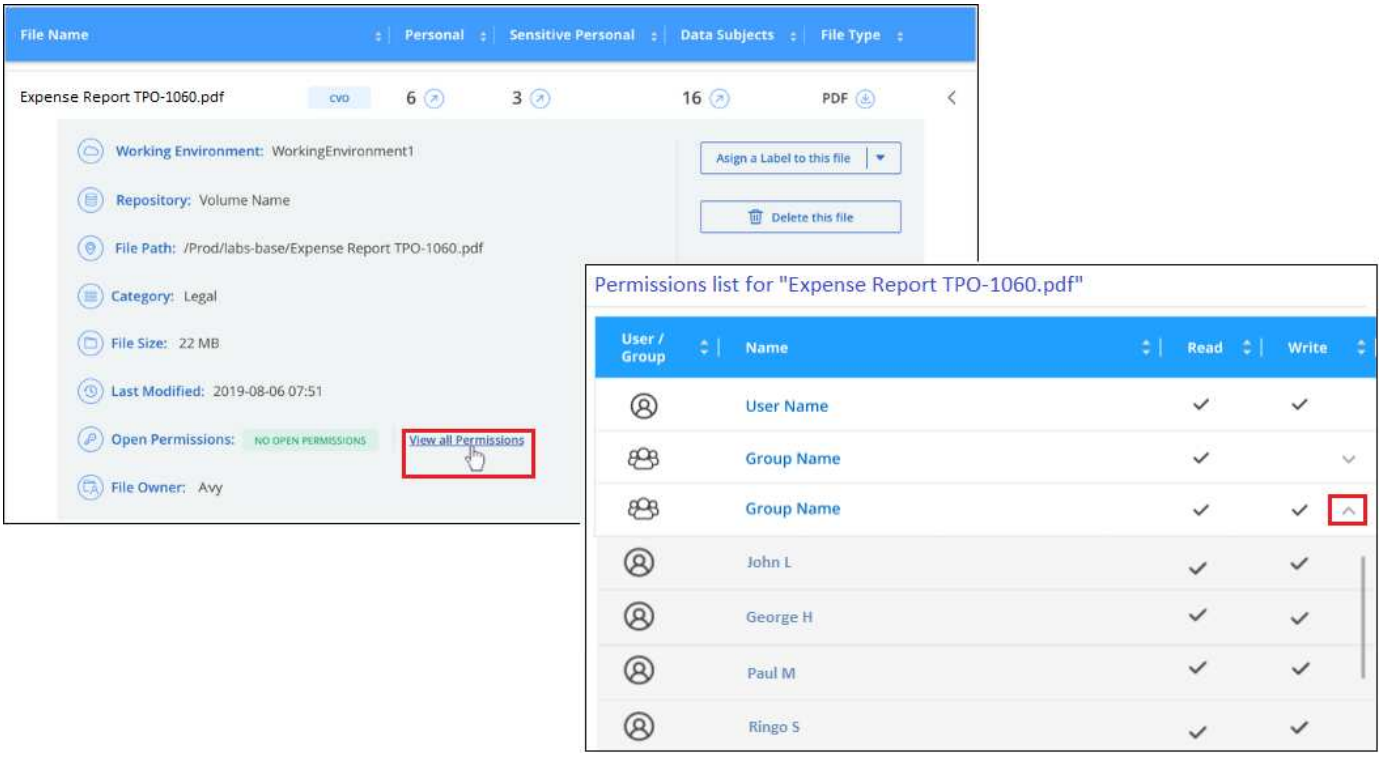
Entsprechende Details.

- Wenn Sie AIP-Labels mit der BlueXP-Klassifizierung integriert haben, können Sie dieser Datei eine Bezeichnung zuweisen oder, sofern vorhanden, zu einer anderen Bezeichnung wechseln. Siehe "Manuelles Zuweisen von AIP-Beschriftungen" Entsprechende Details.

Berechtigungen für Dateien und Verzeichnisse anzeigen

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.

Wenn Sie SIDs (Security Identifiers) anstelle von Benutzer- und Gruppennamen sehen, sollten Sie Ihr Active Directory in die BlueXP Klassifizierung integrieren. "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.

Überprüfen Sie auf doppelte Dateien in Ihren Speichersystemen

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.

Alle Ihre Dateien (ohne Datenbanken), die 1 MB oder größer sind und persönliche oder sensible personenbezogene Daten enthalten, werden verglichen, um zu sehen, ob es Duplikate gibt. Sie können die Filter auf der Untersuchungsseite „Dateigröße“ zusammen mit „Duplikate“ verwenden, um zu sehen, welche

Dateien eines bestimmten Größenbereichs in Ihrer Umgebung dupliziert werden.

Die BlueXP Klassifizierung verwendet Hashing-Technologie, um doppelte Dateien zu ermitteln. 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.

Alle duplizierten Dateien anzeigen

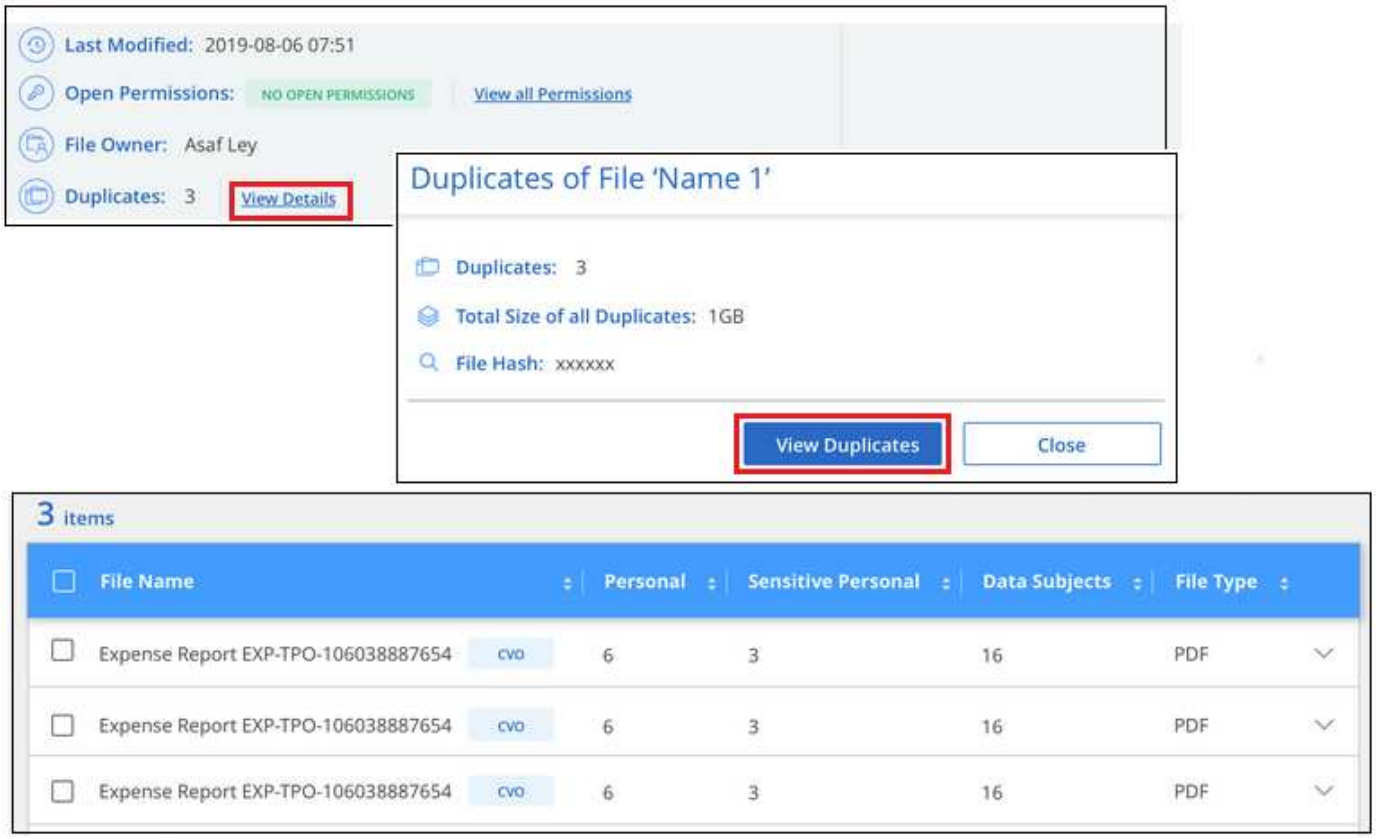
Wenn Sie eine Liste aller Dateien wünschen, die in den Arbeitsumgebungen und Datenquellen, die Sie scannen, dupliziert werden, können Sie den Filter **Duplicates > has Dubletten** auf der Seite Data Investigation verwenden.

Alle duplizierten Dateien werden auf der Ergebnisseite angezeigt.

Anzeigen, ob eine bestimmte Datei dupliziert wurde

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.

Bericht Zur Datenuntersuchung

Der Untersuchungsbericht ist ein Download des gefilterten Inhalts der Seite Datenuntersuchung.

Der Bericht ist in zwei verschiedenen Formaten verfügbar:

- Als CSV-Datei, die Sie auf dem lokalen Computer speichern können.

  Dieser Bericht kann maximal 10,000 Datenzeilen enthalten.

- Als JSON-Datei, die Sie in eine NFS-Freigabe exportieren.

  Wenn mehr als 250,000 Datenzeilen vorhanden sind, werden zusätzliche JSON-Dateien erstellt.

  Stellen Sie beim Exportieren in eine Dateifreigabe sicher, dass die BlueXP Klassifizierung die richtigen Berechtigungen für den Exportzugriff hat.

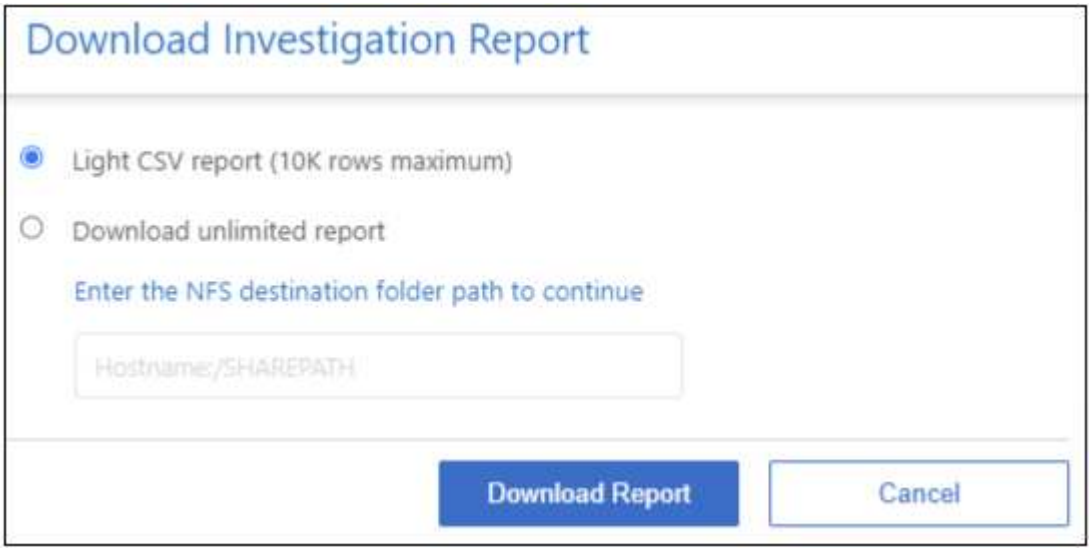
Es können bis zu drei Berichtsdateien heruntergeladen werden, wenn die BlueXP Klassifizierung Dateien (unstrukturierte Daten), Verzeichnisse (Ordner und Dateifreigaben) und Datenbanken (strukturierte Daten) scannt.

Generieren Sie den Bericht zur Datenermittlung

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 den einzelnen Datenuntersuchungs-Berichten enthalten

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

- Dateiname
- Positionstyp
- Name der Arbeitsumgebung
- Storage-Repository (z. B. Volume, Bucket, Shares)
- Repository-Typ
- Dateipfad
- Dateityp
- Dateigröße (in MB)
- Erstellungszeit
- Zuletzt geändert
- Zuletzt aufgerufen
- Dateibesitzer
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten
- Berechtigungen öffnen
- Fehler Bei Der Scananalyse
- 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:

- Art der Arbeitsumgebung
- Name der Arbeitsumgebung
- Verzeichnisname
- Storage-Repository (beispielsweise ein Ordner oder Dateifreigaben)
- Verzeichniseigentümer
- 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

Private Daten organisieren

Die BlueXP Klassifizierung bietet Ihnen zahlreiche Möglichkeiten zum Managen und Organisieren Ihrer privaten Daten. Auf diese Weise können Sie die für Sie wichtigsten Daten besser einsehen.

