BlueXP Klassifizierung nutzen

BlueXP classification

NetApp
July 22, 2025

This PDF was generated from https://docs.netapp.com/de-de/bluexp-classification/task-controlling-governance-data.html on July 22, 2025. Always check docs.netapp.com for the latest.

Inhalt

BlueXP Klassifizierung nutzen . . . 1
Anzeigen von Governance-Details zu den in Ihrem Unternehmen mit BlueXP -Klassifizierung gespeicherten Daten . . . 1
Überprüfen Sie das Dashboard „Governance“ . . . 1
Erstellen Sie den Data Discovery Assessment Report . . . 4
Erstellen Sie den Übersichtsbericht zur Datenzuordnung . . . 4
Anzeigen von Compliance-Details zu den in Ihrem Unternehmen mit BlueXP Klassifizierung gespeicherten privaten Daten . . . 7
Dateien anzeigen, die personenbezogene Daten enthalten . . . 8
Dateien anzeigen, die sensible personenbezogene Daten enthalten . . . 10
Dateien nach Kategorien anzeigen . . . 12
Dateien nach Dateitypen anzeigen . . . 13
Kategorien von privaten Daten in BlueXP -Klassifizierung . . . 14
Arten personenbezogener Daten . . . 14
Arten sensibler personenbezogener Daten . . . 19
Arten von Kategorien . . . 20
Dateitypen . . . 21
Genauigkeit der gefundenen Informationen . . . 21
Erstellen Sie eine benutzerdefinierte Klassifizierung in der BlueXP -Klassifizierung . . . 22
Erstellen Sie eine benutzerdefinierte Klassifizierung . . . 22
Untersuchen Sie die in Ihrem Unternehmen gespeicherten Daten mit der BlueXP -Klassifizierung . . . 23
Filtern Sie die Daten auf der Seite „Datenuntersuchung“ . . . 24
Anzeigen von Datei-Metadaten . . . 27
Benutzerberechtigungen für Dateien und Verzeichnisse anzeigen . . . 28
Überprüfen Sie auf doppelte Dateien in Ihren Speichersystemen . . . 29
Erstellen Sie den Datenermittlungsbericht . . . 30
Erstellen Sie eine gespeicherte Suche basierend auf ausgewählten Filtern . . . 33
Verwalten Sie gespeicherte Suchen mit BlueXP -Klassifizierung . . . 34
Zeigen Sie die gespeicherten Suchergebnisse auf der Seite Untersuchung an . . . 34
Erstellen Sie benutzerdefinierte gespeicherte Suchen . . . 35
Bearbeiten Sie gespeicherte Suchen . . . 36
Löschen Sie gespeicherte Suchen . . . 38
Standardsuche . . . 38
Ändern Sie die Scaneinstellungen für die BlueXP -Klassifizierung für Ihre Repositorys . . . 39
Anzeigen des Scanstatus für Ihre Repositorys . . . 39
Ändern Sie den Typ der Suche nach einem Repository . . . 40
Priorisieren Sie Scans . . . 41
Beenden Sie die Suche nach einem Repository . . . 42
Halten Sie die Suche nach einem Repository an und setzen Sie sie fort . . . 43
Anzeigen von Compliance-Berichten zur BlueXP -Klassifizierung . . . 44
Wählen Sie die Arbeitsumgebungen für Berichte aus . . . 44
Zugriffsanfrage Für Betroffene . . . 45
Bericht zum Health Insurance Portability and Accountability Act (HIPAA) . . . 47

Bericht zum Payment Card Industry Data Security Standard (PCI DSS) 48
Datenschutzrisiko-Assessment-Bericht 49

BlueXP Klassifizierung nutzen

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

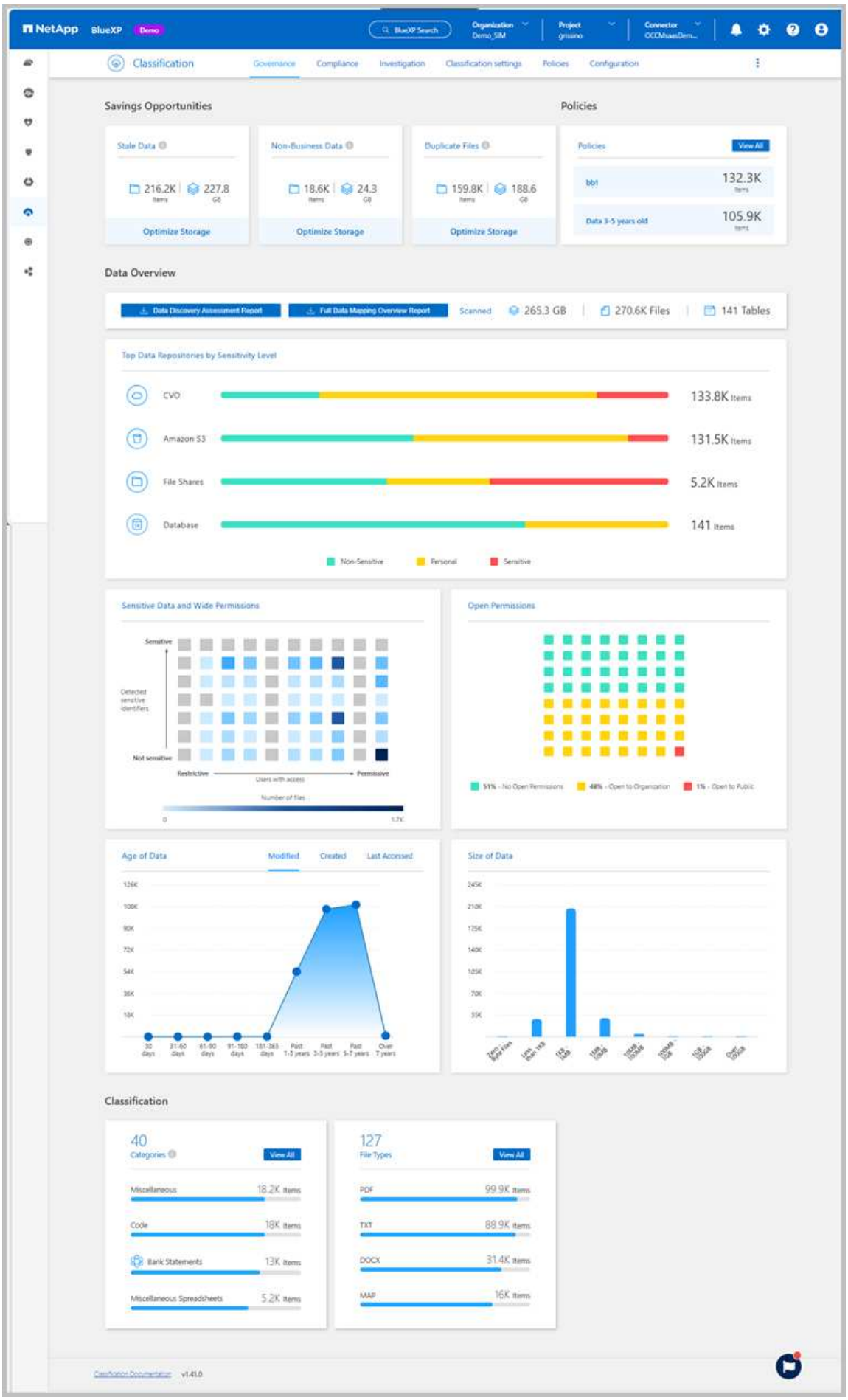
Behalten Sie die Kontrolle über die Kosten im Zusammenhang mit den Daten auf den Speicherressourcen Ihres Unternehmens. Die BlueXP Klassifizierung ermittelt die Menge veralteter Daten, nicht geschäftsferner Daten, mehrfach vorhandener Dateien und sehr großer Dateien auf Ihren Systemen. So können Sie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

Dies ist, wo Sie Ihre Forschung beginnen sollten. Im Dashboard „Governance“ können Sie einen Bereich für weitere Untersuchungen auswählen.

Wenn Sie zudem Daten von lokalen Speicherorten in die Cloud migrieren möchten, können Sie die Größe der Daten und auch prüfen, ob sensible Daten vor dem Verschieben enthalten sind.

Überprüfen Sie das Dashboard „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.


NetApp
BlueXP
Demo
Classification
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
216.2K Items
227.8 GB
Optimize Storage
Non-Business Data
18.6K Items
24.3 GB
Optimize Storage
Duplicate Files
159.8K Items
188.6 GB
Optimize Storage
Policies
View All
bb1
132.3K Items
Data 3-5 years old
105.9K Items
Data Overview
Data Discovery Assessment Report
Full Data Mapping Overview Report
Scanned
265.3 GB
270.6K Files
141 Tables
Top Data Repositories by Sensitivity Level
CVO
133.8K Items
Amazon S3
131.5K Items
File Shares
5.2K Items
Database
141 Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Open Permissions
Age of Data
Modified
Created
Last Accessed
Size of Data
Classification
40
Categories
View All
Miscellaneous
18.2K Items
Code
18K Items
Bank Statements
13K Items
Miscellaneous Spreadsheets
5.2K Items
127
File Types
View All
PDF
99.9K Items
TXT
88.9K Items
DOCX
31.4K Items
MAP
16K Items

Schritte

1. Wählen Sie im Menü BlueXP die Option **Steuerung > Klassifizierung**.
2. Wählen Sie **Governance**.

   Das Dashboard „Governance“ wird angezeigt.

Prüfen Sie die Einsparmöglichkeiten

Die Komponente „Einsparmöglichkeiten“ zeigt Daten an, die Sie löschen oder in einen kostengünstigeren Objektspeicher verschieben können. Die Daten in „Einsparmöglichkeiten“ werden alle zwei Stunden aktualisiert und können manuell aktualisiert werden.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Governance**.
2. Wählen Sie in jeder Kachel „Einsparungsmöglichkeiten“ des Governance-Dashboards **Speicher optimieren** aus, um die gefilterten Ergebnisse auf der Seite „Untersuchung“ anzuzeigen. Um herauszufinden, welche Daten Sie löschen oder auf einen günstigeren Speicher verschieben sollten, untersuchen Sie die *Sparmöglichkeiten*.
   - **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".

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

Überprüfen Sie gespeicherte Suchen mit der größten Anzahl von Ergebnissen

Auf der Registerkarte *Saved searches* werden die Suchen mit der größten Anzahl von Ergebnissen am Anfang der Liste angezeigt. Diese Daten werden alle zwei Stunden aktualisiert.

Weitere Informationen zu gespeicherten Suchen finden Sie unter "Erstellen Sie gespeicherte Suchen".

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Governance**.
2. Suchen Sie im Governance-Dashboard nach der Kachel „Gespeicherte Suchvorgänge“. Wählen Sie den Namen einer gespeicherten Suche aus, um die Ergebnisse auf der Seite Untersuchung anzuzeigen.
3. Wählen Sie **Alle anzeigen**, um die Liste aller verfügbaren gespeicherten Suchen anzuzeigen. Im Bereich

Saved searches werden die Suchen mit der größten Anzahl von Ergebnissen am Anfang der Liste angezeigt.

Erstellen Sie den Data Discovery Assessment Report

Der Data Discovery Assessment Report bietet eine allgemeine Analyse der gescannten Umgebung, um 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:

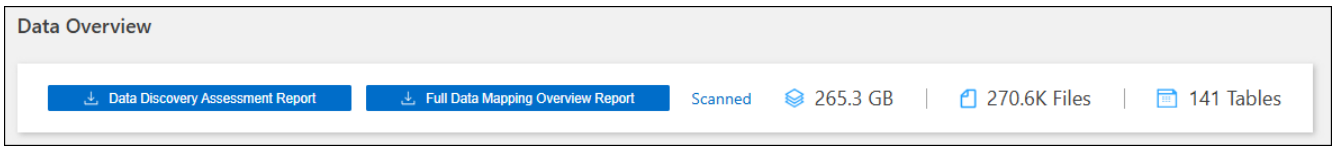
Merkmal	Beschreibung
Bedenken hinsichtlich der Daten-Governance	Ein detaillierter Überblick über alle Daten, die Sie besitzen, und Bereiche, in denen Sie die Datenmenge möglicherweise reduzieren und Kosten einsparen können.
Risiken im Hinblick auf die Datensicherheit	Bereiche, in denen Daten aufgrund 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.

Mit diesem Bericht können Sie folgende Maßnahmen ergreifen:

- 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

Schritte

1. Wählen Sie im Menü BlueXP die Option **Steuerung > Klassifizierung**.
2. Wählen Sie **Governance**.
3. Wählen Sie **Data Discovery Assessment Report**.



Ergebnis

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

Erstellen Sie den Übersichtsbericht zur Datenzuordnung

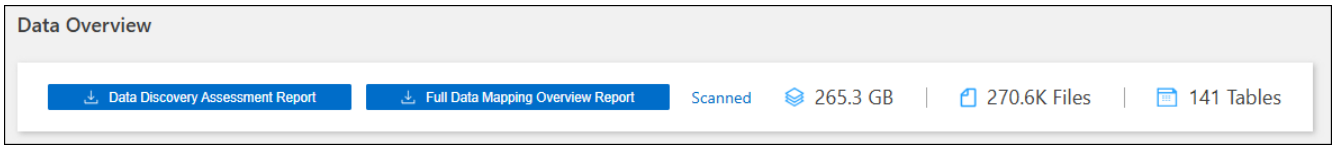
Der Data Mapping Overview Report bietet einen Überblick über die Daten, die in Ihren Unternehmensdatenquellen gespeichert werden, um Sie bei Entscheidungen über Migration, Backup, Sicherheit und Compliance-Prozesse zu unterstützen. Der Bericht fasst alle Arbeitsumgebungen und Datenquellen zusammen. Außerdem bietet er eine Analyse 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.

Schritte

1. Wählen Sie im Menü BlueXP die Option **Steuerung > Klassifizierung**.
2. Wählen Sie **Governance**.
3. Wählen Sie **Übersichtsbericht Zur Datenzuordnung** Aus.



4. Um den Unternehmensnamen anzupassen, der auf der ersten Seite des Berichts angezeigt wird, wählen Sie oben rechts auf der Seite BlueXP -Klassifizierung die Option . Wählen Sie dann **Firmennamen ändern**. Wenn Sie den Bericht das nächste Mal erstellen, wird er den neuen Namen enthalten.

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 Sie werden eine Popup-Meldung über den genauen Speicherort sehen. Wenn die BlueXP Klassifizierung auf einer lokalen Linux-Maschine oder auf einer Linux-Maschine in der Cloud installiert ist, können Sie direkt zur PDF-Datei navigieren. Wenn die BlueXP-Klassifizierung in der Cloud bereitgestellt wird, müssen Sie per SSH eine Verbindung zur BlueXP-Klassifizierungsinstanz herstellen, um die PDF-Datei herunterzuladen.