- Wenn Sie abonniert sind "Azure Information Protection (AIP)" Um Ihre Dateien zu klassifizieren und zu schützen, können Sie diese AIP-Labels mit der BlueXP Klassifizierung managen.

  Mit der Veröffentlichung im Dezember 2023 (v1.26.6) wurde die Option zur Integration von Daten mit Azure Information Protection (AIP)-Labels vorübergehend aufgehoben.

- 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 E-Mail-Benachrichtigungen an BlueXP-Benutzer oder andere E-Mail-Adressen 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?

Unten finden Sie einen Vergleich zwischen BlueXP Klassifizierungs-Tagging und Azure Information Protection Labelling.

Tags	Etiketten
Datei-Tags sind ein integrierter Teil der BlueXP Klassifizierung.	Voraussetzung ist, dass Sie den Azure Information Protection (AIP) abonniert haben.
Das Tag wird nur in der BlueXP Klassifizierungs-Datenbank aufbewahrt - 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 BlueXP-Klassifizierungsaktionen wie 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 managen, die die BlueXP Klassifizierung 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 der BlueXP Klassifizierung können Sie die Labels anzeigen, die bereits Dateien zugewiesen sind, Labels zu Dateien hinzufügen und Labels ändern, wenn bereits eine Labels vorhanden sind.

Die BlueXP Klassifizierung unterstützt AIP-Labels innerhalb der 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, betrachtet die BlueXP Klassifizierung dieses Label als Datei ohne Label.
- Wenn Sie die BlueXP Klassifizierung in einer Regierungsregion oder an einem lokalen Standort ohne Internetzugang (auch als Dark Site bezeichnet) implementiert haben, ist die AIP-Label-Funktion nicht verfügbar.

Integrieren Sie AIP-Beschriftungen in Ihren Arbeitsbereich

Bevor Sie AIP-Labels managen können, müssen Sie die AIP-Label-Funktionalität in die BlueXP Klassifizierung integrieren, indem Sie sich in Ihr bestehendes Azure Konto anmelden. Nach der Aktivierung können Sie AIP-Beschriftungen in Dateien für alle verwalten "Datenquellen" In Ihrem BlueXP Workspace.

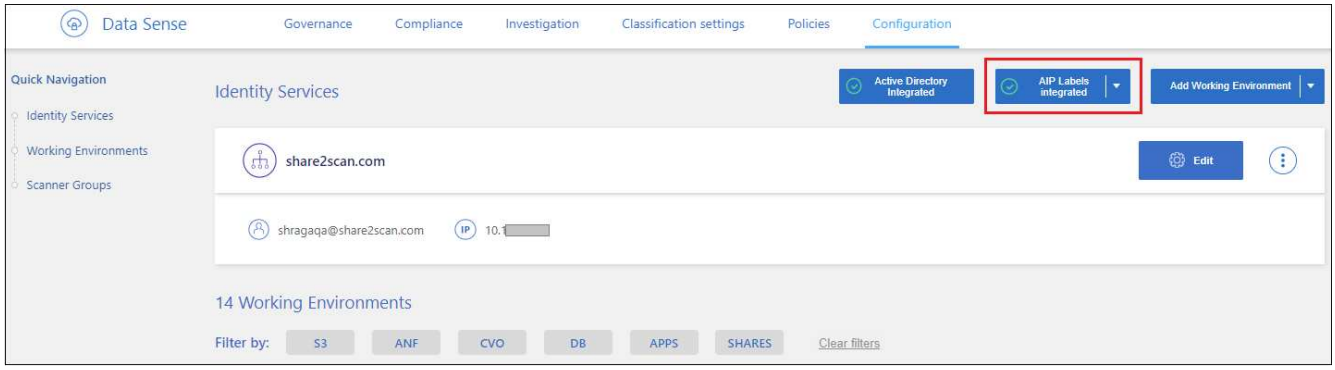
Anforderungen

- 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 BlueXP classification Configuration auf **Integration AIP Labels**.

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 BlueXP Klassifizierung zurück und Sie sehen die Meldung "*AIP-Labels was successfully integrated with the Account <account_name>*".
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.

AIP-Etiketten in Ihren Dateien anzeigen

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.

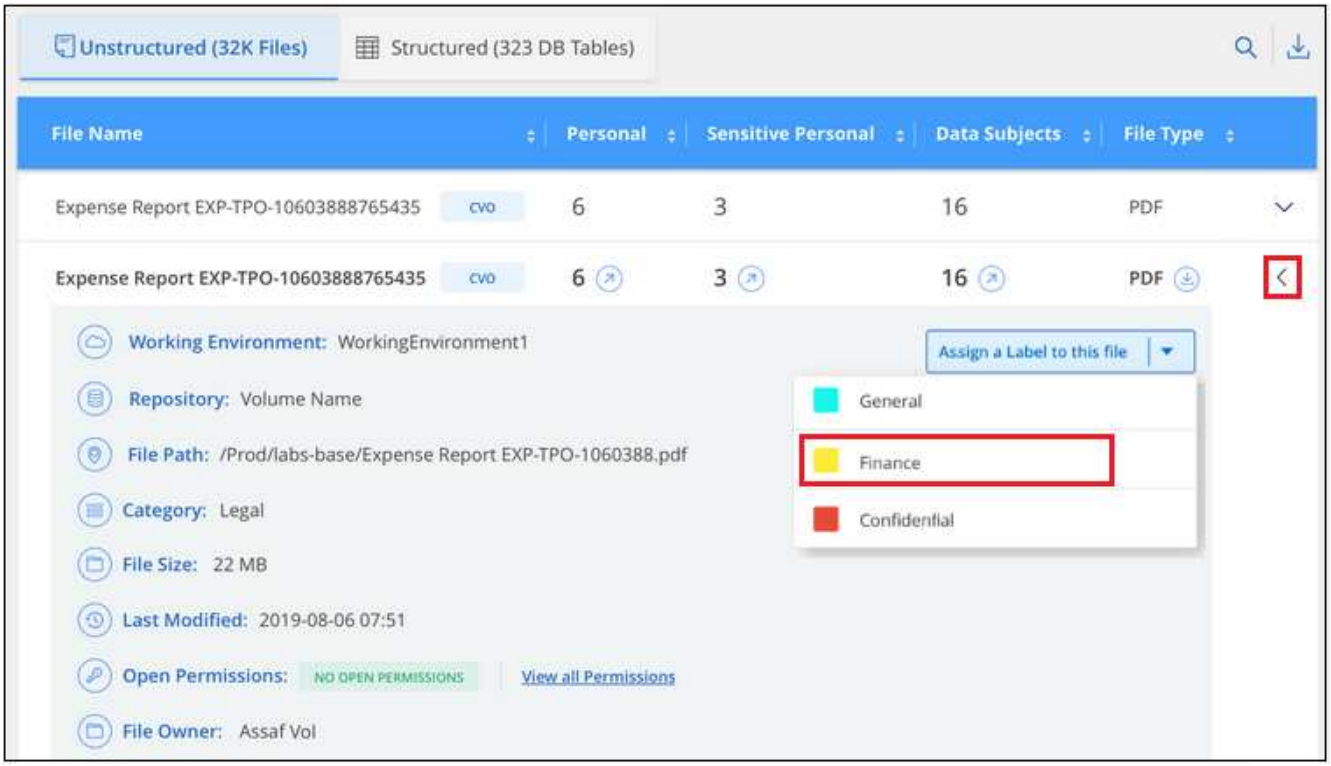
Weisen Sie AIP-Beschriftungen manuell zu

Mit der BlueXP Klassifizierung können Sie AIP-Labels zu 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.

Führen Sie die folgenden Schritte aus, um mehreren Dateien eine AIP-Bezeichnung zuzuweisen. Beachten Sie, dass Sie maximal 20 Dateien gleichzeitig (eine Seite in der Benutzeroberfläche) eine AIP-Bezeichnung zuweisen können.

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.

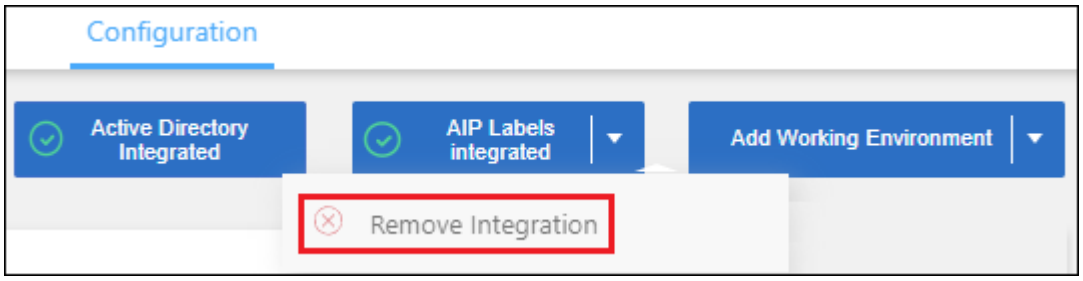
Entfernen Sie die AIP-Integration

Wenn Sie AIP-Labels in Dateien nicht mehr verwalten möchten, können Sie das AIP-Konto von der BlueXP Klassifizierungs-Schnittstelle entfernen.

Beachten Sie, dass an den Labels, die Sie mit der BlueXP Klassifizierung hinzugefügt haben, keine Änderungen vorgenommen 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**.

Wenden Sie Tags an, um die gescannten Dateien zu verwalten

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 der BlueXP Klassifizierung können Sie die Tags anzeigen, die Dateien zugewiesen sind, Tags aus Dateien hinzufügen oder entfernen sowie den Namen ändern oder ein vorhandenes Tag löschen.

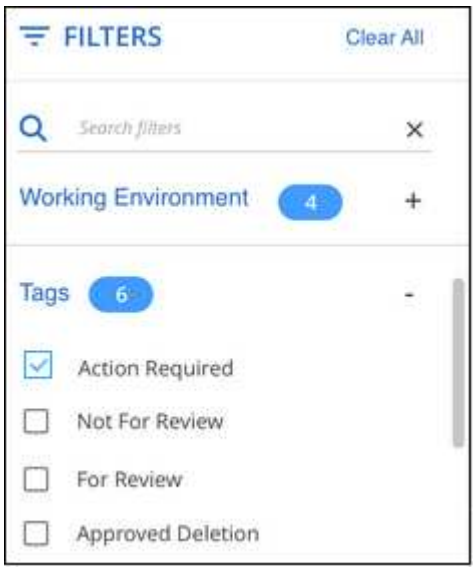
Beachten Sie, dass das Tag der Datei nicht auf die gleiche Weise hinzugefügt wird wie AIP-Etiketten Teil der Dateimetadaten sind. Das Tag wird gerade von BlueXP Benutzern angezeigt, die die BlueXP Klassifizierung verwenden. Sie können also erkennen, ob eine Datei gelöscht oder auf eine bestimmte Art von Follow-up überprüft werden muss.

> Die Tags, die Dateien in der BlueXP Klassifizierung zugewiesen sind, stehen nicht mit den Tags zusammen, die Sie zu Ressourcen wie Volumes oder Instanzen von Virtual Machines hinzufügen können. BlueXP Klassifizierungs-Tags werden auf Dateiebene angewendet.

Zeigen Sie Dateien an, auf die bestimmte Tags angewendet wurden

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

1. Klicken Sie in der BlueXP-Klassifizierung auf die Registerkarte **Investigation**.
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.

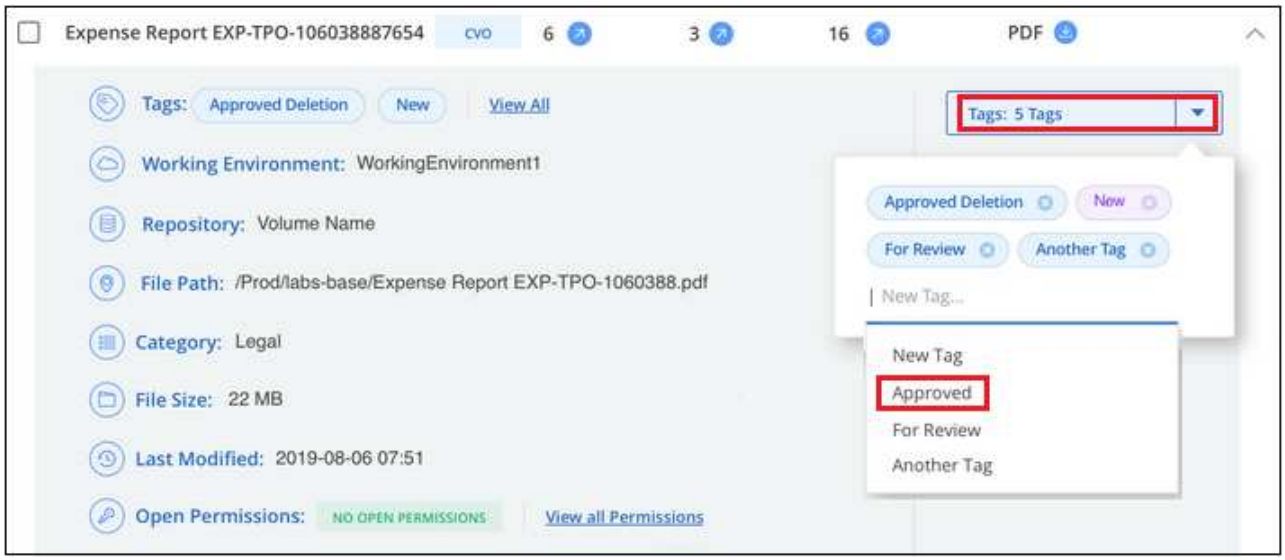
Weisen Sie Dateien Tags zu

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.

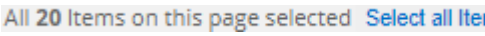
So fügen Sie einem mehrere Dateien ein Tag hinzu:

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).

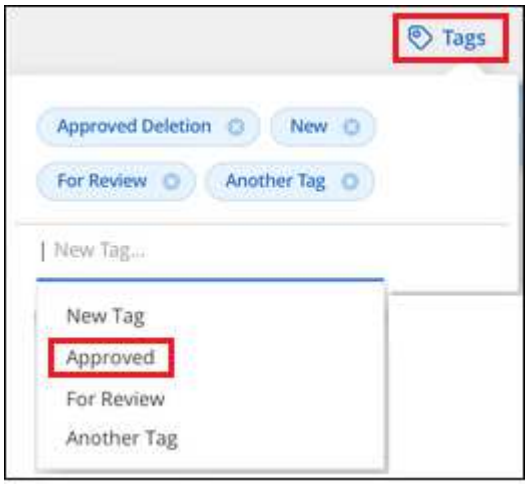
- Um alle Dateien auf allen Seiten auszuwählen, aktivieren Sie das Kontrollkästchen in der Titelzeile (

), und dann in der Pop-up-Nachricht 

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

  Sie können Tags auf maximal 100,000 Dateien gleichzeitig anwenden.

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 löschen

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.

Weisen Sie Benutzer zu, um bestimmte Dateien zu verwalten

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.

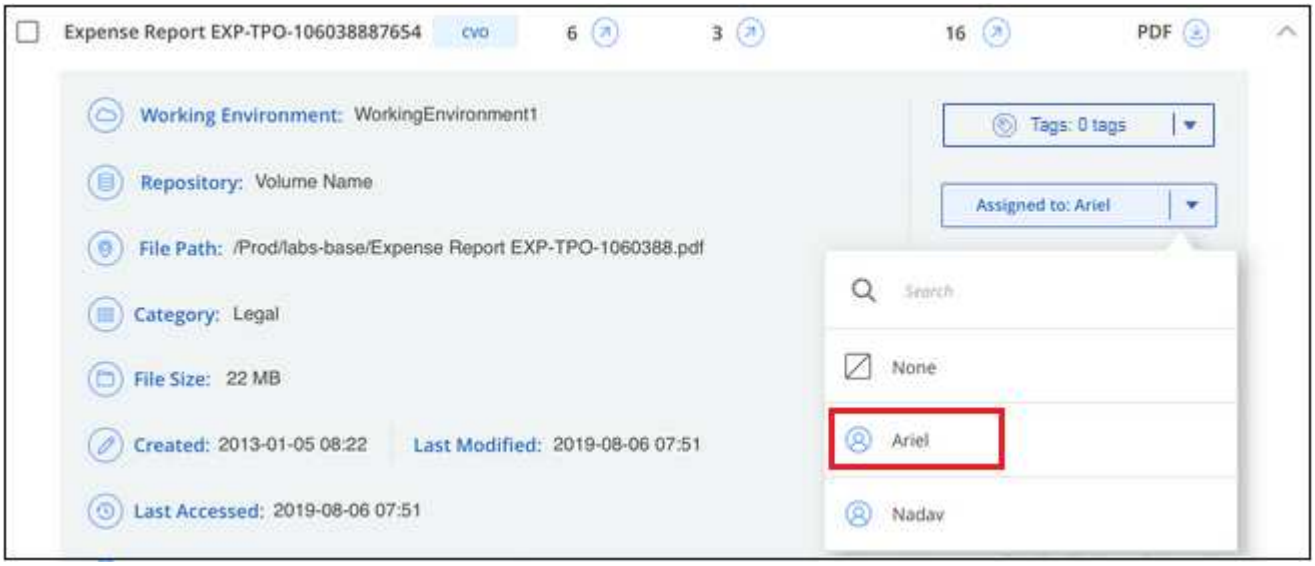
Beachten Sie, dass der Benutzername nicht als Teil der Datei-Metadaten zur Datei hinzugefügt wird. Er wird gerade von BlueXP Benutzern bei der Nutzung der BlueXP Klassifizierung gesehen.

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

Führen Sie die folgenden Schritte aus, um einen Benutzer einer einzelnen Datei zuzuweisen.

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.

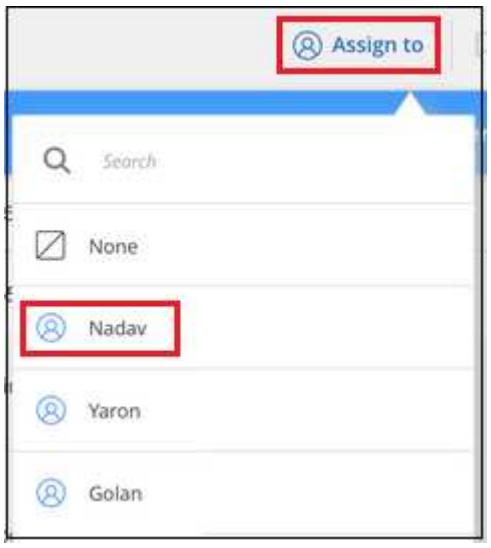
Führen Sie diese Schritte aus, um einen Benutzer mehreren Dateien zuzuweisen. Beachten Sie, dass Sie einen Benutzer maximal 20 Dateien gleichzeitig zuweisen können (eine Seite in der Benutzeroberfläche).

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.

Weisen Sie Daten Richtlinien zu

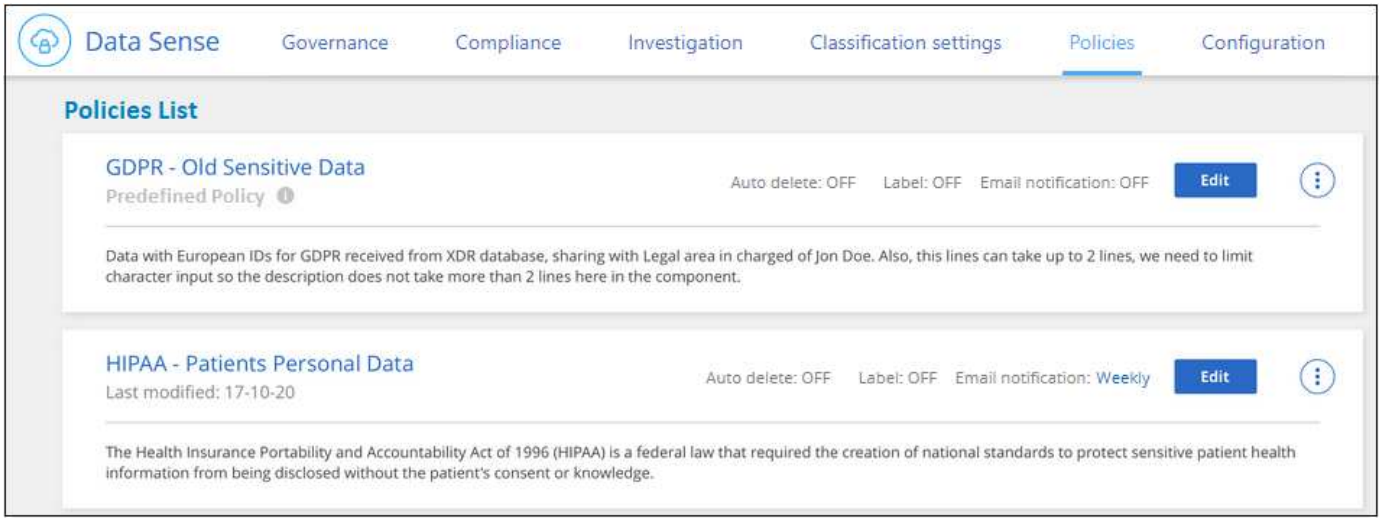
Richtlinien sind wie eine Favoritenliste mit benutzerdefinierten Filtern, die Suchergebnisse auf der Untersuchungsseite für häufig angeforderte Compliance-Abfragen liefern. Die BlueXP Klassifizierung bietet einen Satz vordefinierter Richtlinien auf der Basis allgemeiner Kundenanfragen. Sie können benutzerdefinierte 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 oder andere E-Mail-Adressen, wenn bestimmte kritische Richtlinien Ergebnisse liefern, 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

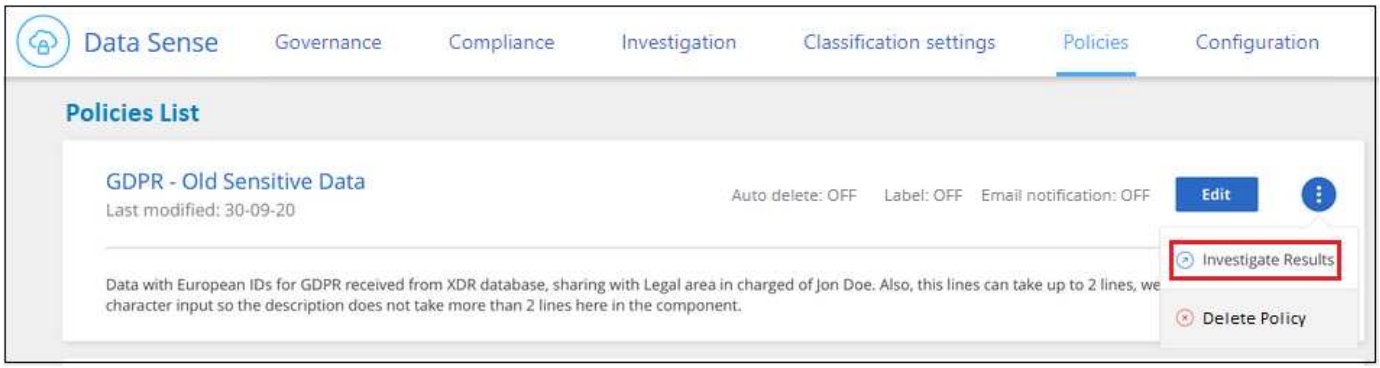
Auf der Registerkarte **Policies** im Compliance Dashboard werden alle vordefinierten und benutzerdefinierten Richtlinien aufgelistet, die auf dieser Instanz der BlueXP-Klassifizierung verfügbar sind.



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

Zeigen Sie die Ergebnisse der Richtlinie auf der Seite Untersuchung an

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**.



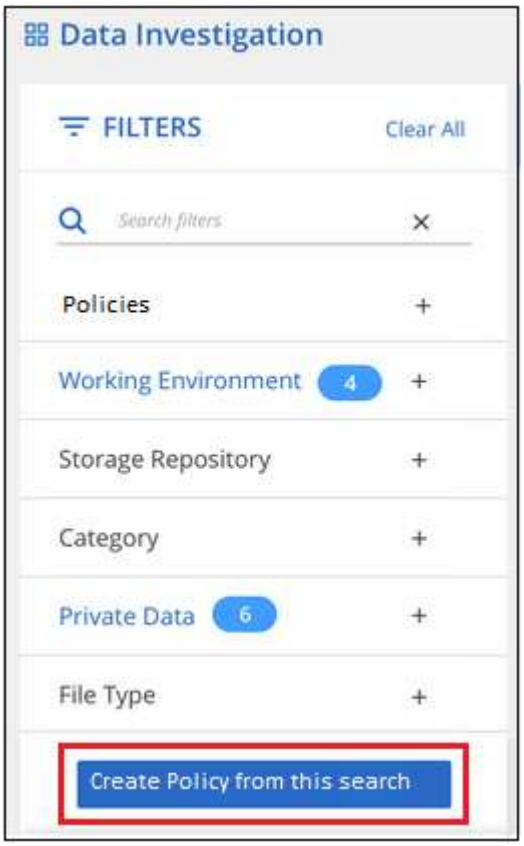
Erstellen Sie benutzerdefinierte Richtlinien

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.