Prüfen Sie die wichtigsten Daten-Repositorys nach Datensensibilität

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

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

Diese Daten werden alle zwei Stunden aktualisiert und können manuell aktualisiert werden.

Schritte

1. Um die Gesamtanzahl der Elemente in jeder Kategorie anzuzeigen, setzen Sie den Cursor über die einzelnen Bereiche der Leiste.
2. Um die Ergebnisse zu filtern, die auf der Untersuchungsseite angezeigt werden, wählen Sie jeden Bereich in der Leiste aus und untersuchen Sie ihn weiter.

Überprüfung sensibler Daten und breiter Berechtigungen

Der Bereich *sensible Daten und weite Berechtigungen* des Berichts Data Mapping Overview zeigt den Prozentsatz der Dateien an, die sensible Daten enthalten und über breite Berechtigungen verfügen. Das Diagramm zeigt die folgenden Berechtigungstypen:

- Von den restriktivsten Berechtigungen bis zu den freizügigsten Einschränkungen auf der horizontalen Achse.
- Von den am wenigsten sensiblen Daten zu den sensibelsten Daten auf der vertikalen Achse.

Schritte

1. Um die Gesamtanzahl der Dateien in jeder Kategorie anzuzeigen, setzen Sie den Cursor über jedes Feld.
2. Um die Ergebnisse zu filtern, die auf der Untersuchungsseite angezeigt werden, wählen Sie ein Feld aus, und untersuchen Sie es weiter.

Überprüfen Sie die Daten, die nach Typen offener Berechtigungen aufgelistet sind

Im Bereich *Open Permissions* des Berichts Data Mapping Overview wird der Prozentsatz für jeden Berechtigungstyp angezeigt, 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

Schritte

1. Um die Gesamtanzahl der Dateien in jeder Kategorie anzuzeigen, setzen Sie den Cursor über jedes Feld.
2. Um die Ergebnisse zu filtern, die auf der Untersuchungsseite angezeigt werden, wählen Sie ein Feld aus, und untersuchen Sie es weiter.

Überprüfen Sie das Alter und die Größe der Daten

Vielleicht sollten Sie die Elemente in den Diagrammen *Alter* und *Größe* im Bericht Data Mapping Overview untersuchen, um zu ermitteln, ob Daten gelöscht werden sollten oder in einen kostengünstigeren Objektspeicher verschoben werden sollten.

Schritte

1. Um Details über das Alter der Daten anzuzeigen, bewegen Sie den Cursor im Diagramm über einen Punkt.
2. Um nach einem Alter oder Größenbereich zu filtern, wählen Sie dieses Alter oder diese Größe aus.
    - **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.

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

Prüfen Sie die am häufigsten identifizierten Datenklassifizierungen in Ihren Daten

Der *Classification*-Bereich des Berichts Data Mapping Overview enthält eine Liste der am häufigsten identifizierten "Kategorien" und "Dateitypen"gescannten Daten.

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 sich die Ergebnisse genauer anschauen, stellen Sie möglicherweise fest, dass Mitarbeiterverträge an einem nicht sicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Weitere Informationen finden Sie unter "Anzeigen von Dateien nach Kategorien" .

Schritte

1. Wählen Sie im Menü BlueXP die Option **Steuerung > Klassifizierung**.
2. Wählen Sie **Governance** und dann die Schaltfläche **Data Discovery Assessment Report**.

Ergebnis

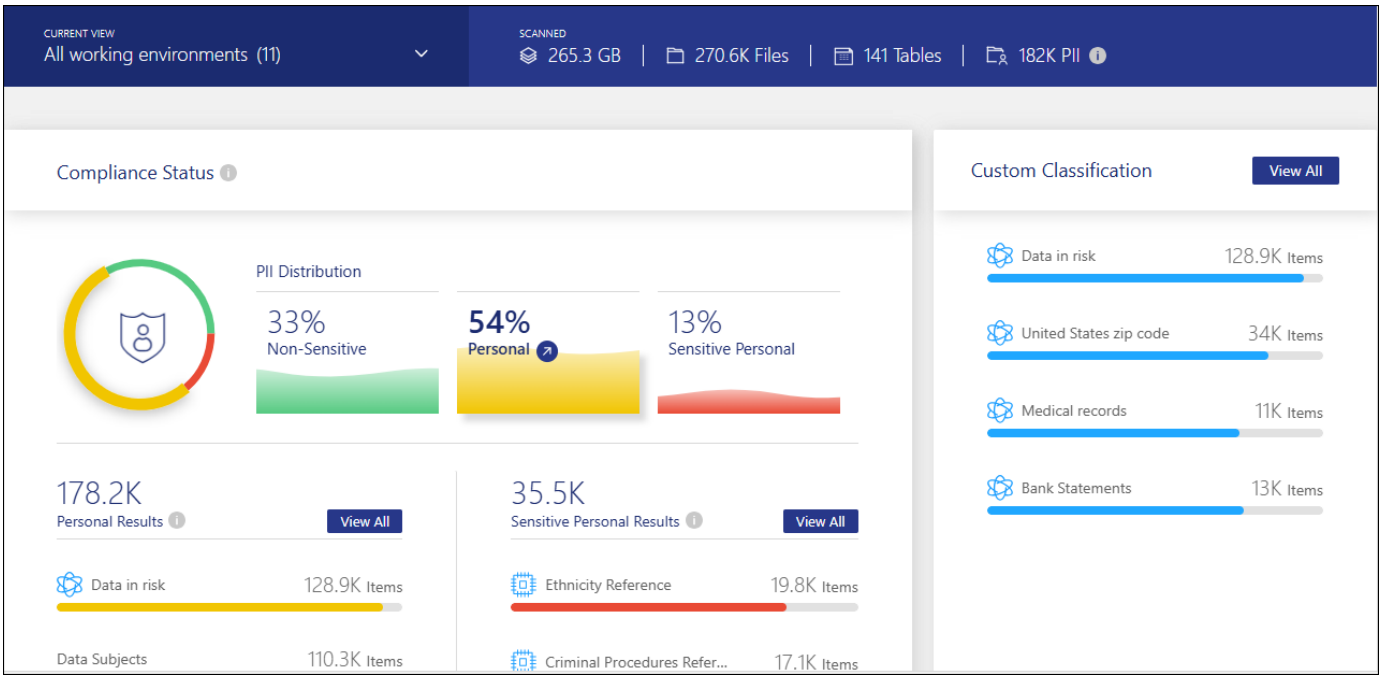
Die BlueXP Klassifizierung generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Anzeigen von Compliance-Details zu den in Ihrem Unternehmen mit BlueXP Klassifizierung gespeicherten privaten Daten

Behalten Sie die Kontrolle über Ihre privaten Daten, indem Sie sich Details zu den persönlichen Daten (PII) und sensiblen persönlichen Daten (SPII) in Ihrem Unternehmen ansehen. 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. Um Daten nur für einige Arbeitsumgebungen anzuzeigen, wählen Sie sie aus.



Filtern Sie die Ergebnisse auf der Seite „Datenuntersuchung“, und laden Sie einen Bericht der Ergebnisse als CSV-Datei herunter. Weitere Informationen finden Sie unter "Filtern von Daten auf der Seite „Datenuntersuchung“" .

Dateien anzeigen, die personenbezogene Daten enthalten

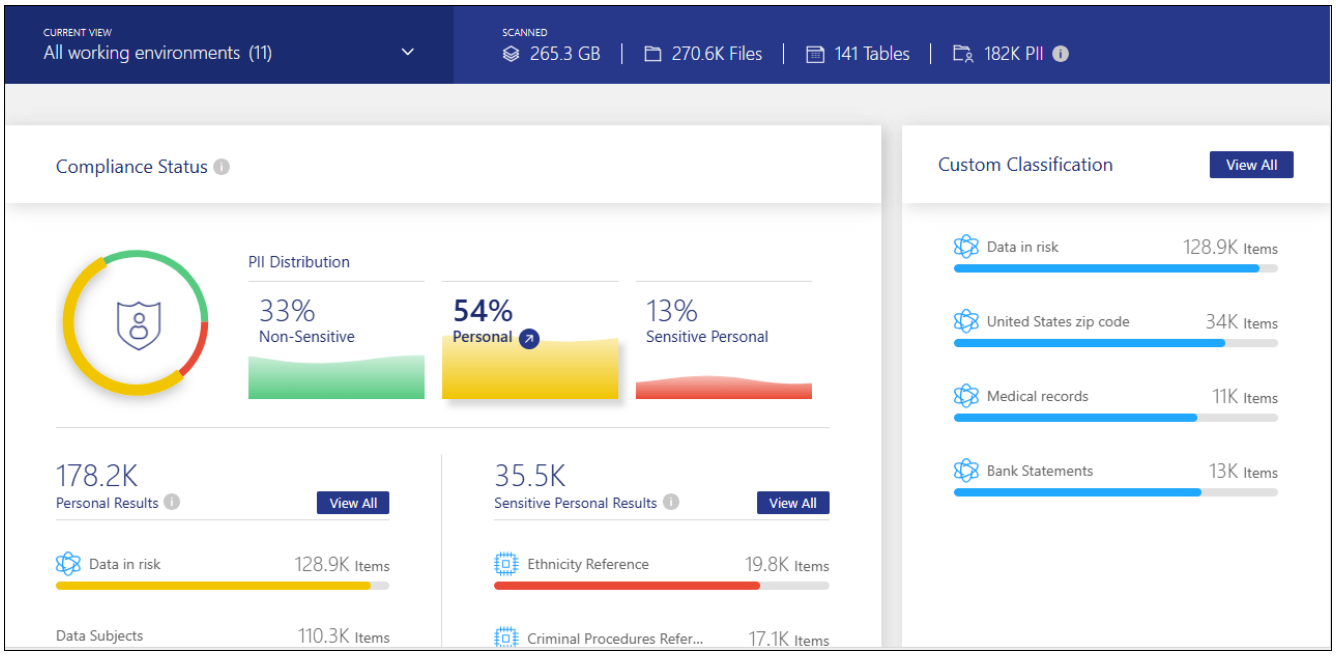
Durch die BlueXP Klassifizierung werden automatisch bestimmte Wörter, Strings und Muster (Regex) innerhalb der Daten identifiziert. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern, Kontonummern, Passwörter, Und vieles mehr. "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.

Sie können auch benutzerdefinierte Suchbegriffe erstellen, um personenbezogene Daten für Ihr Unternehmen zu identifizieren. Weitere Informationen finden Sie unter "Erstellen Sie eine benutzerdefinierte Klassifizierung".

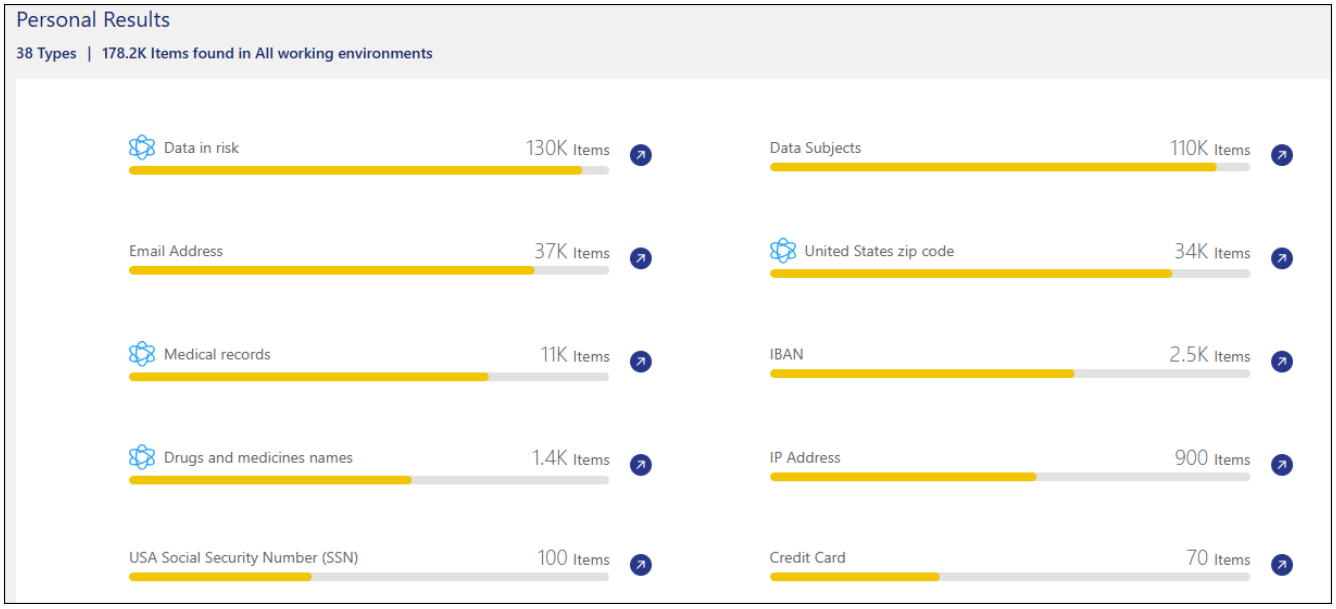
Für einige Arten von personenbezogenen Daten verwendet die BlueXP Klassifizierung *Proximity Validation*, um ihre Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. So identifiziert die BlueXP -Klassifikation beispielsweise eine US-Sozialversicherungsnummer (SSN) als SSN, wenn sie ein Nachbarschaftswort daneben sieht, z. B. *SSN* oder *soziale Sicherheit*. "Der Tisch der personenbezogenen Daten" Zeigt an, wann die BlueXP -Klassifizierung die Annäherungsvalidierung verwendet.

Schritte

1. Wählen Sie im Menü BlueXP Classification die Registerkarte **Compliance** aus.
2. Um die Details für alle persönlichen Daten zu untersuchen, wählen Sie das Symbol neben dem Prozentsatz der persönlichen Daten aus.