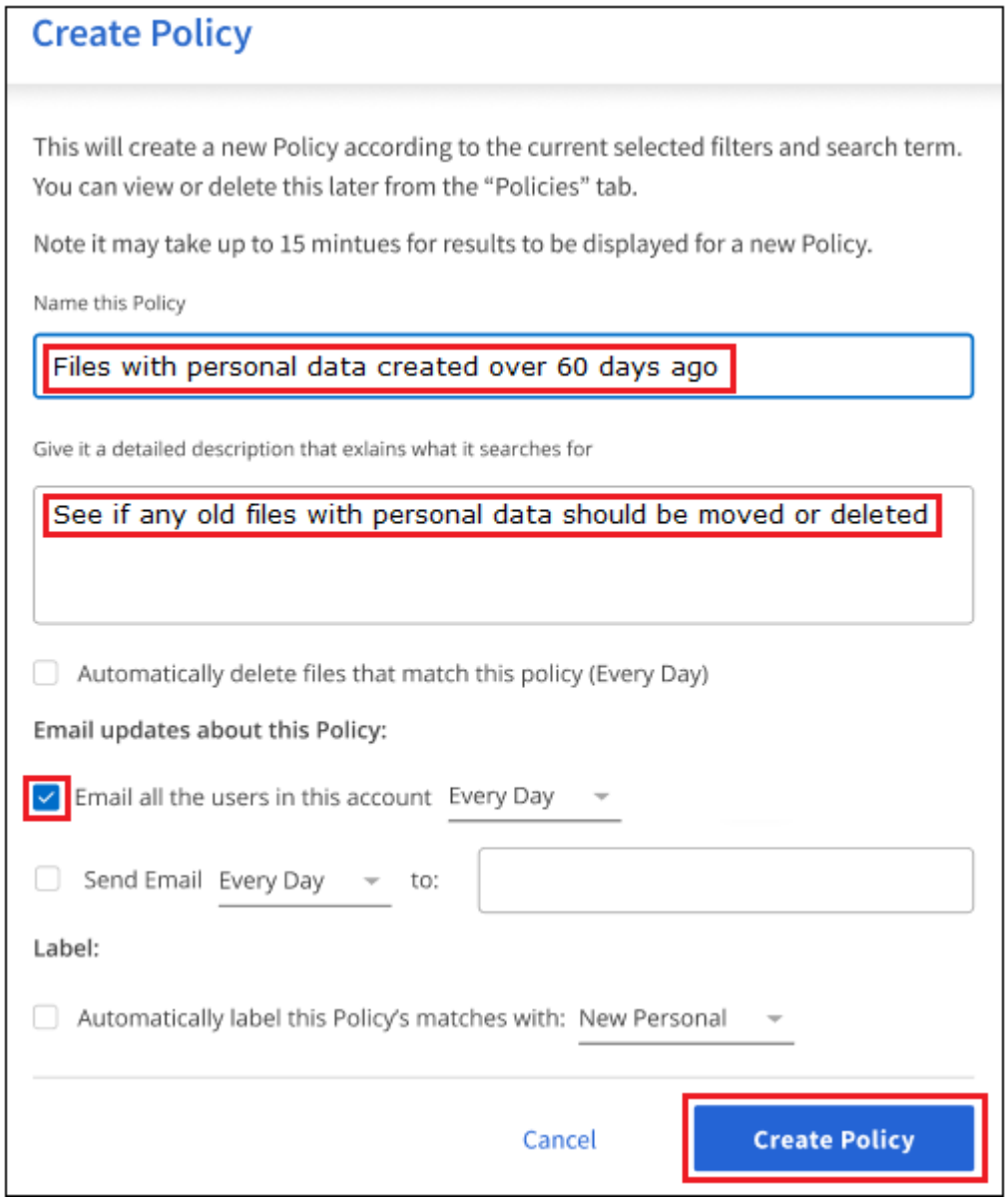
Schritte

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 Sie Benachrichtigungen-E-Mails an BlueXP-Benutzer in Ihrem Konto senden möchten, und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird. Weitere Informationen zu wenn nicht konforme Daten gefunden werden,Senden von E-Mail-Warnmeldungen anhand von Richtlinienergebnissen.
   d. Aktivieren Sie optional das Kontrollkästchen, wenn Sie Benachrichtigungs-E-Mails an andere Benutzer senden möchten, geben Sie bis zu 20 E-Mail-Adressen ein und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird.
   e. 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".)

f. Klicken Sie Auf **Create Policy**.



Ergebnis

Die neue Richtlinie wird auf der Registerkarte Richtlinien angezeigt.

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

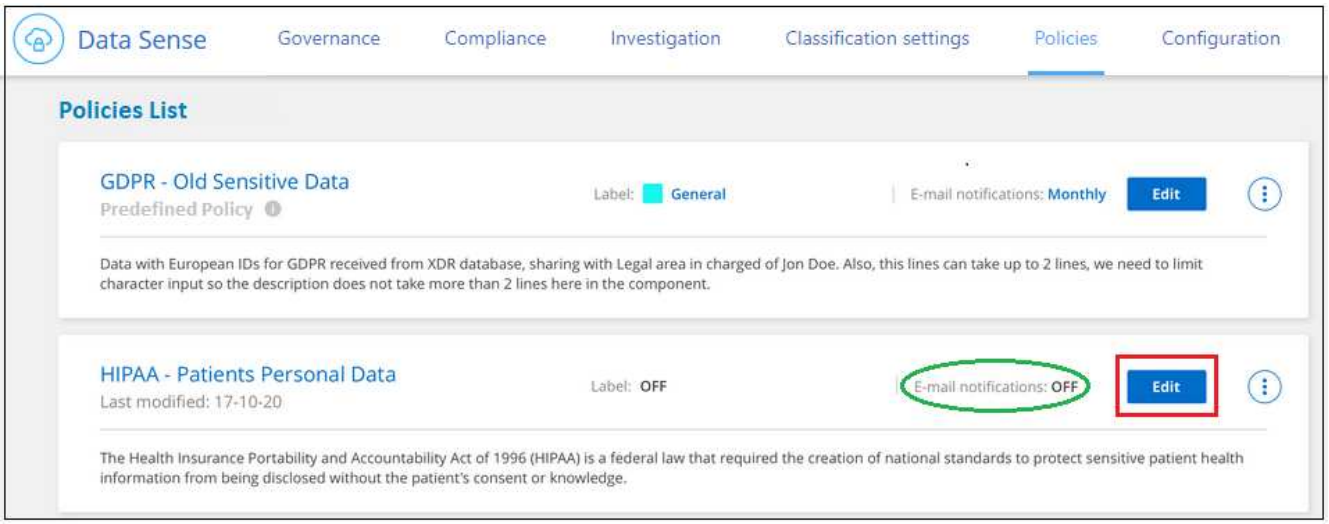
Die BlueXP Klassifizierung kann E-Mail-Benachrichtigungen an BlueXP Benutzer in Ihrem Konto senden, wenn bestimmte kritische Richtlinien Ergebnisse liefern, sodass Sie Benachrichtigungen zum Schutz Ihrer Daten erhalten. Sie können die E-Mail-Benachrichtigungen täglich, wöchentlich oder monatlich versenden. Sie können auch E-Mail-Benachrichtigungen an eine andere E-Mail-Adresse senden - bis zu 20 E-Mail-Adressen - nicht in Ihrem BlueXP-Konto.

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

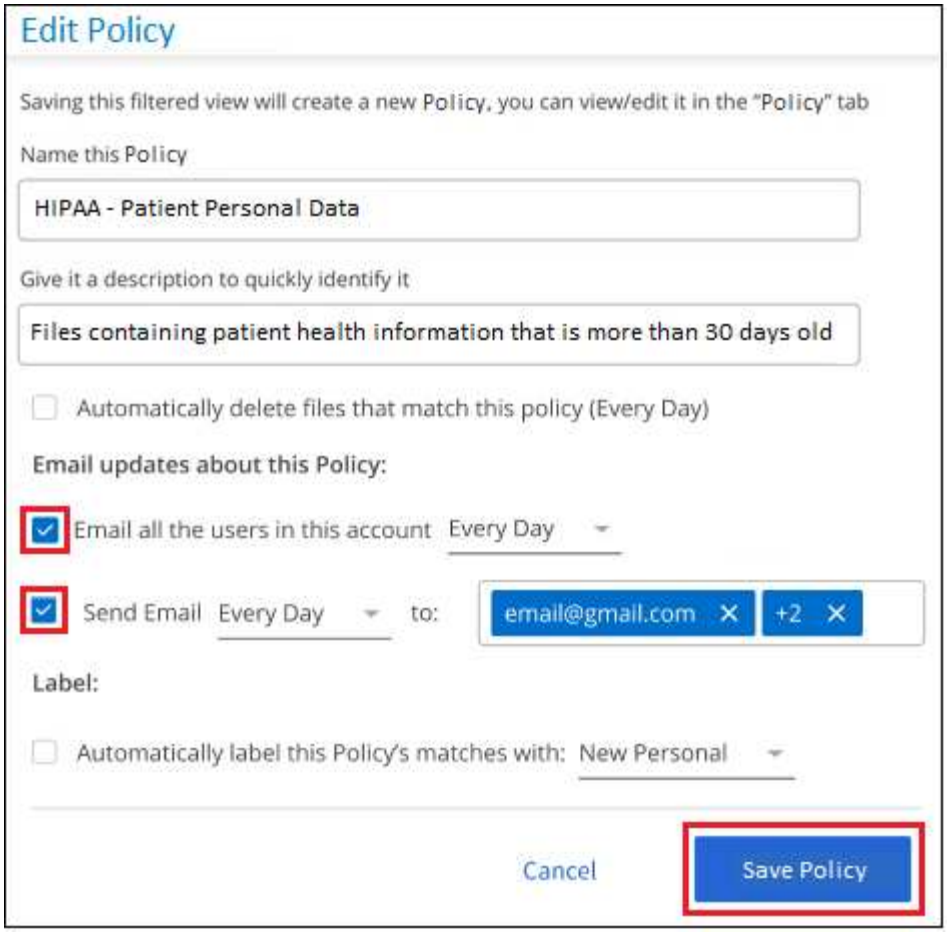
Befolgen Sie diese Schritte, um E-Mail-Updates zu einer bestehenden Richtlinie hinzuzufügen.

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. Auf der Seite Richtlinie bearbeiten:
   a. Aktivieren Sie das Kontrollkästchen „E-Mail all the users in this Account“, wenn Sie Benachrichtigungen-E-Mails an Benutzer in Ihrem BlueXP-Konto senden möchten, und wählen Sie das Intervall aus, in dem die E-Mail gesendet wird (z. B. **every Day**).
   b. Aktivieren Sie das Kontrollkästchen „E-Mail senden“, wenn Sie Benachrichtigungs-E-Mails an weitere Benutzer senden möchten, wählen Sie das Intervall aus, in dem die E-Mail gesendet wird, und geben Sie bis zu 20 E-Mail-Adressen ein.



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.

Löschen Sie Quelldateien automatisch mithilfe von Richtlinien

Sie können eine benutzerdefinierte Richtlinie erstellen, um Dateien zu löschen, die der Richtlinie entsprechen. Beispielsweise können Sie Dateien löschen, die sensible Informationen enthalten und von der BlueXP Klassifizierung in den letzten 30 Tagen erkannt wurden.