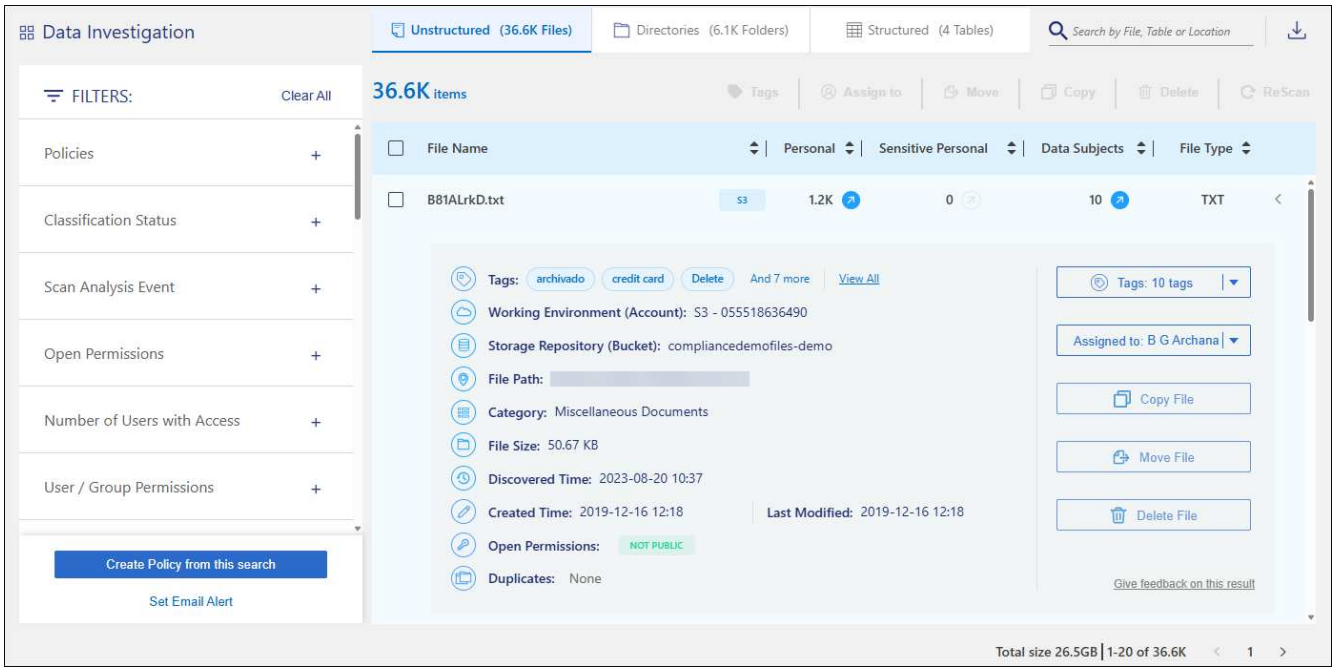


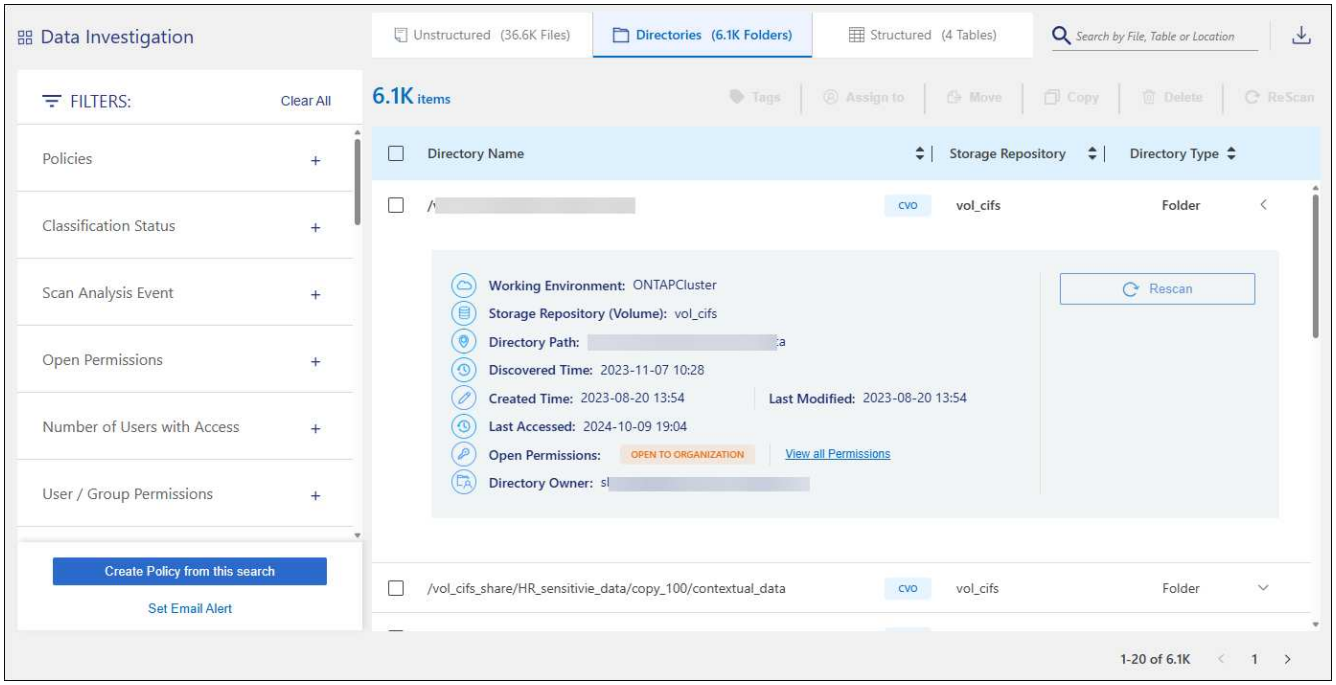
3. Um die Details für einen bestimmten Typ von persönlichen Daten zu untersuchen, wählen Sie **Alle anzeigen** und wählen Sie dann das Pfeilsymbol **Ergebnisse untersuchen** für einen bestimmten Typ von persönlichen Daten, z. B. E-Mail-Adressen.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, den Pfeil **Ergebnisse untersuchen** auswählen, um maskierte Informationen anzuzeigen, oder indem Sie die Dateiliste herunterladen.

   Die beiden folgenden Screenshots zeigen persönliche Daten, die in einzelnen Dateien gefunden wurden und in Dateien innerhalb von Verzeichnissen (Freigaben und Ordner) gefunden wurden. 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 spezielle Arten von sensiblen personenbezogenen Daten, wie sie durch Datenschutzvorschriften wie definiert "Artikel 9 und 10 der DSGVO" sind. 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.

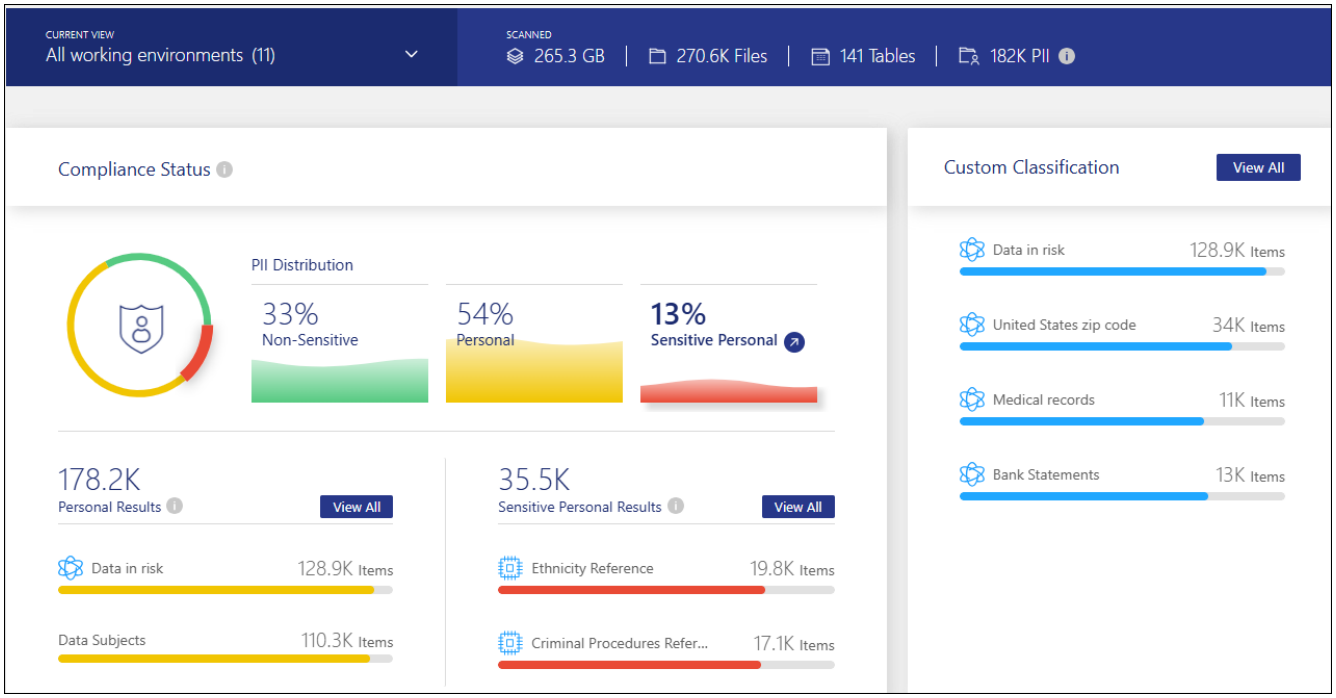
Die BlueXP Klassifizierung verwendet künstliche Intelligenz (KI), Natural Language Processing (NLP), Machine Learning (ML) und Cognitive Computing (CC), um die Bedeutung des gescannten Inhalts zu verstehen. Anhand dessen werden Entitäten extrahiert und entsprechend kategorisiert.

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“.

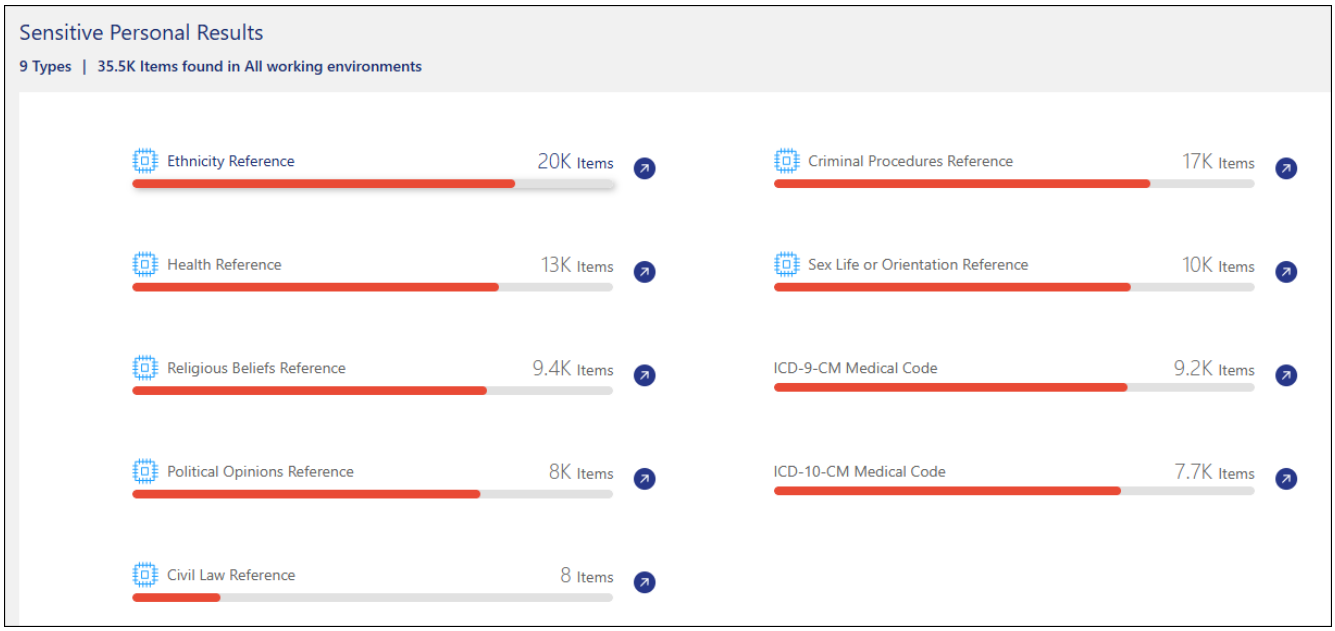
Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Wählen Sie im Menü BlueXP Classification die Option **Compliance**.
2. Um die Details für alle sensiblen persönlichen Daten zu untersuchen, wählen Sie das Symbol neben dem Prozentsatz der sensiblen persönlichen Daten.



3. Um die Details für einen bestimmten Typ von sensiblen persönlichen Daten zu untersuchen, wählen Sie **Alle anzeigen** und wählen Sie dann das Pfeilsymbol **Ergebnisse untersuchen** für einen bestimmten Typ von sensiblen persönlichen 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

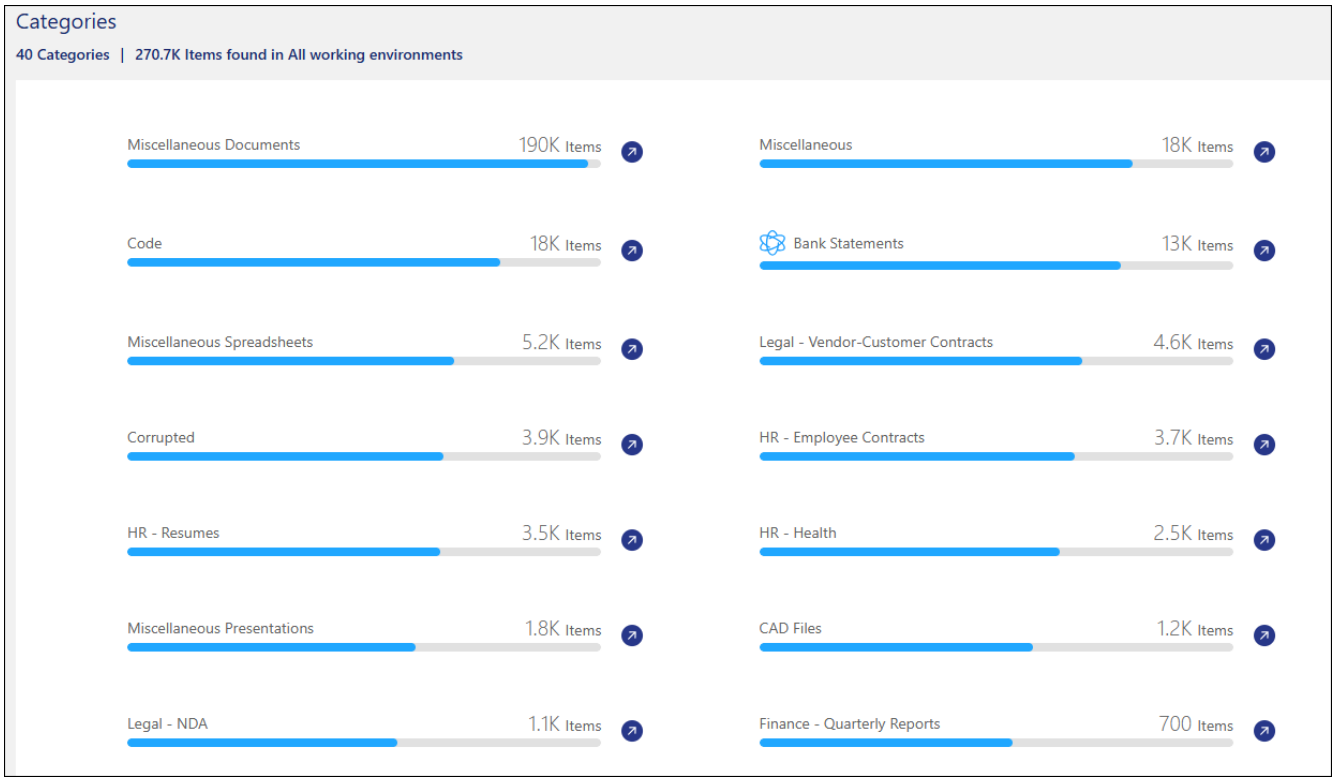
Die BlueXP Klassifizierung unterteilt die gescannten Daten in unterschiedliche Kategorien. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Siehe die Liste der Kategorien".