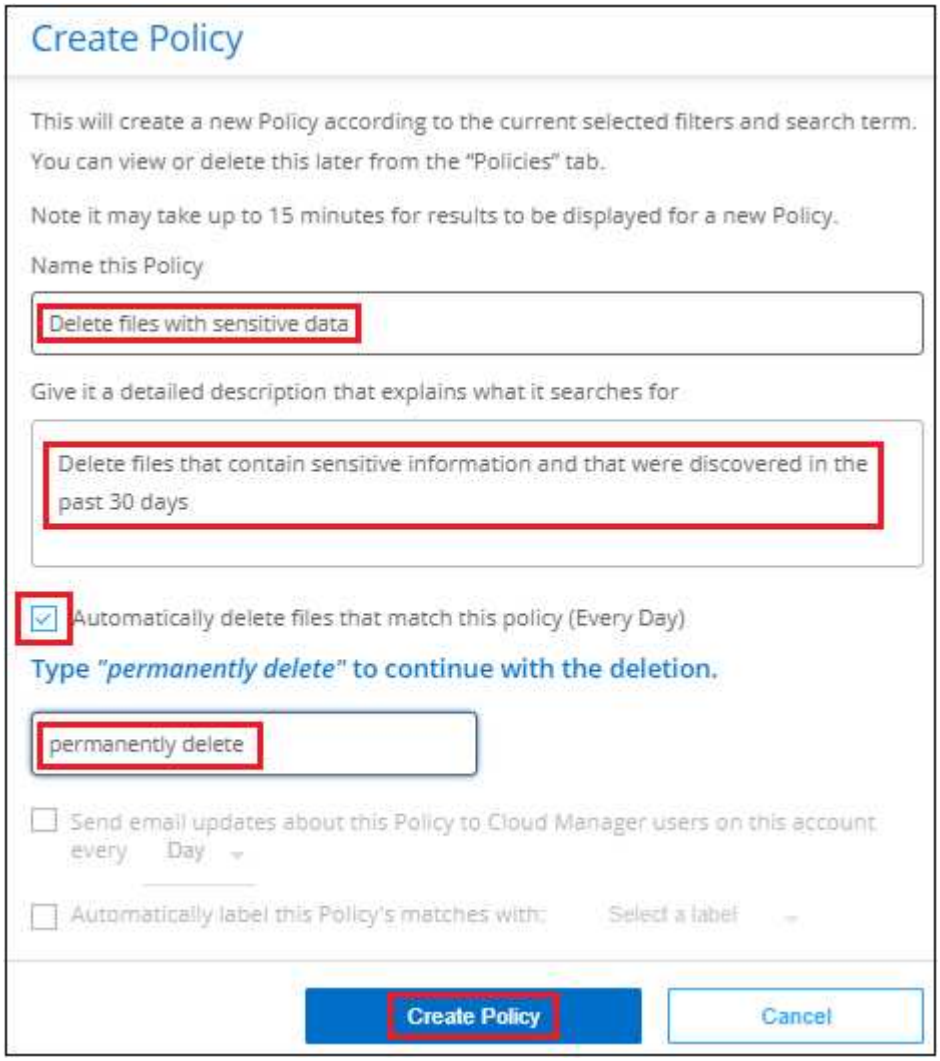
Nur Kontoadministratoren können eine Richtlinie zum automatischen Löschen von Dateien erstellen.

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".

Weisen Sie AIP-Etiketten automatisch mit Richtlinien zu

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.

Während die BlueXP Klassifizierung Ihre Dateien scannt, werden Labels fortlaufend in Dateien hinzugefügt oder aktualisiert.

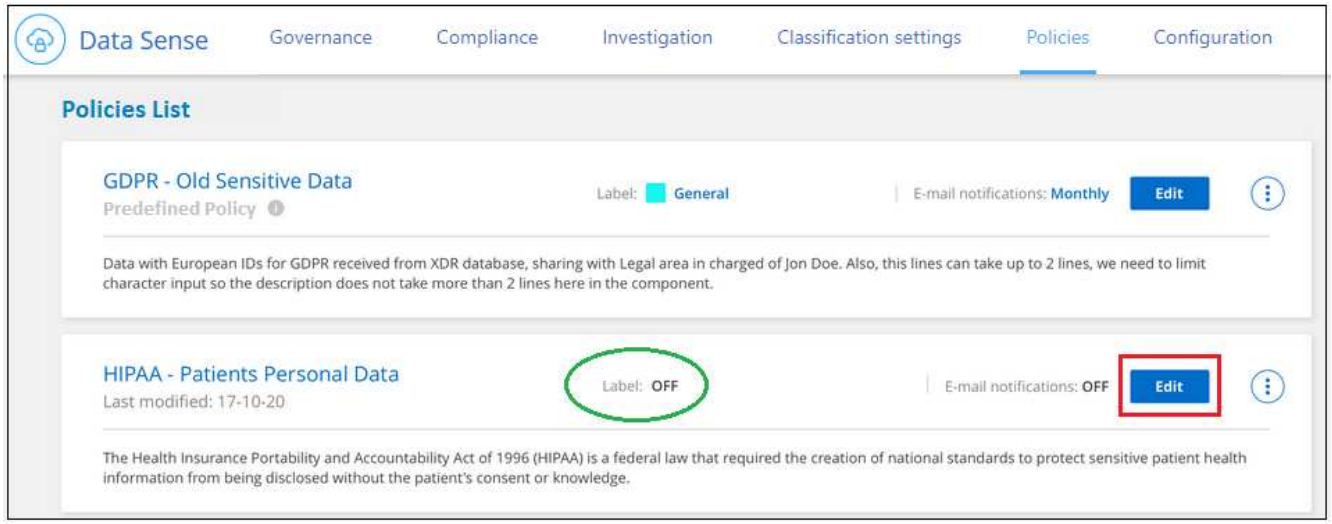
Je nachdem, ob bereits ein Label auf eine Datei und die Klassifizierungsstufe des Etiketts angewendet wurde, werden beim Ändern einer Bezeichnung folgende Aktionen ausgeführt:

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

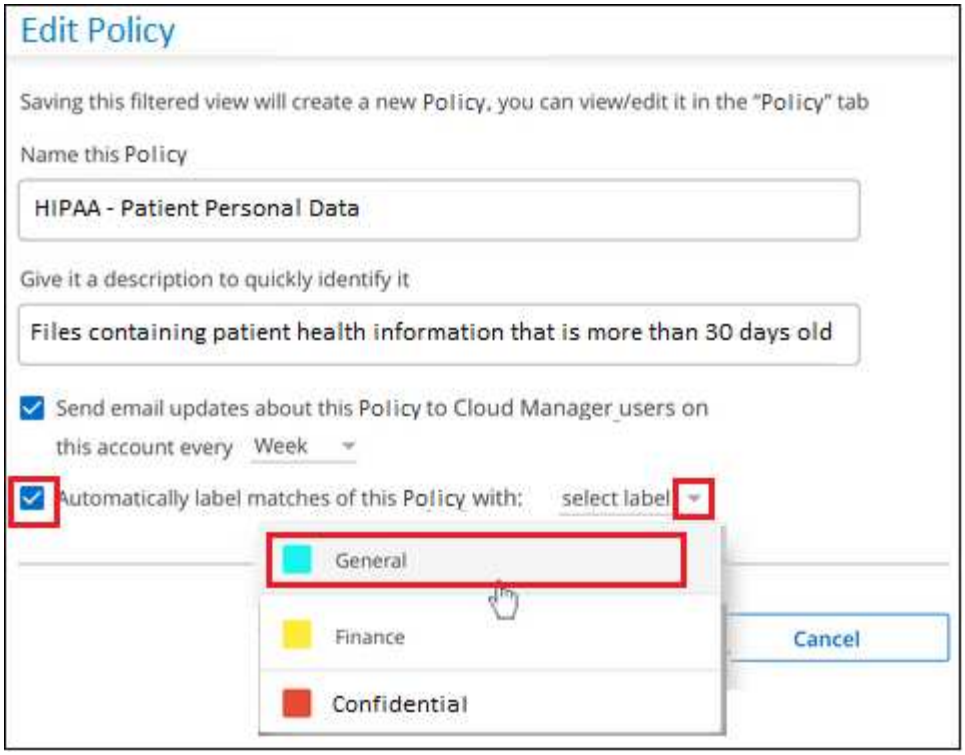
Führen Sie diese Schritte aus, um einer vorhandenen Richtlinie eine AIP-Beschriftung hinzuzufügen.

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.

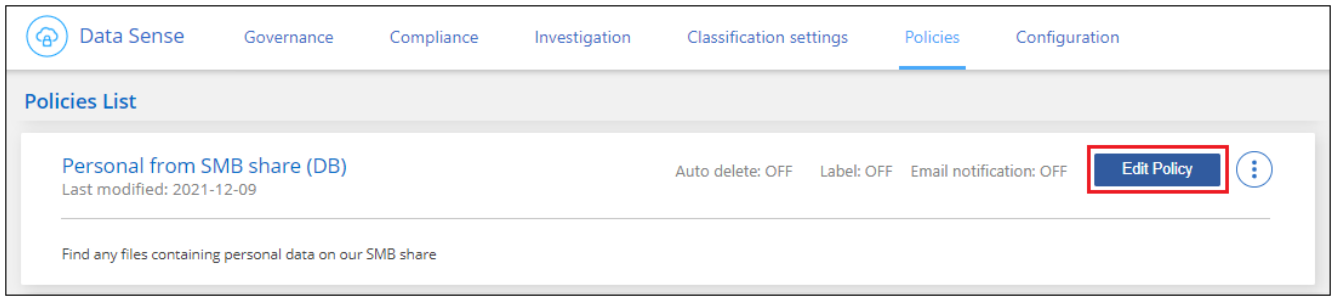
Richtlinien Bearbeiten

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

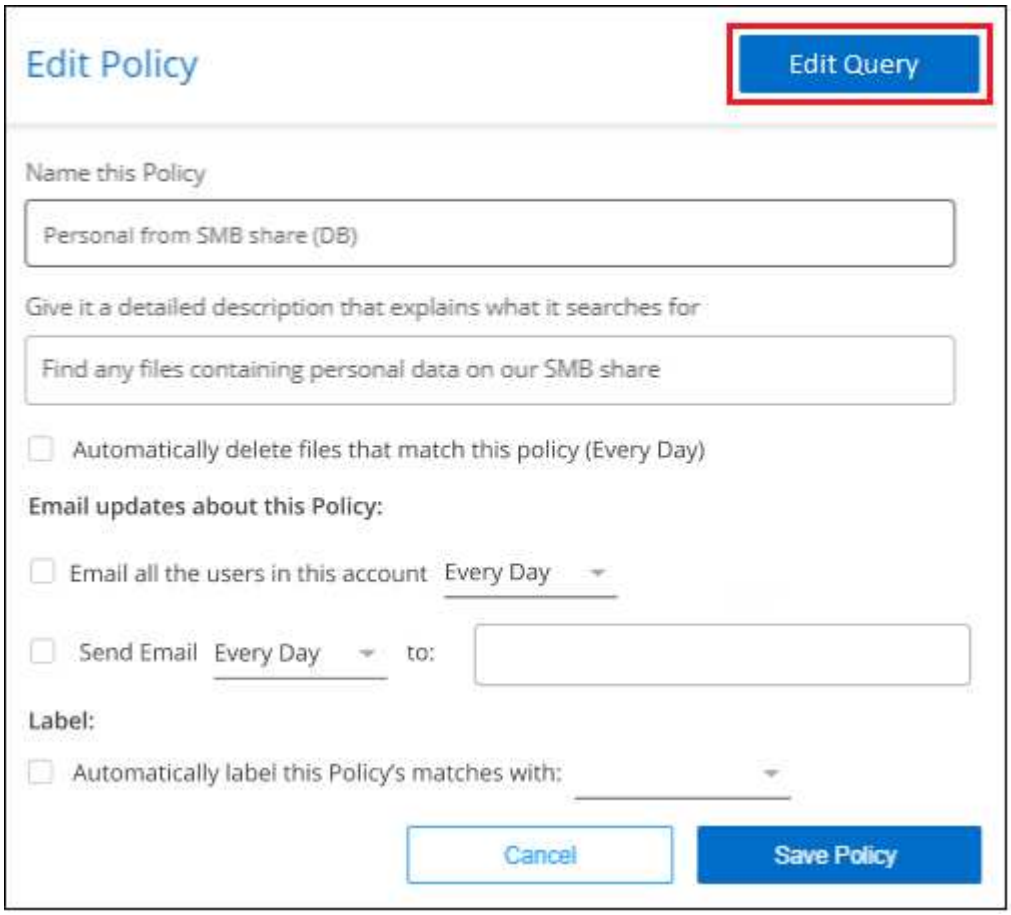
1. Klicken Sie auf der Liste Richtlinien auf **Bearbeiten** für die Richtlinie, die Sie ändern möchten.