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 sich die Ergebnisse genauer anschauen, stellen Sie möglicherweise fest, dass Mitarbeiterverträge an einem nicht sicheren 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. Wählen Sie im Menü BlueXP Classification die Registerkarte **Compliance** aus.
2. Wählen Sie das Pfeilsymbol **Ergebnisse untersuchen** für eine der Top 4 Kategorien direkt auf dem Hauptbildschirm aus, oder wählen Sie **Alle anzeigen** und wählen Sie dann das Symbol für eine der Kategorien.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, den Pfeil **Ergebnisse untersuchen** auswählen, um maskierte Informationen anzuzeigen, oder indem Sie die Dateiliste herunterladen.

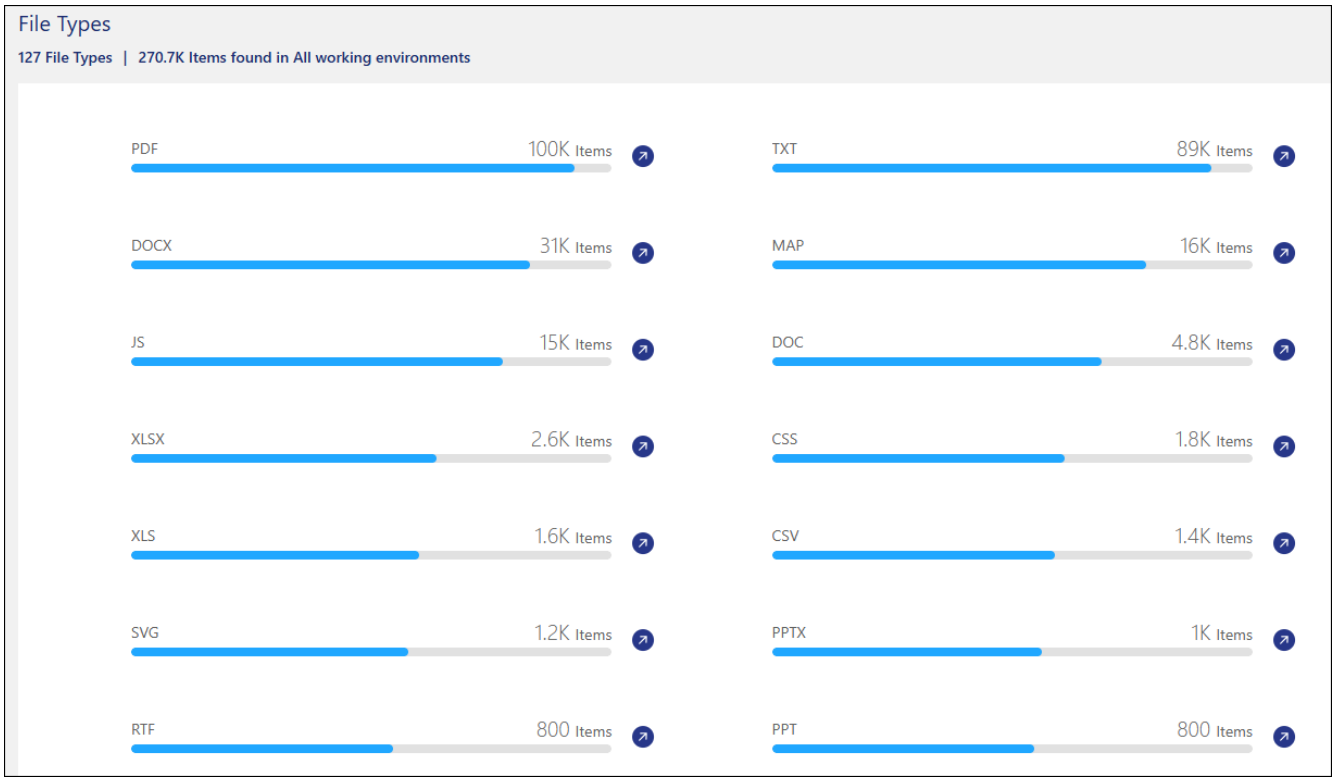
Dateien nach Dateitypen anzeigen

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. Wählen Sie im BlueXP -Klassifizierungsmemu die Registerkarte **Compliance** aus.
2. Wählen Sie das Pfeilsymbol **Ergebnisse untersuchen** für einen der Top 4 Dateitypen direkt auf dem Hauptbildschirm aus, oder wählen Sie **Alle anzeigen** und wählen Sie dann das Symbol für einen der Dateitypen aus.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, den Pfeil **Ergebnisse untersuchen** auswählen, um maskierte Informationen anzuzeigen, oder indem Sie die Dateiliste herunterladen.

Kategorien von privaten Daten in BlueXP -Klassifizierung

Es gibt viele Arten von privaten Daten, die durch die BlueXP Klassifizierung in Ihren Volumes und Datenbanken identifiziert werden können.

Durch die BlueXP Klassifizierung werden zwei Arten von personenbezogenen Daten identifiziert:

- **Personenbezogene Informationen (PII)**
- **Sensible personenbezogene Daten (SPII)**

Wenn Sie zur Identifizierung anderer privater Datentypen eine BlueXP -Klassifizierung benötigen, z. B. zusätzliche nationale ID-Nummern oder Kennungen für das Gesundheitswesen, wenden Sie sich an Ihren Account Manager.

Arten personenbezogener Daten

Die in Dateien enthaltenen personenbezogenen Daten bzw. *personenbezogene Informationen* (PII) können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte der folgenden Tabelle wird angegeben, ob die BlueXP -Klassifizierung zur Validierung der Ergebnisse für die Kennung verwendet"Prüfung der Nähe".

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

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
Allgemein	Kreditkartennummer	Ja.	✓	✓	✓		✓
	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

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch

Typ	Kennung	Näherungsvalidierung?	Englisch	Deutsch	Spanisch	Französisch	Japanisch
	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.	✓	✓	✓		
	UK-ID (NINO)	Ja.	✓	✓	✓		
	USA California Driver’s License	Ja.	✓	✓	✓		
	USA Indiana Führerschein	Ja.	✓	✓	✓		
	USA New York Führerschein	Ja.	✓	✓	✓		
	USA Texas Driver’s License	Ja.	✓	✓	✓		
	USA Sozialversicherungsnummer (SSN)	Ja.	✓	✓	✓		

Arten sensibler personenbezogener Daten

Die BlueXP -Klassifizierung kann folgende sensible personenbezogene Daten (SPII) in Dateien finden.

Die Artikel in dieser Kategorie können derzeit nur auf Englisch erkannt werden.

- **Strafprozessreferenz**: Daten über die strafrechtlichen Verurteilungen und Straftaten einer natürlichen Person.
- **Ethnizitätsreferenz**: Daten über die rassische oder ethnische Herkunft einer natürlichen Person.
- **Gesundheitsreferenz**: Daten über die Gesundheit einer natürlichen Person.
- **ICD-9-CM Medical Codes**: Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.
- **ICD-10-CM Medical 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.
- **Verweise auf religiöse Überzeugungen**: Daten über die religiösen Überzeugungen einer natürlichen Person.
- **Sexualleben oder Orientierungsreferenz**: Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person.

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	✓	✓	✓
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 in denselben unterstützten Sprachen kategorisiert und identifiziert:

- Applikationsdaten
- Archivdateien
- Audio
- Breadcrumbs aus der BlueXP Klassifizierung Daten Von Business-Applikationen
- CAD-Dateien
- Codieren

- Beschädigt
- Datenbank- und Indexdateien
- 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 die BlueXP-Klassifizierung personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt:

`.CSV, .DCM, .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 %

Erstellen Sie eine benutzerdefinierte Klassifizierung in der BlueXP -Klassifizierung

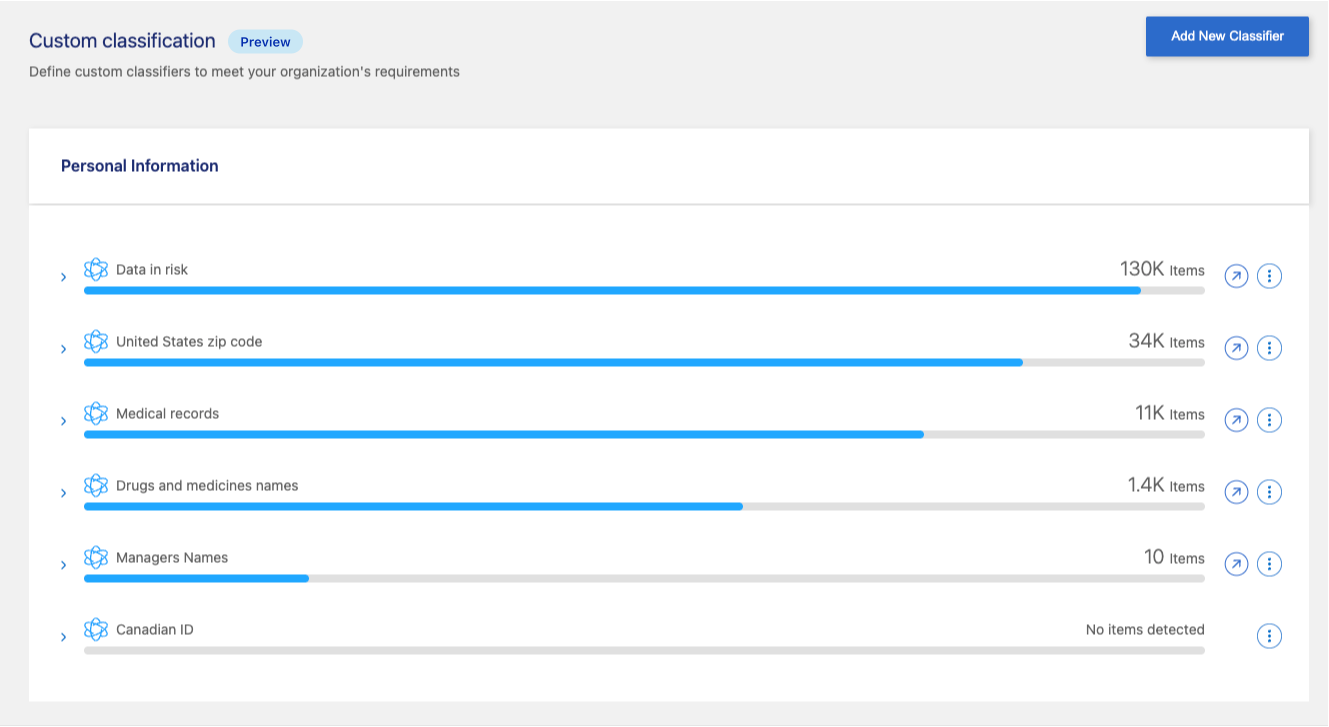
Mit der BlueXP -Klassifizierung können Sie eine benutzerdefinierte Suche nach sensiblen Informationen erstellen. Die Suche kann auf einen regulären Ausdruck (regex) übertragen werden.

Erstellen Sie eine benutzerdefinierte Klassifizierung

Benutzerdefinierte Klassifizierung ist nur für Karten- und Klassifikations-Scans verfügbar, nicht für nur-Mapping-Scans. Diese Funktion befindet sich derzeit in der Vorschau.

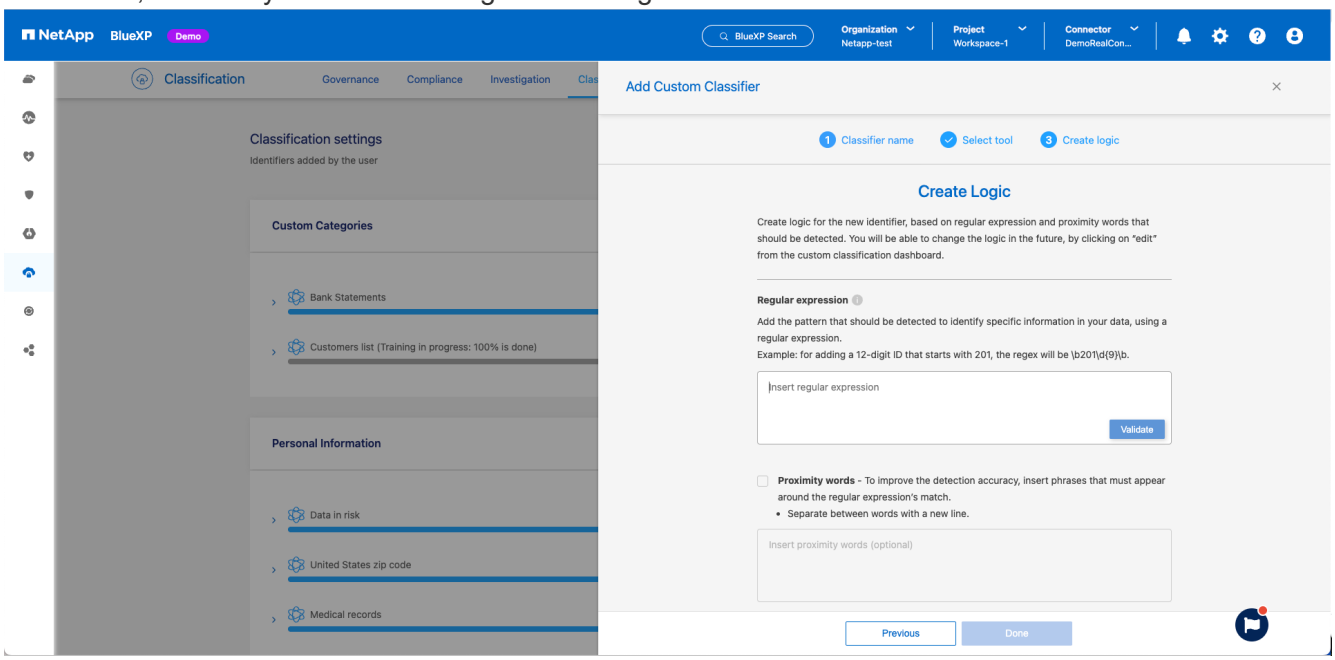
Schritte

1. Wählen Sie die Registerkarte **Benutzerdefinierte Klassifizierung**.



2. Klicken Sie auf die Schaltfläche **Neuen Klassierer hinzufügen**.

3. Fügen Sie einen Namen und eine Beschreibung für den neuen Klassifikator hinzu.
4. Um die Anpassung als regulärer Ausdruck hinzuzufügen, wählen Sie **Benutzerdefinierter regulärer Ausdruck** und dann **Weiter**.
5. Fügen Sie ein Muster hinzu, um die spezifischen Informationen Ihrer Daten zu erkennen. Wählen Sie **Validieren**, um die Syntax Ihres Eintrags zu bestätigen.



6. Wählen Sie **Fertig**, um die benutzerdefinierte Klassifizierung zu erstellen.

Die neue Anpassung wird beim nächsten geplanten Scan erfasst. Informationen zum Anzeigen der Ergebnisse finden Sie unter Erstellen von Compliance-Berichten.

Untersuchen Sie die in Ihrem Unternehmen gespeicherten Daten mit der BlueXP -Klassifizierung

Untersuchen Sie die Daten Ihrer Organisation, indem Sie Details auf der Seite „Datenuntersuchung“ anzeigen. Hier können Sie Ihre Recherche fortsetzen, nachdem Sie sich das Governance Dashboard ansehen. Auf der Seite Untersuchung können Sie die Daten mithilfe eines der vielen Filter filtern, um nur die Ergebnisse anzuzeigen, die Sie anzeigen möchten. Darüber hinaus können Sie Dateimetadaten und Berechtigungen für Dateien und Verzeichnisse anzeigen und nach doppelten Dateien in Ihren Storage-Systemen suchen.

Sie können diese Seite aus vielen Bereichen der BlueXP -Klassifizierungs-UI aufrufen, einschließlich der Governance- und Compliance-Dashboards mit den bereits auf diesen Seiten ausgewählten Filtern. Sie können die Daten in eine CSV- oder JSON-Datei exportieren, um sie weiter zu analysieren oder mit anderen zu teilen.

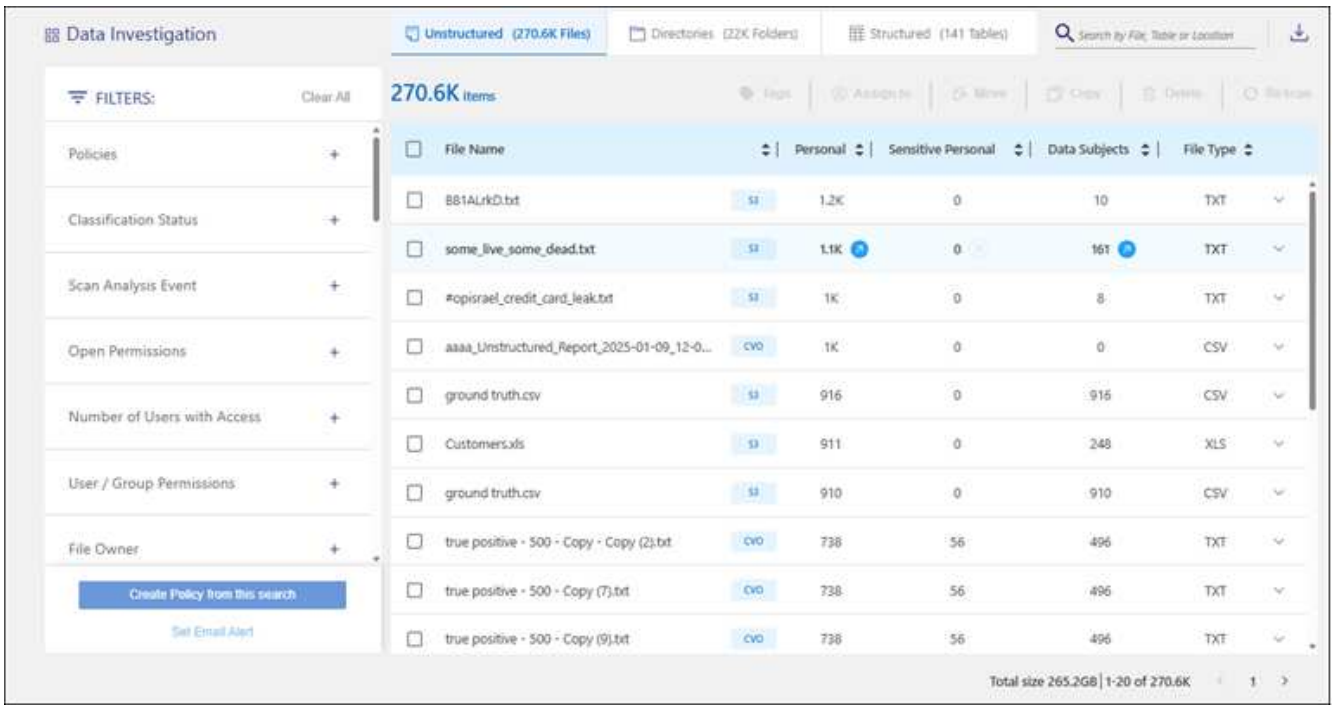
Die in diesem Abschnitt beschriebenen Funktionen sind nur verfügbar, wenn Sie eine vollständige Klassifizierungsprüfung Ihrer Datenquellen durchgeführt haben. Datenquellen, bei denen nur ein Mapping-Scan vorliegt, zeigen keine Details auf Dateiebene an.

Filtern Sie die Daten auf der Seite „Datenuntersuchung“

Sie können den Inhalt der Untersuchungsseite filtern, um nur die Ergebnisse anzuzeigen, die Sie sehen möchten.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option **Untersuchung**.
2. Führen Sie auf der Seite Datenuntersuchung einen der folgenden Schritte aus:
3. Um den Inhalt der Seite nach der Refinierung als Bericht herunterzuladen, klicken Sie auf die Schaltfläche.



4. Um die Daten aus Dateien (unstrukturierte Daten), Verzeichnissen (Ordner und Dateifreigaben) oder Datenbanken (strukturierte Daten) anzuzeigen, wählen Sie oben eine der Registerkarten aus.
5. Um die Ergebnisse in numerischer oder alphabetischer Reihenfolge zu sortieren, wählen Sie das Steuerelement oben in jeder Spalte aus.
6. Um die Ergebnisse noch weiter zu verfeinern, wählen Sie einen der Filter im Filterbereich aus.

Auf der Seite „Datenuntersuchung“ können Sie nur die ersten 10,000 Ergebnisse oder 500 Seiten für einen Scan anzeigen.

Filtern Sie 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 "Arten von Kategorien".
Empfindlichkeitsstufe	Wählen Sie die Empfindlichkeitsstufe aus: Persönlich, sensibel persönlich oder nicht empfindlich.

Filtern	Details
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 Option zur Berechnung der Anzahl der personenbezogenen Daten (PII) nach Verzeichnissen entfernt.
Persönliche Daten	Wählen Sie die "Arten personenbezogener Daten".
Sensible Personenbezogene Daten	Wählen Sie die "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 von Daten nach Benutzereigentümerberechtigungen

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.

Daten nach Zeit filtern

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.

Filtern	Details
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. Die BlueXP Klassifizierung extrahiert nicht den „Zeitpunkt des letzten Zugriffs“ aus den folgenden Datenquellen: SharePoint Online, SharePoint On-Premises (SharePoint Server), OneDrive, Google Drive und Amazon S3.

Daten nach Metadaten filtern

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 "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.

Daten nach Speichertyp filtern

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 von Daten nach gespeicherten Suchen

Verwenden Sie den folgenden Filter, um Daten nach gespeicherten Suchen anzuzeigen.

Filtern	Details
Gespeicherte Suche	Wählen Sie eine gespeicherte Suche oder ein Vielfaches aus. Gehen Sie zum"Registerkarte gespeicherte Suchen", um die Liste der vorhandenen gespeicherten Suchen anzuzeigen und neue zu erstellen.

Daten nach Analysestatus filtern

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.

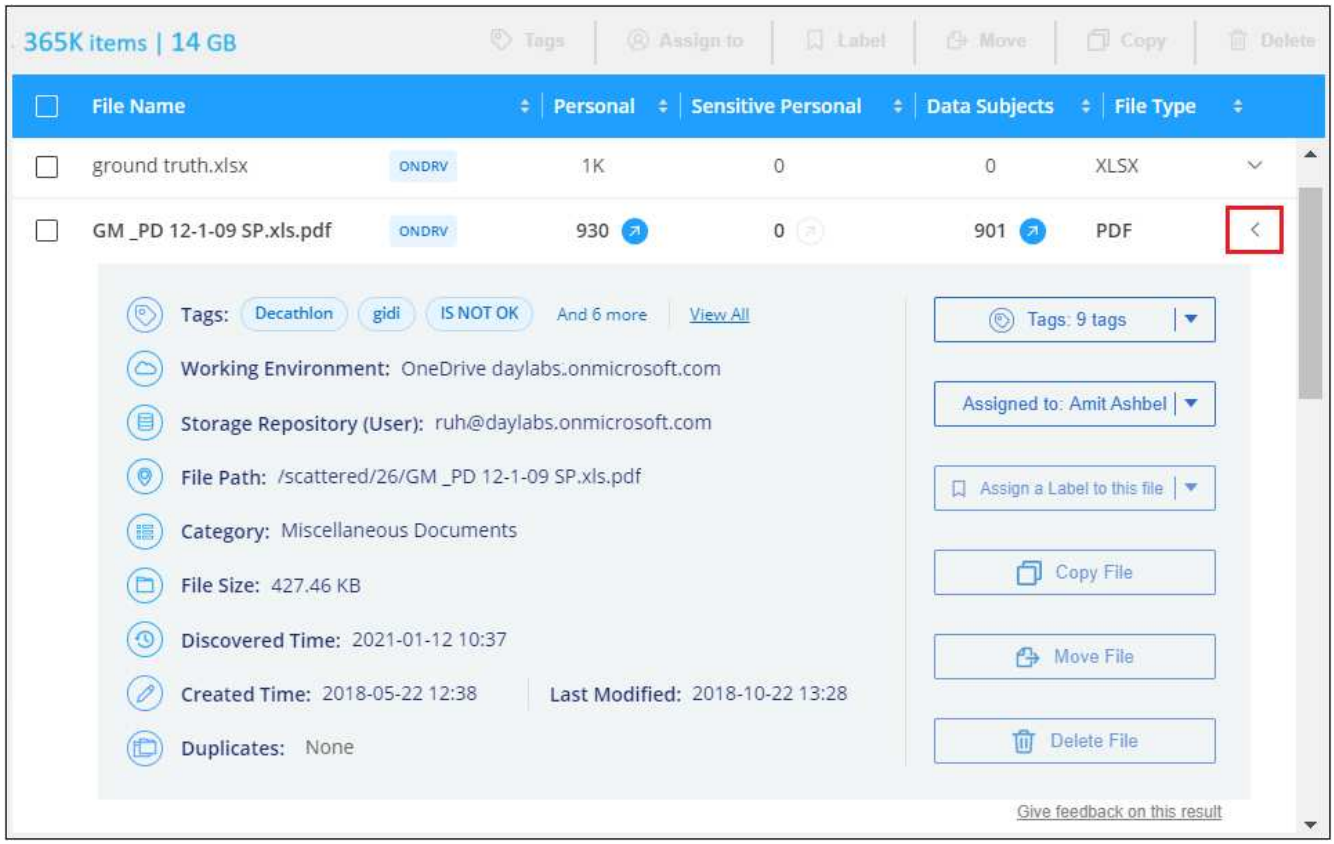
Anzeigen von Datei-Metadaten

Sie sehen nicht nur die Arbeitsumgebung und das Volume, in dem sich die Datei befindet, sondern auch viel mehr Informationen, wie etwa die Dateiberechtigungen oder der Dateieigentümer und ob Duplikate dieser Datei vorliegen. Diese Informationen sind nützlich, wenn Sie planen"Erstellen Sie gespeicherte Suchen", weil Sie alle Informationen sehen können, die Sie zum Filtern Ihrer Daten verwenden können.

Die Verfügbarkeit von Informationen hängt von der Datenquelle ab. Beispielsweise werden Volumename und Berechtigungen für Datenbankdateien nicht freigegeben.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option **Untersuchung**.
2. Wählen Sie in der Liste Datenuntersuchung auf der rechten Seite das Down-Caret für jede einzelne Datei aus, um die Metadaten der Datei anzuzeigen.