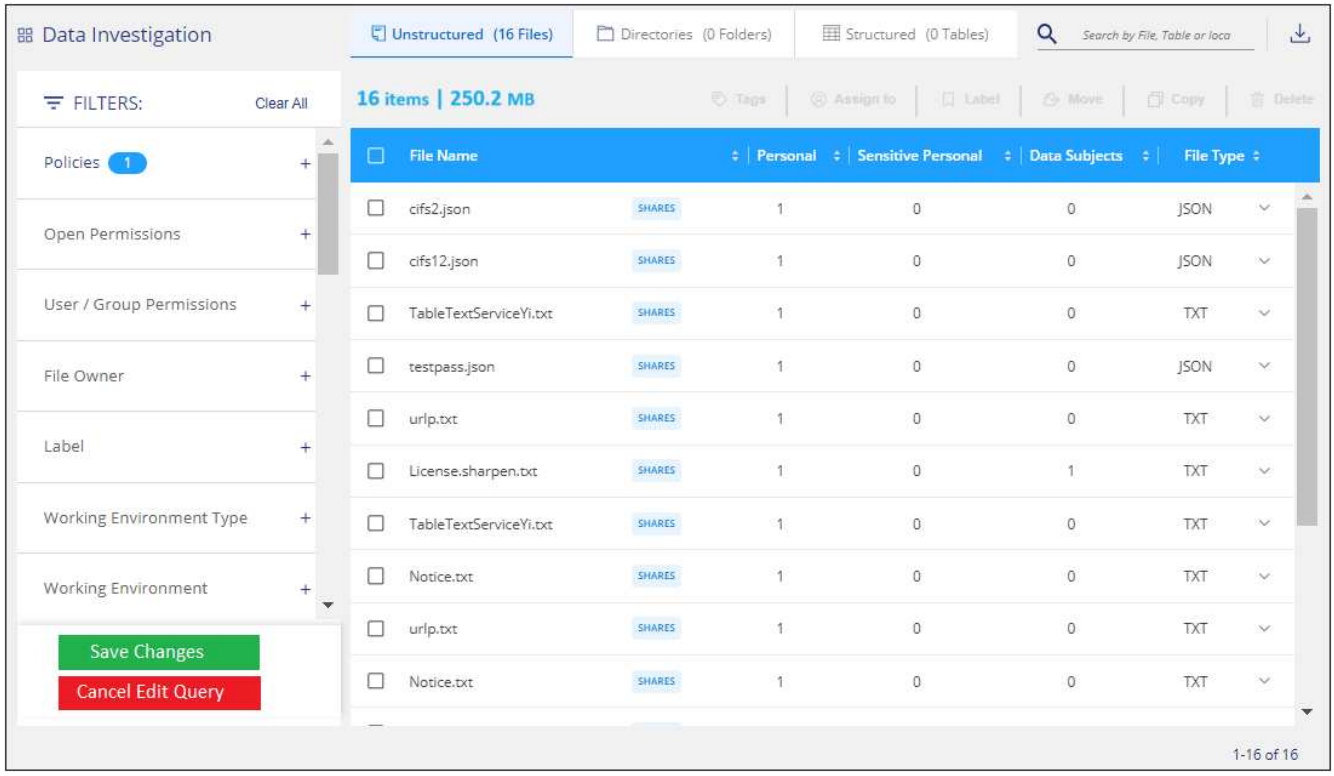
2. Wenn Sie nur die Elemente auf dieser Seite ändern möchten (Name, Beschreibung, ob E-Mail-Benachrichtigungen gesendet werden, und ob AIP-Beschriftungen hinzugefügt werden), ändern Sie die

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 Löschen

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

Die BlueXP Klassifizierung bietet die folgenden systemdefinierten Richtlinien:

Name	Beschreibung	Logik
S3 öffentlich - offengelegte 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: Die europäischen Bürger	Dateien mit mehr als 5 Kennungen von EU-Bürgern oder DB-Tabellen, die Kennungen von EU-Bürgern enthalten	Dateien mit mehr als 5 Kennungen von (einem) EU-Bürgern oder DB-Tabellen, 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 mit mehr als 10 California Driver's License Identifier ODER DB-Tabellen mit California Driver's License
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

Die BlueXP Klassifizierung bietet Ihnen viele Möglichkeiten für das Management Ihrer 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 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 in Situationen, in denen Sie Daten von einem Quellsystem zu einem anderen migrieren, während noch einige letzte Aktivitäten in den Quelldateien vorliegen.
- Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, auf jede beliebige NFS-Freigabe verschieben.

- 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 kopieren

Sie können beliebige Quelldateien kopieren, die von der BlueXP Klassifizierung 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 BlueXP Kopier- und Synchronisierungsfunktion" Funktion zum Kopieren und Synchronisieren von Daten von einer Quelle an ein Ziel

Kopieren Sie Quelldateien auf eine NFS-Freigabe

Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, auf eine beliebige NFS-Freigabe kopieren. Die NFS-Freigabe muss nicht in die BlueXP Klassifizierung integriert werden – Sie müssen nur den Namen der NFS-Freigabe kennen, von der alle ausgewählten Dateien im Format kopiert werden `<host_name>:/<share_path>`.

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

Anforderungen

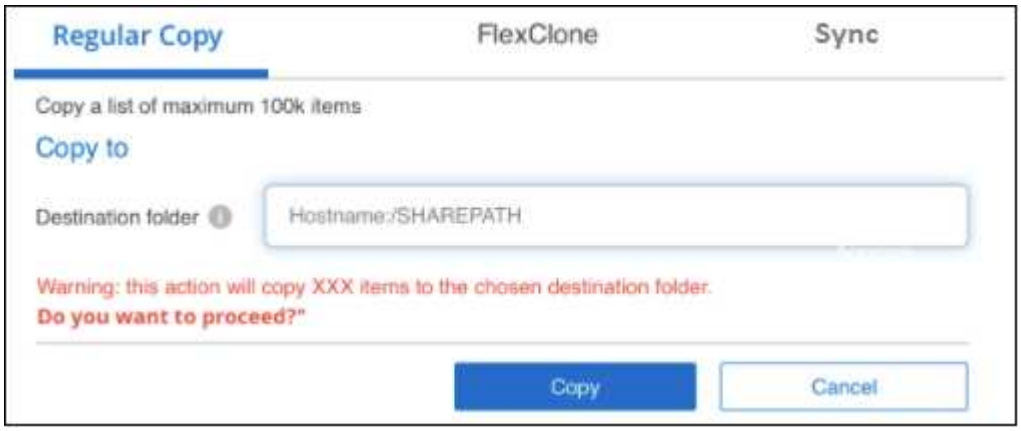
- Sie müssen über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen, um Dateien zu kopieren.
- Für das Kopieren von Dateien muss die NFS-Zielfreigabe den Zugriff über die BlueXP Klassifizierungsinstanz ermöglichen.
- Sie können zwischen 1 und 100,000 Dateien gleichzeitig kopieren.

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**.

Volume-Daten auf ein neues Volume klonen

Sie können ein vorhandenes ONTAP Volume klonen, das von der BlueXP Klassifizierung gescannt wird, mit der NetApp *FlexClone* Funktion. 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.

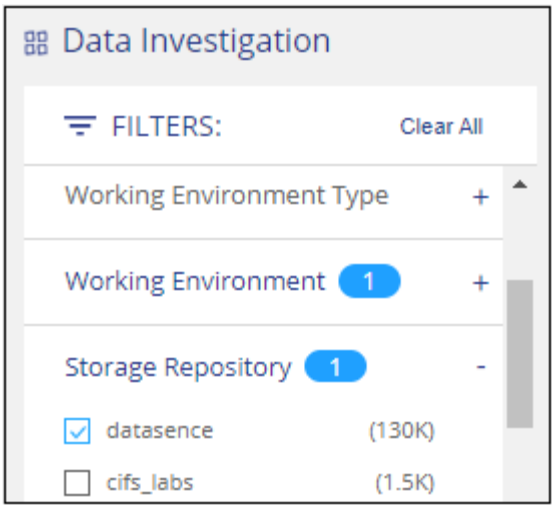
Hinweis: FlexGroup Volumes können nicht geklont werden, da sie nicht von FlexClone unterstützt werden.

Anforderungen

- Sie müssen über die Rolle „Kontoadministrator“ oder „Workspace-Admin“ verfügen, um Dateien zu kopieren.
- Sie müssen mindestens 20 Dateien auswählen.
- 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.

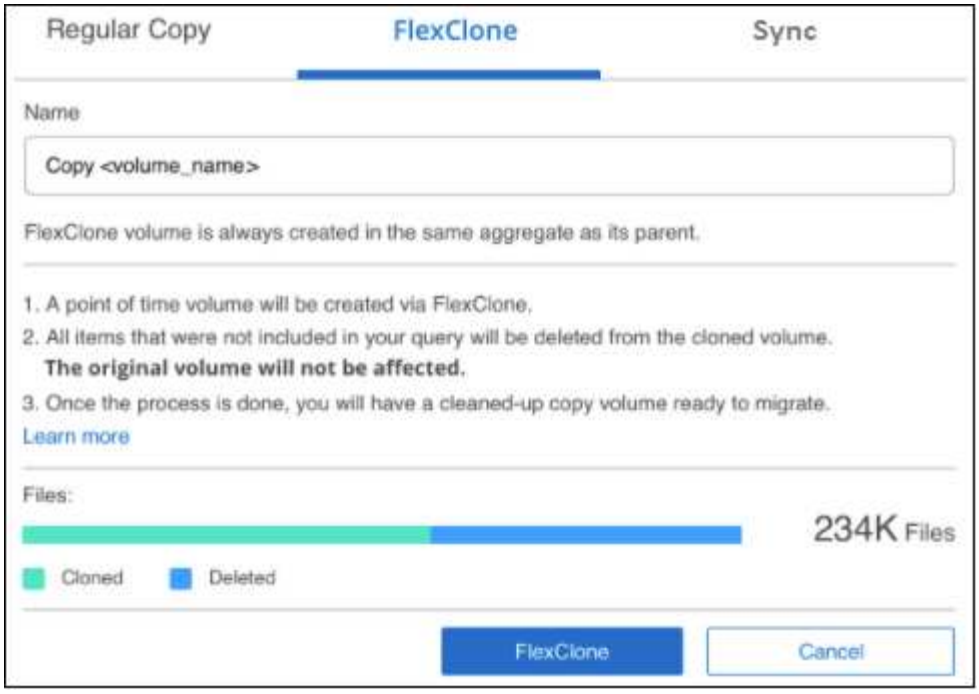


Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie auf dem neuen Volume klonen möchten.

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 (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)**.

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 zunächst **Alle Volumes zuweisen** oder **alle Volumes zuordnen und klassifizieren** ausgewählt haben, wenn Sie die BlueXP-Klassifizierung für die Arbeitsumgebung aktiviert haben, in der sich das Quell-Volume befindet, wird die BlueXP-Klassifizierung 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 Sie Quelldateien auf ein Zielsystem

Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, von einer unterstützten unstrukturierten Datenquelle in ein Verzeichnis an einem bestimmten Zielspeicherort kopieren ("Zielorte, die von der BlueXP Kopier- und Synchronisierungsfunktion 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 BlueXP Kopier- und Synchronisierungsfunktion" 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

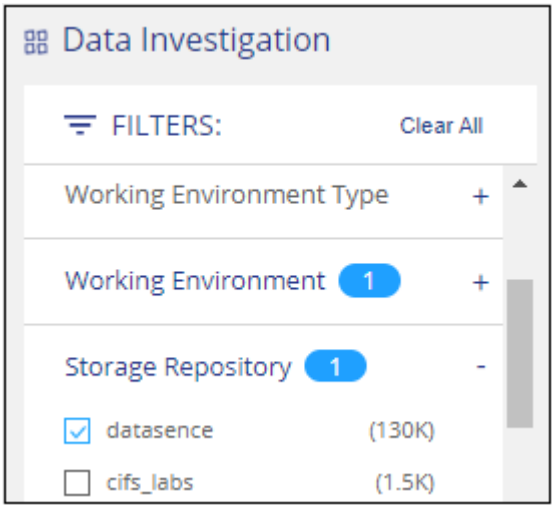
- Zum Kopieren und Synchronisieren von Dateien müssen Sie über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen.

- Sie müssen mindestens 20 Dateien auswählen.
- Alle ausgewählten Dateien müssen aus demselben Quell-Repository stammen (ONTAP Volume, S3 Bucket, NFS oder CIFS-Freigabe usw.).
- Sie müssen den BlueXP Kopier- und Synchronisierungsservice aktivieren und mindestens einen Daten-Broker konfigurieren, mit dem Dateien zwischen Quell- und Zielsystemen übertragen werden können. Prüfen Sie die BlueXP Kopier- und Synchronisierungsanforderungen beginnend mit "Kurzanleitung".

  Beachten Sie, dass für den BlueXP Kopier- und Synchronisierungsservice unterschiedliche Servicegebühren für Ihre Synchronisierungsbeziehungen anfallen und Ressourcengebühren anfallen, wenn Sie den Daten-Broker in der Cloud implementieren.

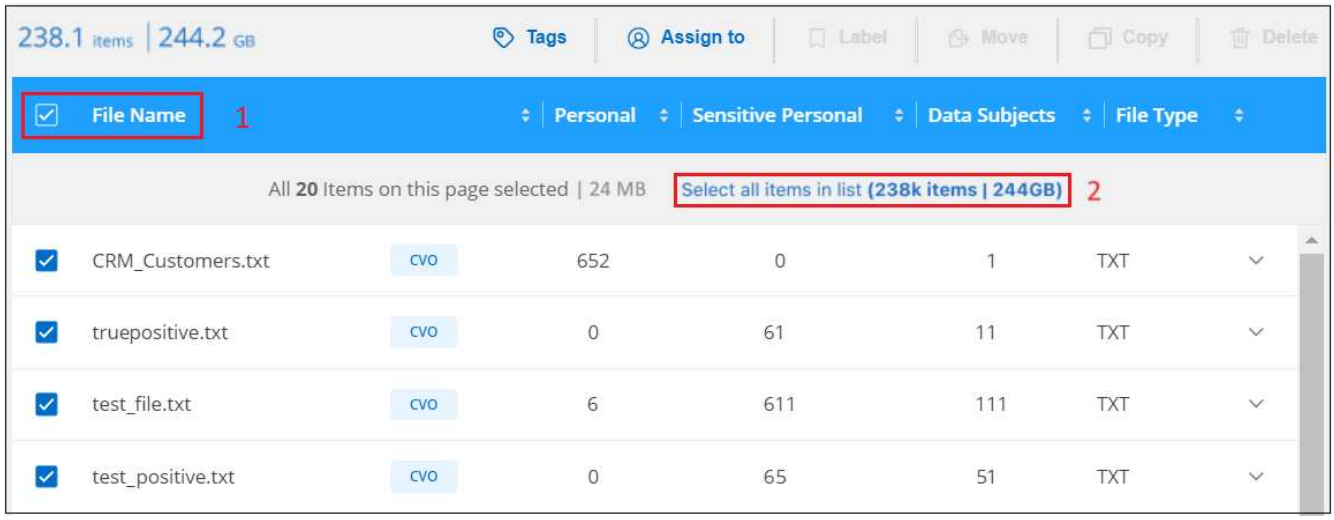
Schritte

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.

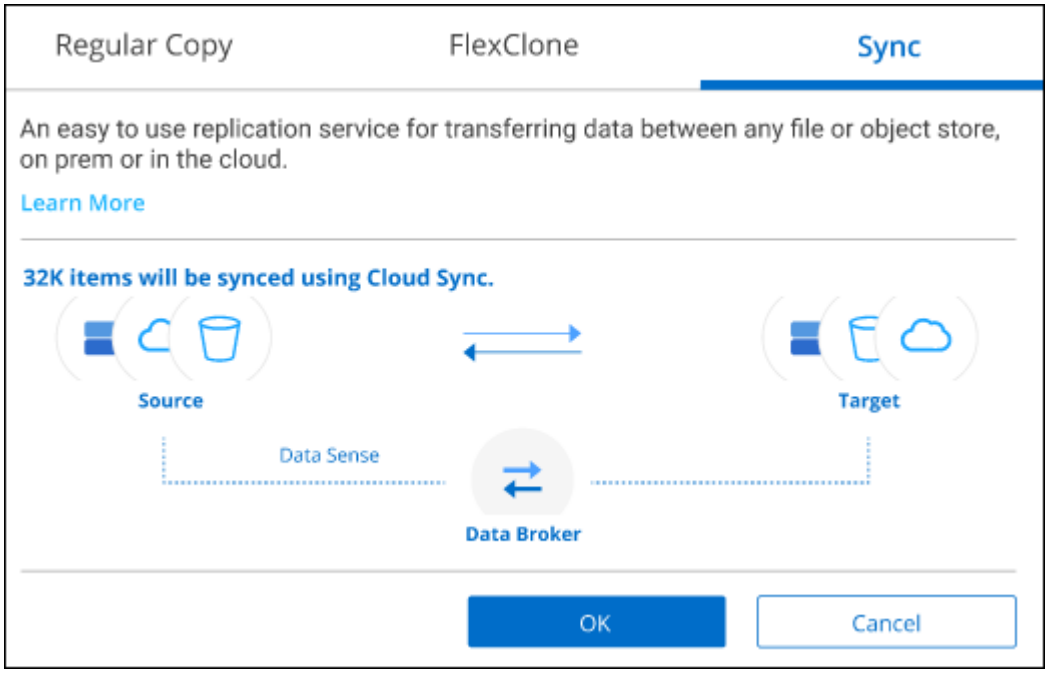


   Wenden Sie alle anderen Filter an, sodass nur die Dateien zu sehen sind, die Sie kopieren und mit dem Zielsystem synchronisieren möchten.

2. Wählen Sie im Bereich Untersuchungsergebnisse alle Dateien auf allen Seiten aus, indem Sie das Kästchen in der Titelzeile (aktivieren File Name), 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 BlueXP Kopier- und Synchronisierungs-UI wird in BlueXP geöffnet.

   Sie werden aufgefordert, die Synchronisierungsbeziehung zu definieren. Das Quellsystem basiert auf dem Repository und den Dateien, die Sie bereits in der BlueXP Klassifizierung ausgewählt haben, und wird entsprechend vorausgefüllt.

5. Sie müssen das Zielsystem auswählen und dann den zu verwendenden Daten-Broker (oder erstellen) auswählen. Prüfen Sie die BlueXP Kopier- und Synchronisierungsanforderungen beginnend mit "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 BlueXP Kopier- und Synchronisierungsvorgänge deaktiviert sind, wenn sie aus der BlueXP Klassifizierung aufgerufen werden:

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

Verschieben Sie Quelldateien auf eine NFS-Freigabe

Sie können Quelldateien, die von der BlueXP Klassifizierung gescannt werden, auf jede beliebige NFS-Freigabe verschieben. Die NFS-Freigabe muss nicht in die BlueXP Klassifizierung integriert werden.

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.

Beachten Sie, dass die Unterverzeichnisstruktur aus der Quelldatei beim Verschieben der Datei auf der Zielfreigabe neu erstellt wird, sodass Sie leichter verstehen können, woher die Datei verschoben wurde. 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

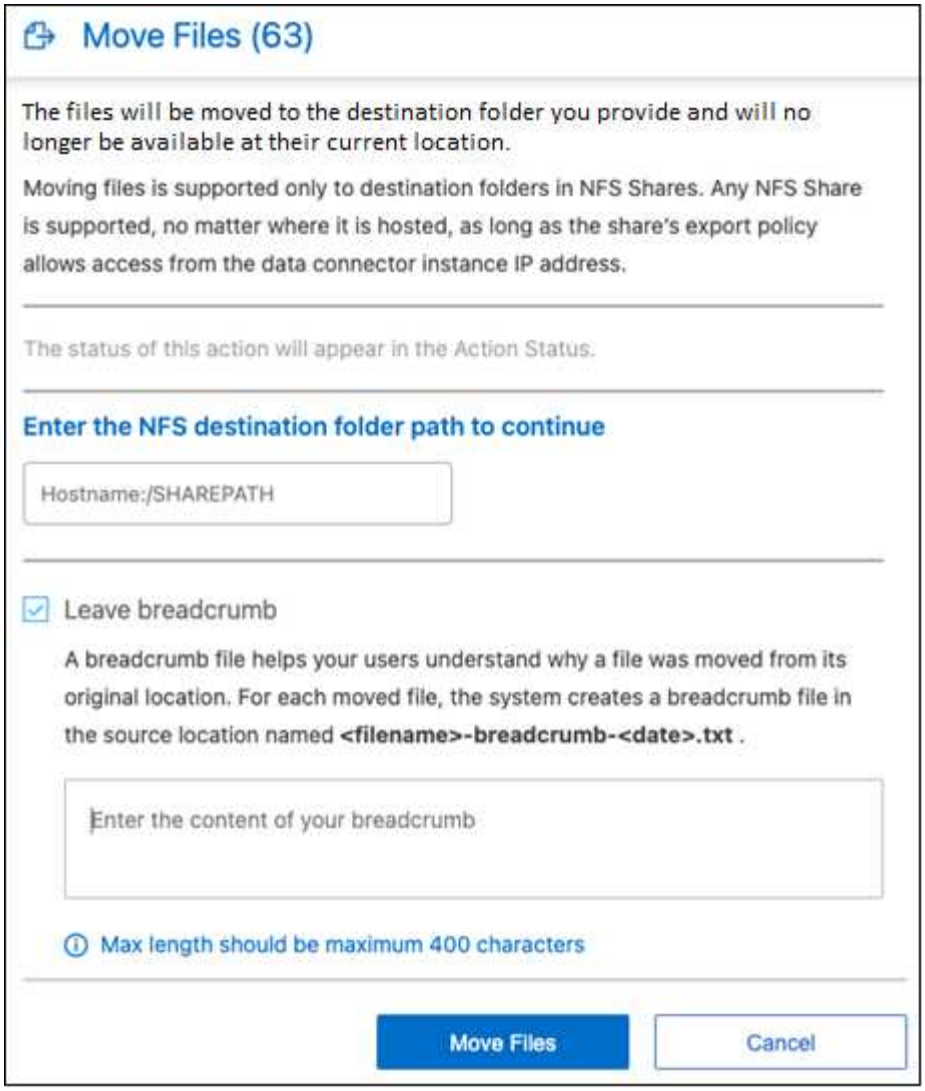
- Sie müssen über die Rolle „Kontoadministrator“ oder „Arbeitsbereichsadministrator“ verfügen, um Dateien zu verschieben.
- Die Quelldateien lassen sich in den folgenden Datenquellen befinden: On-Premises ONTAP, Cloud Volumes ONTAP, Azure NetApp Files, File Shares und SharePoint Online.
- Sie können maximal 15 Millionen Dateien gleichzeitig verschieben.
- Es werden nur Dateien verschoben, die 50 MB oder kleiner sind.
- Die NFS-Zielfreigabe muss den Zugriff von der IP-Adresse der BlueXP Klassifizierungsinstanz ermöglichen.

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 löschen

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 löschen, oder "Automatische Verwendung von Richtlinien".

> Sie können keine Dateien löschen, die sich in Datenbanken befinden. Alle anderen Datenquellen werden unterstützt.

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 manuell löschen

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**.

Anzeigen von Compliance-Berichten

Die BlueXP Klassifizierung bietet Berichte, die Sie verwenden können, um besseren Einblick in den Status Ihres Unternehmenskonzepts zum Datenschutz zu erhalten.

Standardmäßig zeigen die BlueXP Klassifizierungs-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 die Genauigkeit der personenbezogenen Daten und sensiblen personenbezogenen Daten, die durch die BlueXP Klassifizierung identifiziert werden, nicht zu 100 % garantieren. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Datenschutzrisiko-Assessment-Bericht

Der Datenschutzrisiko-Assessment-Bericht bietet einen Überblick über den Datenschutz-Risikostatus Ihres Unternehmens, wie durch Datenschutzvorschriften wie DSGVO und CCPA erforderlich. 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

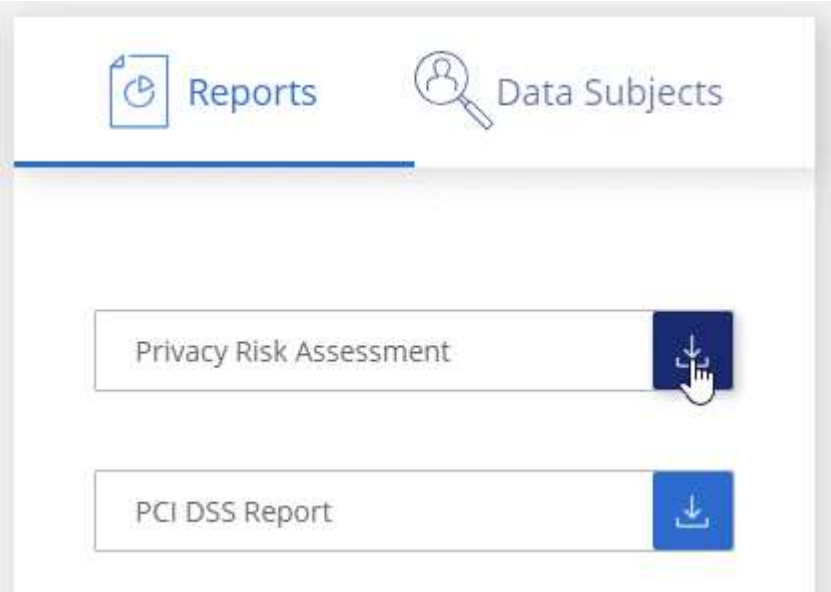
Die Anzahl der Personen, nach Ort, für die nationale Kennungen gefunden wurden.