Benutzerberechtigungen für Dateien und Verzeichnisse anzeigen

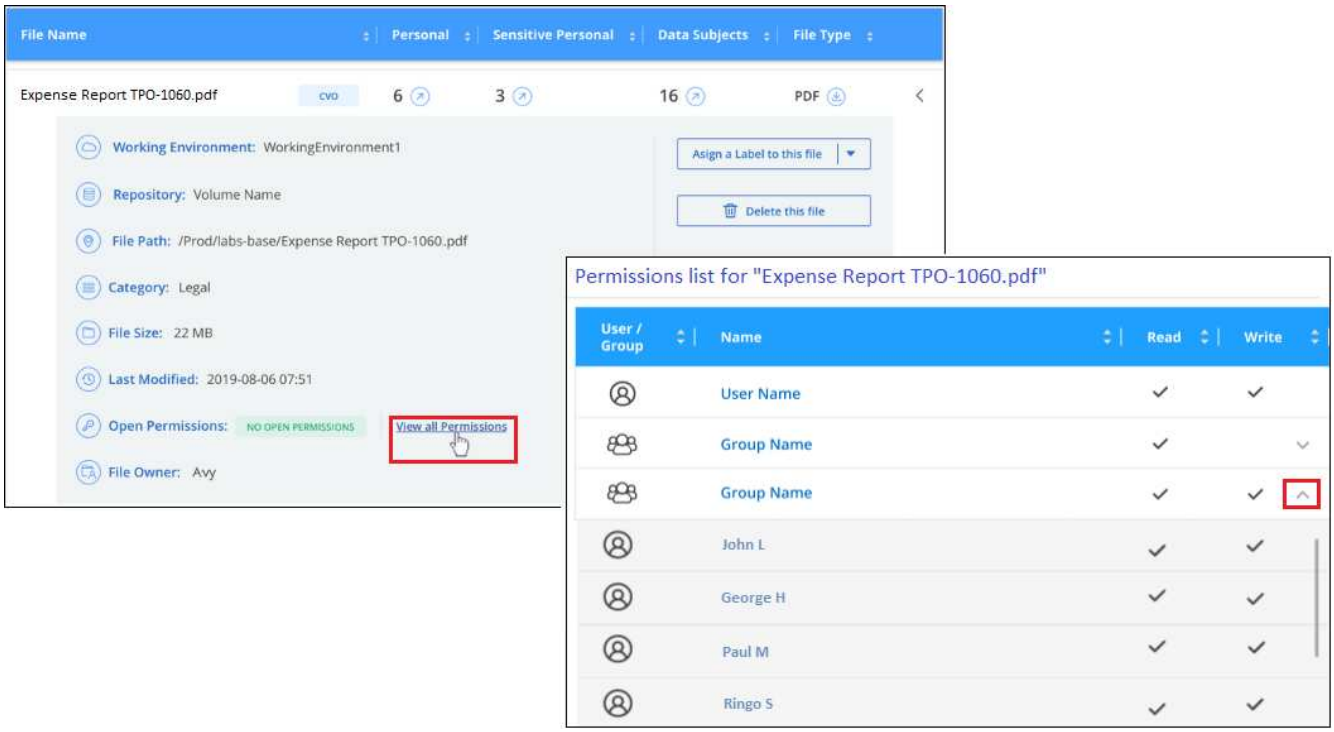
Wenn Sie eine Liste aller Benutzer oder Gruppen anzeigen möchten, die Zugriff auf eine Datei oder ein Verzeichnis haben, wählen Sie **Alle Berechtigungen anzeigen**. Diese Schaltfläche ist nur für Daten in CIFS-Freigaben verfügbar.

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

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option **Untersuchung**.
2. Wählen Sie in der Liste Datenuntersuchung auf der rechten Seite das Down-Caret für jede einzelne Datei aus, um die Metadaten der Datei anzuzeigen.
3. 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, wählen Sie im Feld Offene Berechtigungen die Option **Alle Berechtigungen anzeigen**.

Die BlueXP -Klassifizierung zeigt bis zu 100 Benutzer in der Liste.



4. Wählen Sie die Schaltfläche Down-Caret für jede Gruppe aus, um die Liste der Benutzer anzuzeigen, die Teil der Gruppe sind.

Sie können eine Ebene der Gruppe erweitern, um die Benutzer anzuzeigen, die Teil der Gruppe sind.

5. Wählen Sie den Namen eines Benutzers oder einer Gruppe aus, um die Untersuchungsseite zu aktualisieren, damit 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 überprüfen, ob in Ihren Speichersystemen doppelte Dateien gespeichert werden. Dies ist nützlich, wenn Sie Bereiche ermitteln möchten, in denen Sie Speicherplatz einsparen können. Stellen Sie außerdem sicher, dass bestimmte Dateien mit bestimmten Berechtigungen oder vertraulichen Informationen nicht unnötig dupliziert werden.

Alle Ihre Dateien (ohne Datenbanken), die 1 MB oder größer sind oder persönliche oder sensible personenbezogene Daten enthalten, werden verglichen, um zu sehen, ob es Duplikate gibt.

Die BlueXP Klassifizierung verwendet Hashing-Technologie, um doppelte Dateien zu ermitteln. Wenn eine Datei denselben Hashcode wie eine andere Datei hat, können Sie 100 % sicher sein, dass es sich bei den Dateien um exakte Duplikate handelt – auch wenn die Dateinamen unterschiedlich sind.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option **Untersuchung**.
2. Wählen Sie im Bereich Filter auf der Seite Untersuchung links „Dateigröße“ zusammen mit „Duplikate“ („hat Duplikate“) aus, um zu sehen, welche Dateien eines bestimmten Größenbereichs in Ihrer Umgebung dupliziert werden.
3. Optional laden Sie die Liste der doppelten Dateien herunter und senden Sie sie an Ihren Speicheradministrator, damit Sie entscheiden können, welche Dateien, falls vorhanden, gelöscht werden

können.

4. Sie können sich auch "Löschen Sie die Datei"selbst dann selbst darum kümmern, wenn Sie sicher sind, dass eine bestimmte Version der Datei nicht benötigt wird.

Anzeigen, wenn eine bestimmte Datei dupliziert ist

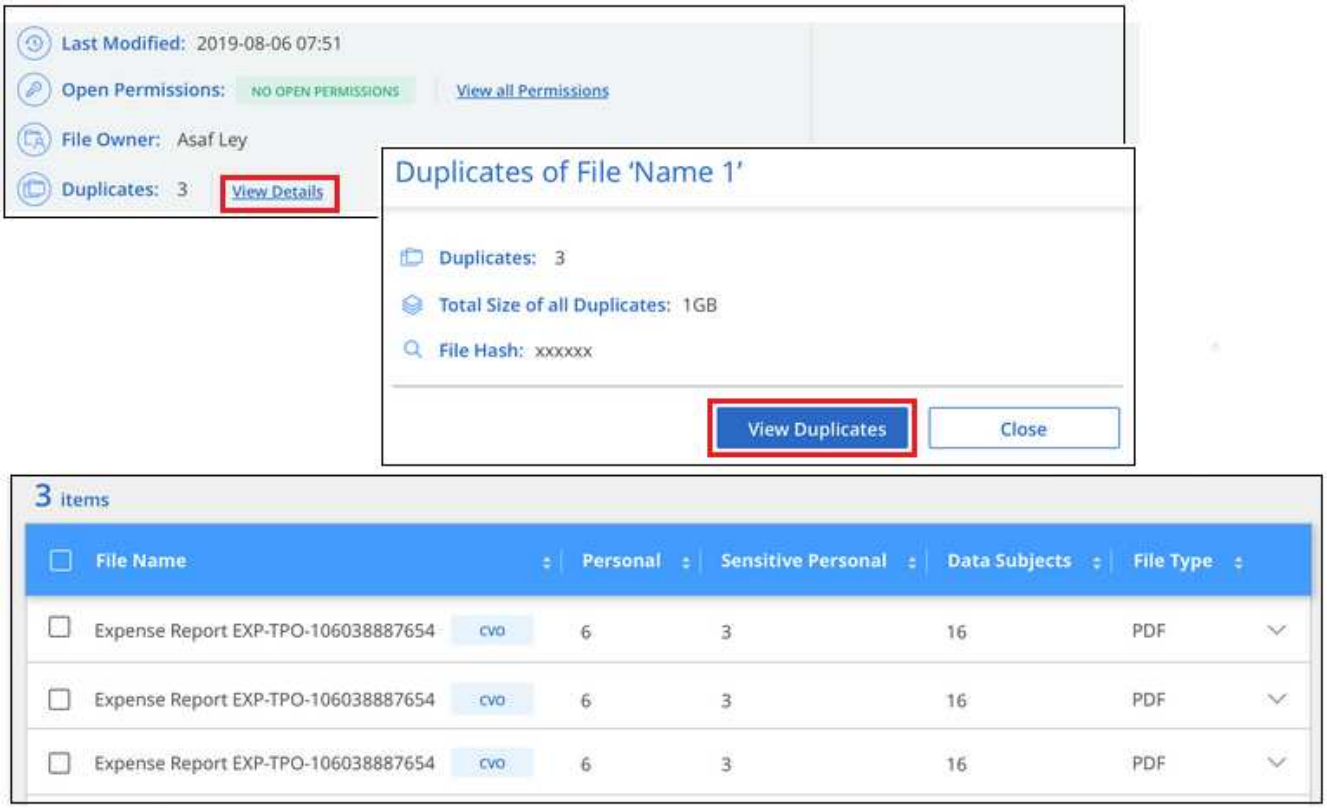
Sie können sehen, ob eine einzelne Datei Duplikate enthält.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option **Untersuchung**.
2. Wählen Sie in der Liste Datenuntersuchung rechts für eine einzelne Datei aus, um die Dateimetadaten anzuzeigen.

   Wenn für eine Datei Duplikate vorhanden sind, wird diese Information neben dem Feld *Duplikate* angezeigt.

3. Um die Liste der doppelten Dateien anzuzeigen und wo sie sich befinden, wählen Sie **Details anzeigen**.
4. Wählen Sie auf der nächsten Seite **Duplikate anzeigen**, um die Dateien auf der Seite Untersuchung 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 diese in einer gespeicherten Suche verwenden.

Erstellen Sie den Datenermittlungsbericht

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

Der Bericht ist als CSV- oder JSON-Datei verfügbar, die Sie auf Ihrem lokalen Computer speichern können.

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

Die Dateien werden in Dateien mit einer festen Anzahl von Zeilen oder Datensätzen aufgeteilt:

- JSON – 100.000 Datensätze pro Bericht, dessen Generierung etwa 5 Minuten dauert
- CSV – 200.000 Datensätze pro Bericht, dessen Generierung etwa 4 Minuten dauert

> Sie können eine Version der CSV-Datei herunterladen, um sie in diesem Browser anzuzeigen. Diese Version ist auf 10,000 Datensätze beschränkt.

Was ist im Untersuchungsbericht 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
  - Die Dateieigentümerdaten umfassen den Kontonamen, den SAM-Kontonamen und die E-Mail-Adresse, wenn Active Directory konfiguriert ist.
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten
- Berechtigungen öffnen
- Fehler Bei Der Scananalyse
- Löscherkennung Datum

  Das Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. So können Sie feststellen, wann sensible Dateien verschoben wurden. Gelöschte Dateien werden nicht in die Dateianzahl im Dashboard oder auf der Seite „Untersuchung“ einbezogen. 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:

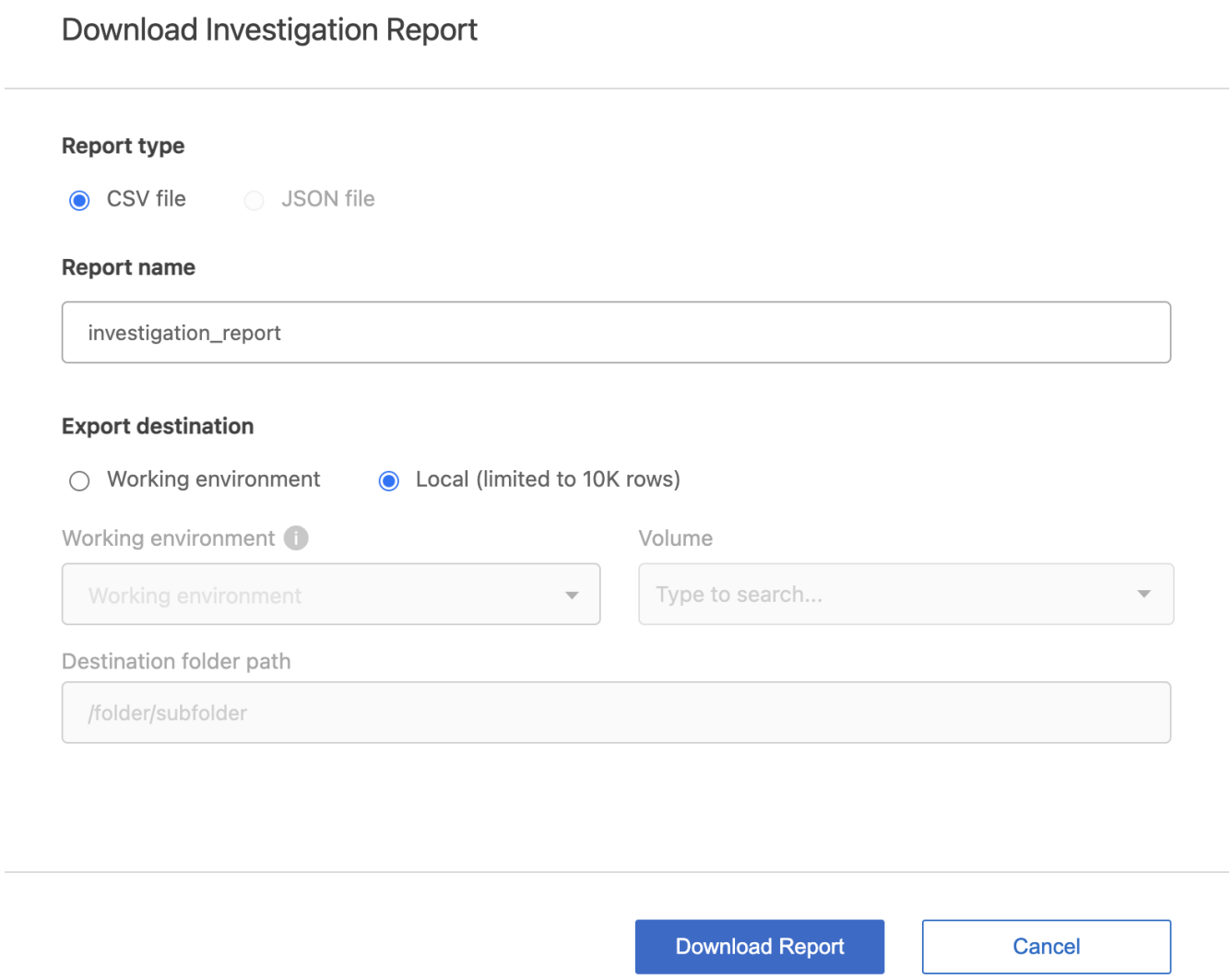
- DB-Tabellenname
- Positionstyp
- Name der Arbeitsumgebung
- Storage-Repository (z. B. ein Schema)
- Anzahl der Spalten
- Zeilenanzahl
- Persönliche Angaben
- Sensible persönliche Daten

Schritte zum Generieren des Berichts

1. Wählen Sie auf der Seite Datenuntersuchung die Schaltfläche oben rechts auf der Seite aus.
2. Wählen Sie den Berichtstyp: CSV oder JSON.
3. Geben Sie einen **Berichtsnamen** ein.
4. Um den vollständigen Bericht herunterzuladen, wählen Sie **Arbeitsumgebung** und dann die Optionen **Arbeitsumgebung** und **Volumen** aus den jeweiligen Dropdown-Menüs. Geben Sie einen Pfad für den Zielordner** an.

   Um den Bericht im Browser herunterzuladen, wählen Sie **Lokal** . Beachten Sie, dass diese Option den Bericht auf die ersten 10,000 Zeilen beschränkt und auf das Format **CSV** beschränkt ist. Sie müssen keine anderen Felder ausfüllen, wenn Sie **Lokal** auswählen.

5. Wählen Sie **Bericht Herunterladen**.



Ergebnis

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

Erstellen Sie eine gespeicherte Suche basierend auf ausgewählten Filtern

Sie können auf der Seite „Datenuntersuchung“ eine gespeicherte Suche nach häufig verwendeten Suchfiltern erstellen, um diese Suchabfragen problemlos zu replizieren.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option **Untersuchung**.
2. Wählen Sie auf der Seite Datenuntersuchung die Filter aus, die Sie zum Erstellen einer gespeicherten Suche verwenden möchten.
3. Wählen Sie unten im Filterfenster **gespeicherte Suche aus dieser Suche erstellen**.
4. Geben Sie einen Namen und eine Beschreibung für die gespeicherte Suche ein.
5. Wählen Sie eine der folgenden Optionen:
6. Wählen Sie **Gespeicherte Suche Erstellen**.

Es kann bis zu 15 Minuten dauern, bis die Ergebnisse auf der Seite „gespeicherte Suchen“ angezeigt werden.

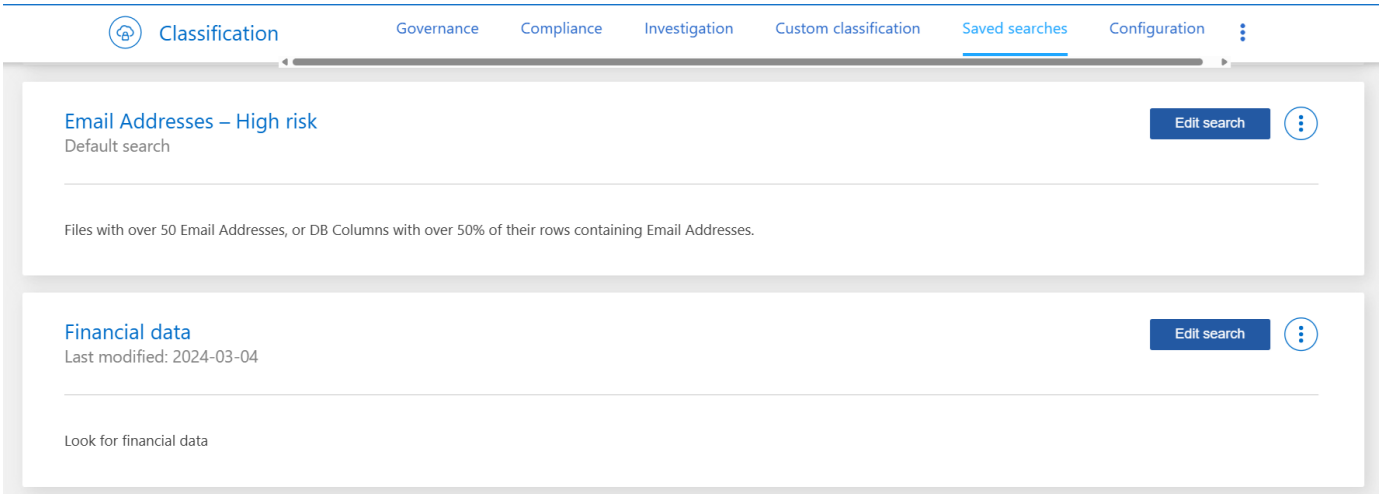
Verwalten Sie gespeicherte Suchen mit BlueXP - Klassifizierung

Die BlueXP -Klassifizierung unterstützt das Speichern Ihrer Suchanfragen. Mit einer gespeicherten Suche können Sie benutzerdefinierte Filter erstellen, um häufige Abfragen Ihrer Datenermittlungsseite zu durchsuchen. Die BlueXP -Klassifizierung umfasst außerdem vordefinierte gespeicherte Suchen auf der Basis gängiger Anforderungen.

In Versionen der BlueXP -Klassifizierung vor 1.43 wurden gespeicherte Suchen aufgerufenRichtlinien.

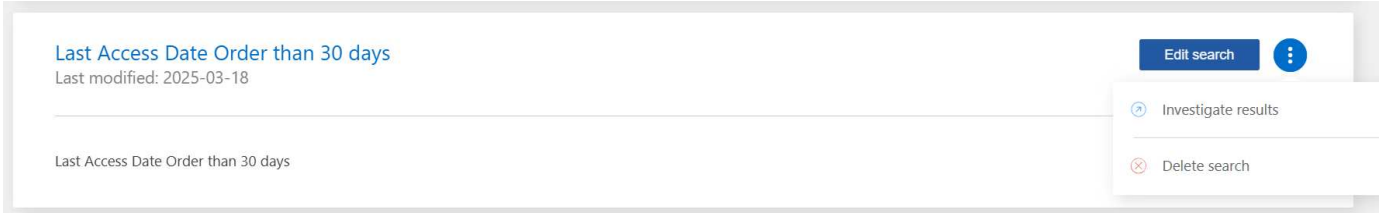
Auf der Registerkarte **gespeicherte Suchen** im Compliance-Dashboard werden alle vordefinierten und benutzerdefinierten gespeicherten Suchen aufgelistet, die für diese Instanz der BlueXP -Klassifizierung verfügbar sind.

Gespeicherte Suchen werden auch in der Liste der Filter auf der Seite Untersuchung angezeigt.



Zeigen Sie die gespeicherten Suchergebnisse auf der Seite Untersuchung an

Um die Ergebnisse für eine gespeicherte Suche auf der Untersuchungsseite anzuzeigen, klicken Sie auf die Schaltfläche für eine bestimmte Suche und wählen Sie dann **Ergebnisse untersuchen**.

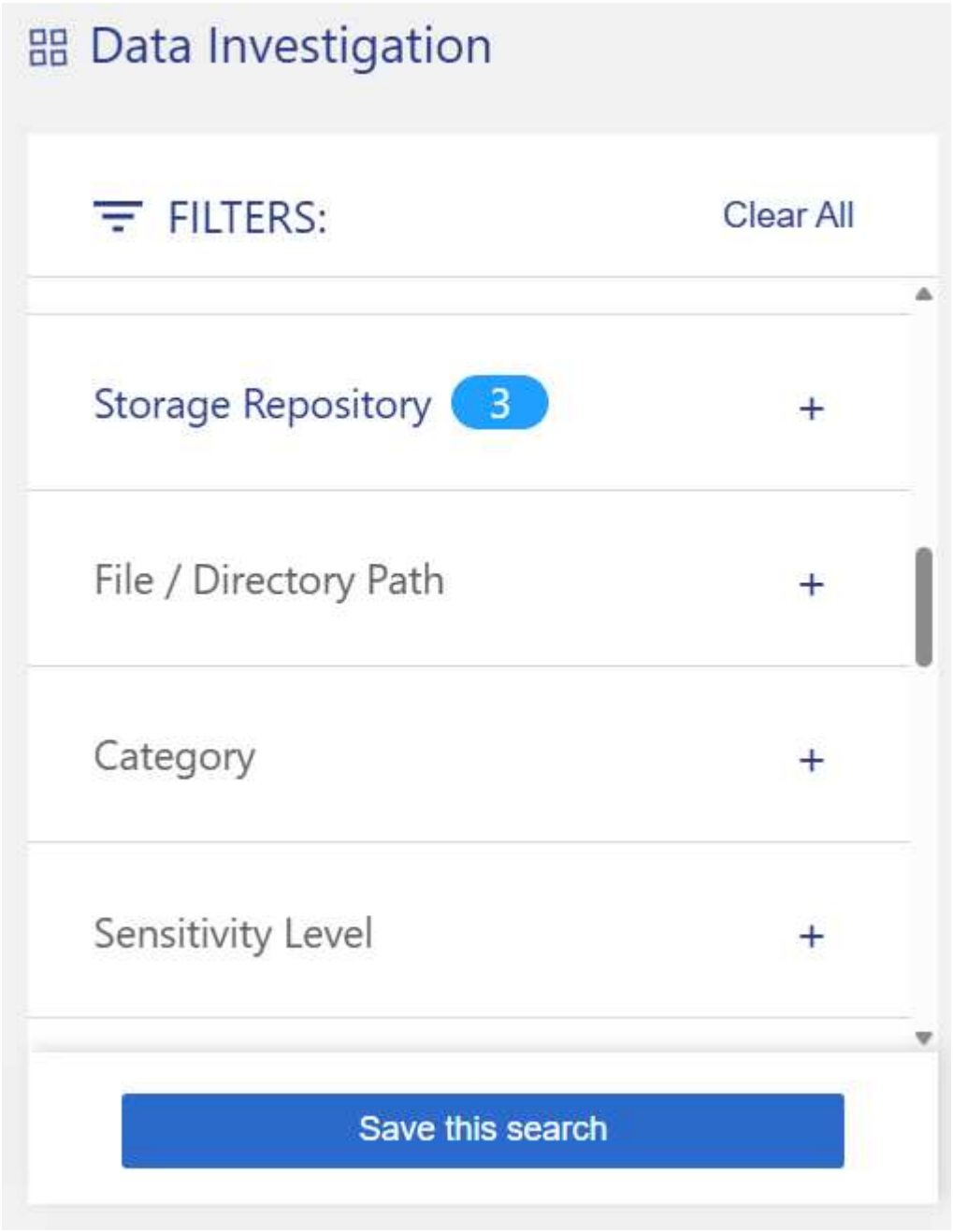


Erstellen Sie benutzerdefinierte gespeicherte Suchen

Sie können Ihre eigenen benutzerdefinierten gespeicherten Suchen erstellen, die Ergebnisse für die für Ihr Unternehmen spezifischen Abfragen liefern. Die Ergebnisse werden für alle Dateien und Verzeichnisse (Freigaben und Ordner) zurückgegeben, die den Suchkriterien entsprechen.

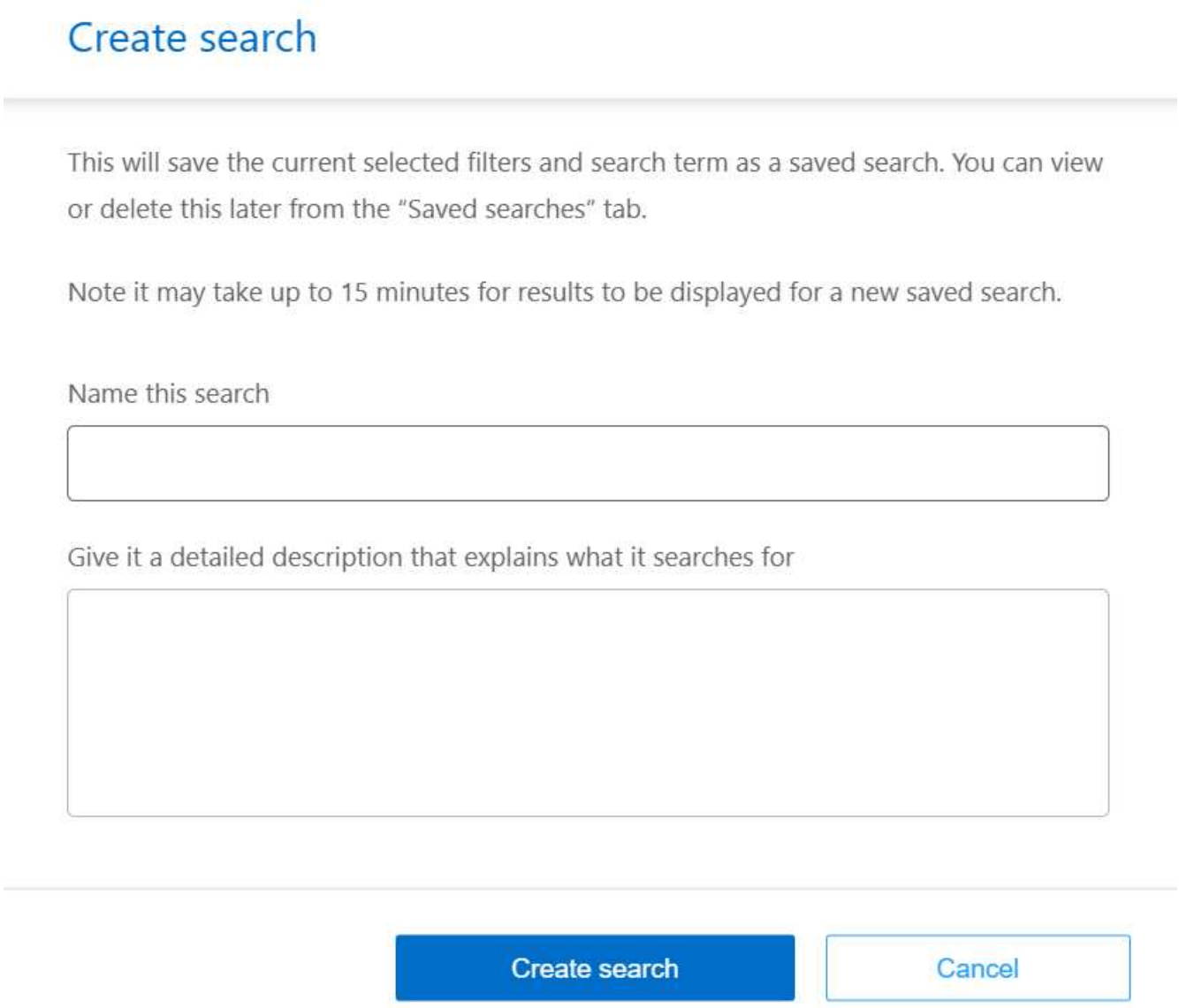
Schritte

1. Definieren Sie auf der Registerkarte Untersuchung eine Suche, indem Sie die gewünschten Filter auswählen. Weitere Informationen finden Sie unter "Filtern von Daten auf der Untersuchungsseite" .
2. Wenn Sie alle Filtereigenschaften nach Ihren Wünschen eingestellt haben, wählen Sie **gespeicherte Suche erstellen**.



3. Benennen Sie die gespeicherte Suche und fügen Sie eine Beschreibung hinzu. Der Name muss eindeutig sein.

4. Wählen Sie **Gespeicherte Suche Erstellen**.



Nachdem Sie die Suche erstellt haben, können Sie sie auf der Registerkarte **gespeicherte Suchen** anzeigen.