Erstellen Sie den Bericht zur Risikoanalyse für den Datenschutz

Rufen Sie die Registerkarte Compliance 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

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Schweregrad

Die BlueXP Klassifizierung berechnet die Bewertung des Schweregrads für den Bericht zur Risikoanalyse personenbezogener Daten auf der Basis 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

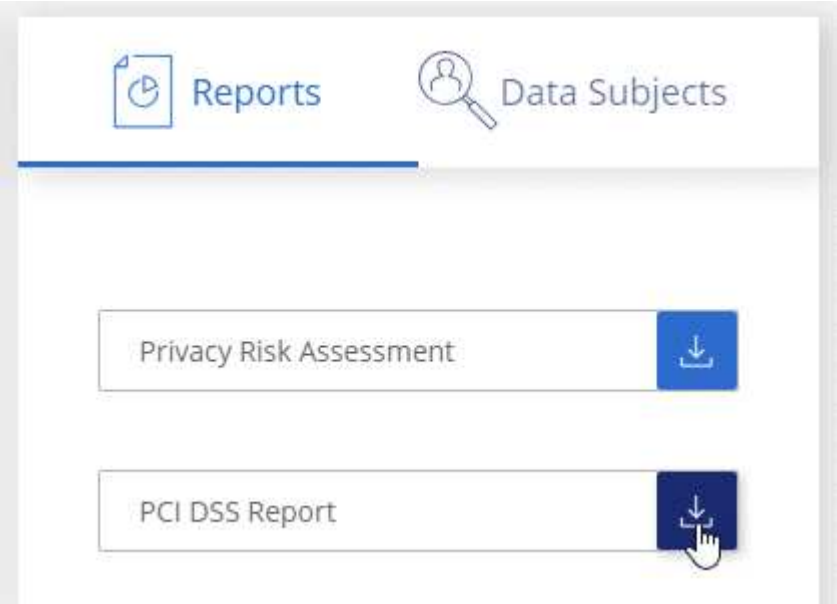
Die Arbeitsumgebungen, in denen Kreditkartendaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

Erstellen Sie den PCI DSS-Bericht

Rufen Sie die Registerkarte Compliance 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

Die BlueXP Klassifizierung generiert 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. Er unterstützt Ihr Unternehmen bei der Einhaltung der HIPAA-Datenschutzgesetze. Die Informationen, für die die BlueXP Klassifizierung geeignet ist, umfassen:

- 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

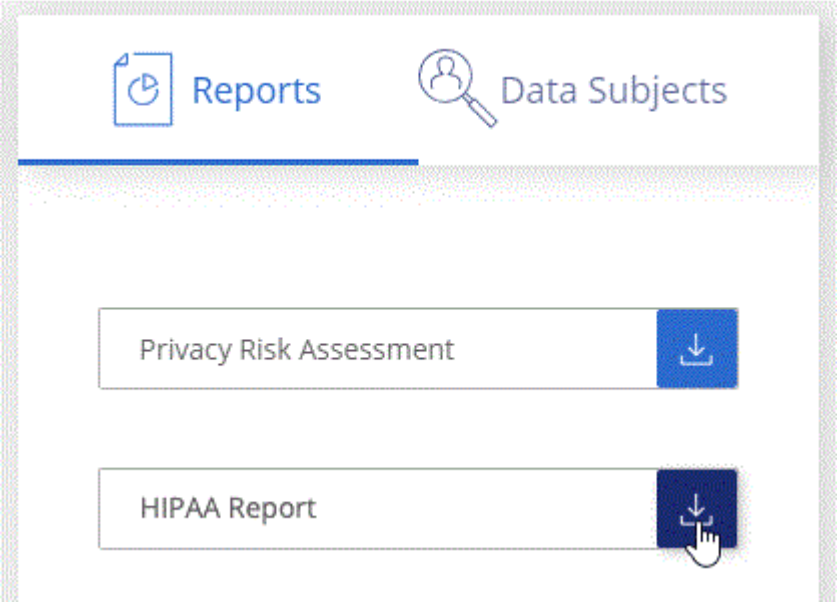
In den Arbeitsumgebungen, in denen die Gesundheitsdaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

Erstellen Sie den HIPAA-Bericht

Rufen Sie die Registerkarte Compliance 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

Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

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.

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

Wie kann die BlueXP Klassifizierung Ihnen helfen, auf eine DSAR zu reagieren?

Wenn Sie eine Suche nach einer bestimmten Person durchführen, findet die BlueXP Klassifizierung alle Dateien, Buckets, OneDrive und SharePoint Konten, die den Namen oder die Kennung dieser Person enthalten. Die BlueXP Klassifizierung überprüft die aktuellsten vorab indizierten Daten nach dem Namen oder der 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.

Suche nach betroffenen Personen und Download von Berichten

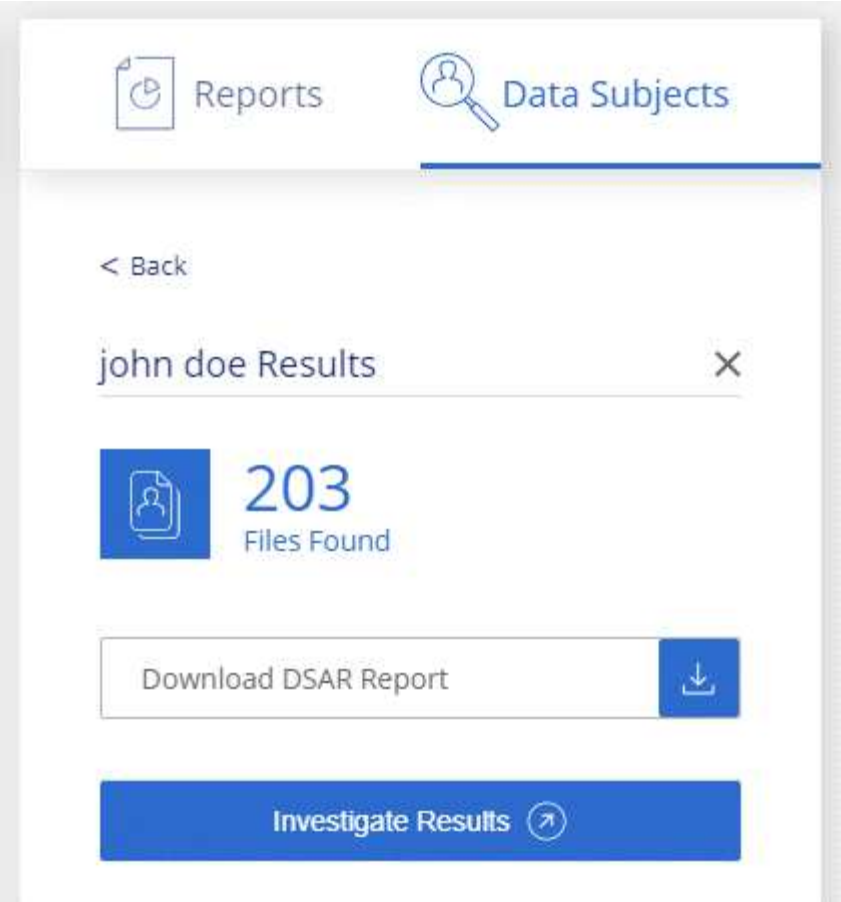
Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Suchen Sie nach "Alle persönlichen Informationstypen".

> Bei der Suche nach den Namen der betroffenen Personen werden Englisch, Deutsch, Japanisch und Spanisch 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, die auf Daten basieren, deren BlueXP-Klassifizierung für den Betroffenen gefunden wurde und als Vorlage dienen. 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.

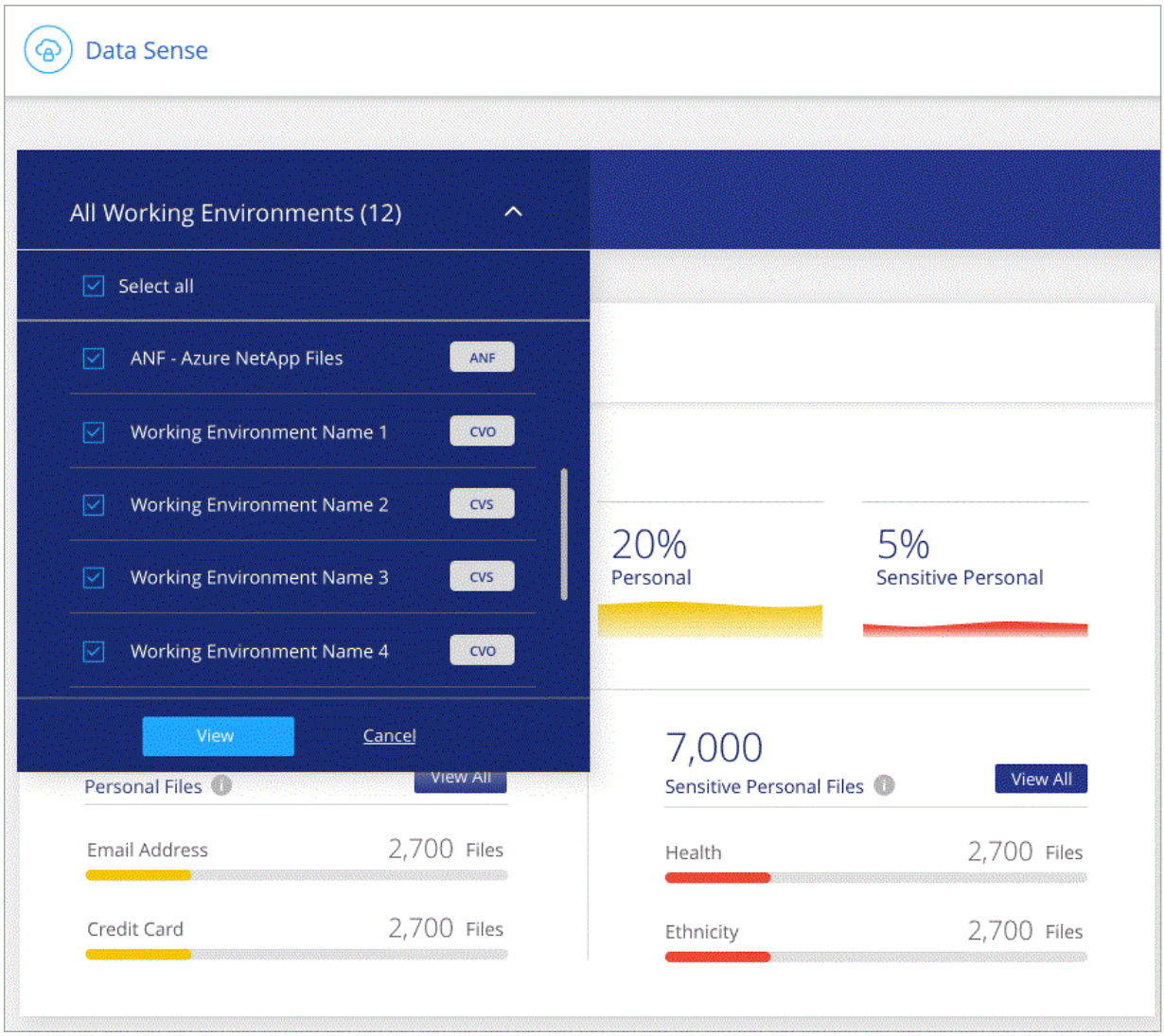
Wählen Sie die Arbeitsumgebungen für Berichte aus

Sie können die Inhalte des BlueXP Klassifizierungs-Compliance-Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen einzusehen.

Wenn Sie das Dashboard filtern, erfasst die BlueXP Klassifizierung die Compliance-Daten und Berichte nur an die von Ihnen ausgewählten Applikationsumgebungen.

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**.


Data Sense
All Working Environments (12)
Select all
ANF - Azure NetApp Files
ANF
Working Environment Name 1
CVO
Working Environment Name 2
CVS
Working Environment Name 3
CVS
Working Environment Name 4
CVO
View
Cancel
20%
Personal
5%
Sensitive Personal
7,000
Sensitive Personal Files
View All
Personal Files
View All
Email Address
2,700 Files
Credit Card
2,700 Files
Health
2,700 Files
Ethnicity
2,700 Files