Bearbeiten Sie gespeicherte Suchen

Sie können die Abfragekriterien für eine gespeicherte Suche (d. h. die definierten Filter) ändern, um bestimmte Parameter hinzuzufügen oder zu entfernen.

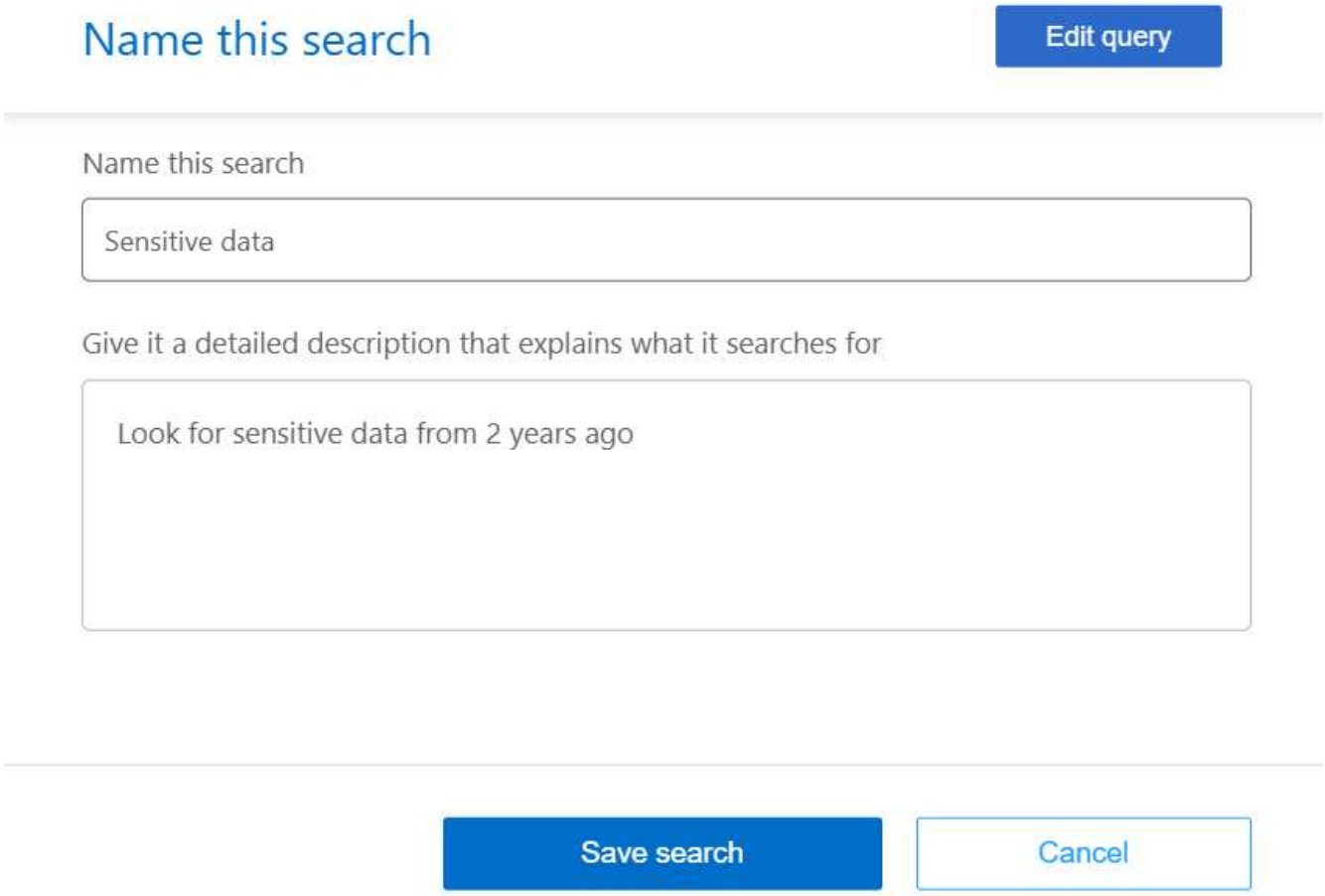
Standardmäßig gespeicherte Suchen können nicht geändert werden.

Schritte

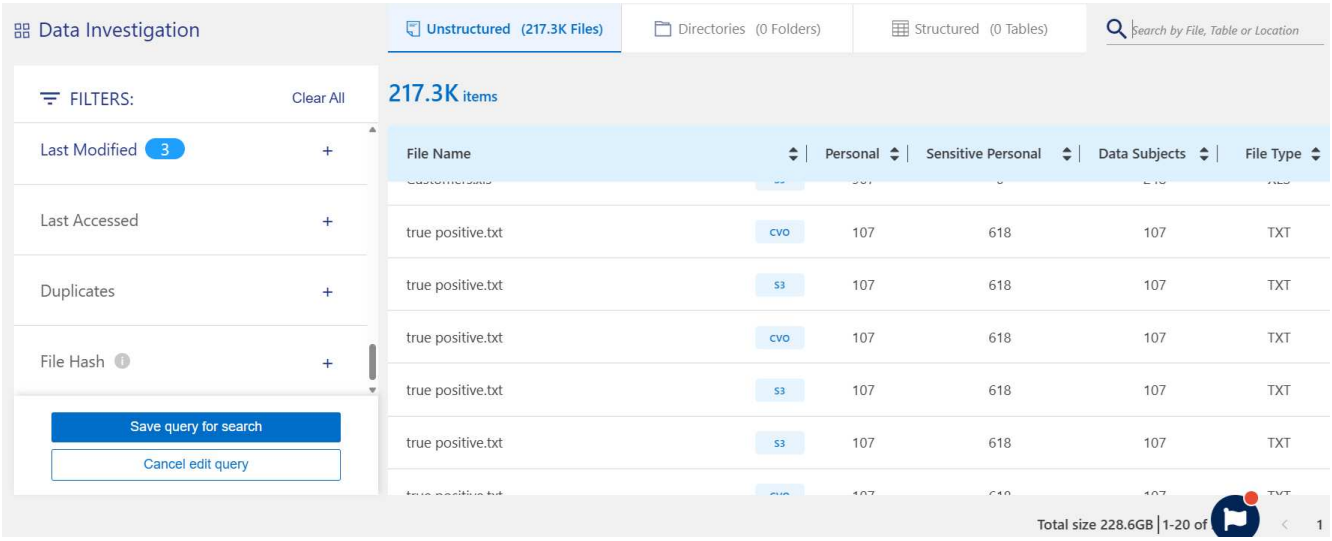
1. Wählen Sie auf der Seite gespeicherte Suchen die Option **Suche bearbeiten** für die Suche aus, die Sie ändern möchten.

2. Nehmen Sie die Änderungen an den Feldern Name und Beschreibung vor. Um nur die Namen- und Beschreibungsfelder zu ändern, wählen Sie **Suche speichern**.

   Um die Filter für die gespeicherte Suche zu ändern, wählen Sie **Abfrage bearbeiten**.



3. Bearbeiten Sie die Abfrage auf der Seite Untersuchung. Sie können Filter hinzufügen, entfernen oder ändern. Um Ihre Änderungen abzuschließen, wählen Sie **Abfrage für diese Suche speichern**.



Löschen Sie gespeicherte Suchen

Sie können jede benutzerdefinierte gespeicherte Suche löschen, wenn Sie sie nicht mehr benötigen. Standardmäßig gespeicherte Suchen können nicht gelöscht werden.

Um eine gespeicherte Suche zu löschen, klicken Sie auf die Schaltfläche für eine bestimmte Suche, wählen Sie **Suche löschen**, und wählen Sie dann im Bestätigungsdialog erneut **Suche löschen** aus.

Standardsuche

BlueXP Classification bietet die folgenden systemdefinierten Suchabfragen:

- **Namen der betroffenen Personen - hohes Risiko**

  Dateien mit mehr als 50 betroffenen Personen

- **E-Mail-Adressen - hohes Risiko**

  Dateien mit mehr als 50 E-Mail-Adressen oder Datenbankspalten mit mehr als 50 % ihrer Zeilen, die E-Mail-Adressen enthalten

- **Persönliche Daten - hohes Risiko**

  Dateien mit mehr als 20 Kennungen persönlicher Daten oder Datenbankspalten mit mehr als 50 % ihrer Zeilen, die persönliche Daten-Kennungen enthalten

- **Private Daten - seit 7 Jahren veraltet**

  Dateien, die persönliche oder sensible personenbezogene Daten enthalten, zuletzt vor mehr als 7 Jahren geändert

- **Schutz - Hoch**

  Dateien oder Datenbankspalten, die ein Passwort, Kreditkarteninformationen, IBAN-Nummer oder Sozialversicherungsnummer enthalten

- **Schutz - Niedrig**

Dateien, auf die seit mehr als 3 Jahren nicht mehr zugegriffen wird

- **Protect - Mittel**

  Dateien, die Dateien oder Datenbankspalten mit persönlichen Datenkennungen enthalten, einschließlich ID-Nummern, Steueridentifikationsnummern, Führerscheinnummern, medizinische IDs oder Passnummern

- **Sensible personenbezogene Daten - hohes Risiko**

  Dateien mit mehr als 20 Identifikatoren für sensible personenbezogene Daten oder Datenbankspalten mit mehr als 50 % ihrer Zeilen, die sensible personenbezogene Daten enthalten

Ändern Sie die Scaneinstellungen für die BlueXP - Klassifizierung für Ihre Repositorys

Sie können managen, wie Ihre Daten in jeder Ihrer Arbeitsumgebungen und Datenquellen gescannt werden. Sie können die Änderungen auf Repository-Basis vornehmen. Dies bedeutet, dass Sie je nach Art der zu scannenden Datenquelle Änderungen für jedes Volume, Schema, jeden Benutzer usw. vornehmen können.

Einige der Dinge, die Sie ändern können, sind, ob ein Repository gescannt wird oder nicht, und ob BlueXP Klassifizierung führt eine "Mapping-Scan oder Mapping Klassifizierungsscan". Sie können den Scanvorgang auch anhalten und fortsetzen, beispielsweise, wenn Sie das Scannen eines Volumens für einen bestimmten Zeitraum beenden müssen.

Anzeigen des Scanstatus für Ihre Repositorys

Sie können die einzelnen Repositorys anzeigen, die von der BlueXP Klassifizierung gescannt werden (Volumes, Buckets usw.), für jede Arbeitsumgebung und Datenquelle. Außerdem können Sie sehen, wie viele "zugeordnet" wurden und wie viele "klassifiziert" wurden. Die Klassifizierung dauert länger, wenn für alle Daten die vollständige KI-Identifizierung durchgeführt wird.

Sie können den Scanstatus jeder Arbeitsumgebung auf der Konfigurationsseite anzeigen:

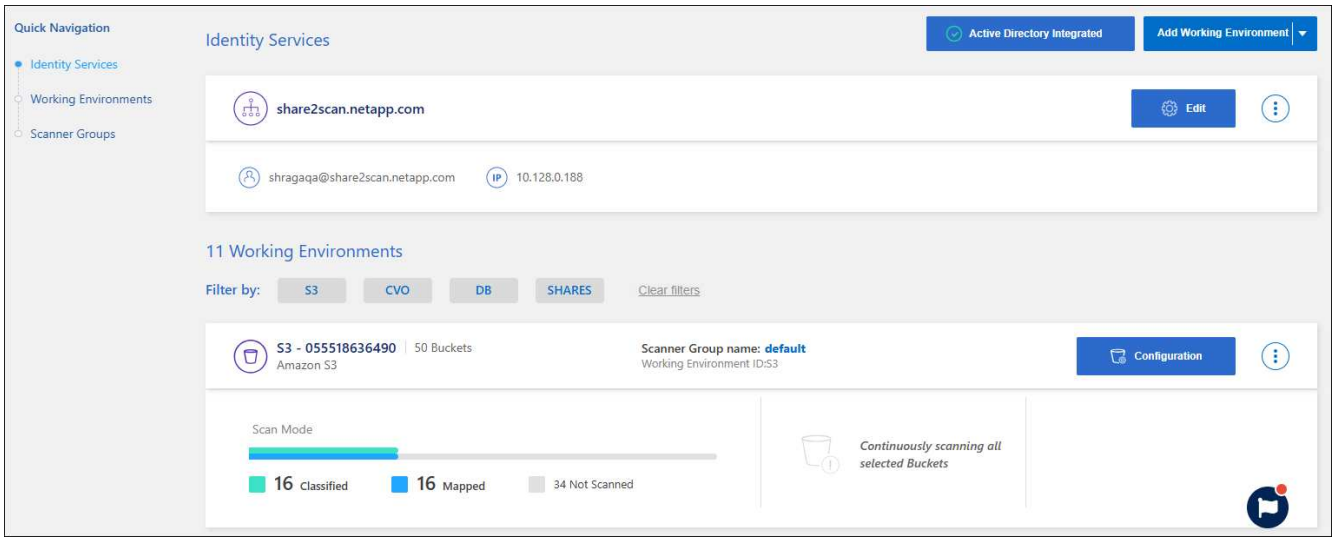
- **Initialisieren** (hellblauer Punkt): Die Map- oder Klassifikationskonfiguration ist aktiviert. Dieser erscheint einige Sekunden lang, bevor der Status „Warteschlange ausstehend“ gestartet wird.
- **Warteschlange ausstehend** (orangefarbener Punkt): Der Scan-Task wartet darauf, in der Scanwarteschlange aufgelistet zu werden.
- **Queued** (orangefarbener Punkt): Die Aufgabe wurde erfolgreich zur Scanwarteschlange hinzugefügt. Das System beginnt mit der Zuordnung oder Klassifizierung des Volumes, wenn es an der Reihe ist.
- **Running** (grüner Punkt): Der Scan-Task, der sich in der Warteschlange befand, wird im ausgewählten Speicher-Repository aktiv ausgeführt.
- **Finished** (grüner Punkt): Der Scan des Speicherarchivs ist abgeschlossen.
- **Pause** (grauer Punkt): Sie haben die Option „Pause“ gewählt, um den Scanvorgang anzuhalten. Während die Änderungen im Volumen nicht im System angezeigt werden, werden die gescannten Erkenntnisse weiterhin angezeigt.
- **Fehler** (roter Punkt): Der Scan kann nicht abgeschlossen werden, da Probleme aufgetreten sind. Wenn Sie eine Aktion abschließen müssen, wird der Fehler in der QuickInfo unter der Spalte „erforderliche Aktion“ angezeigt. Andernfalls zeigt das System einen „Fehler“-Status an und versucht wiederherzustellen.

Nach Abschluss ändert sich der Status.

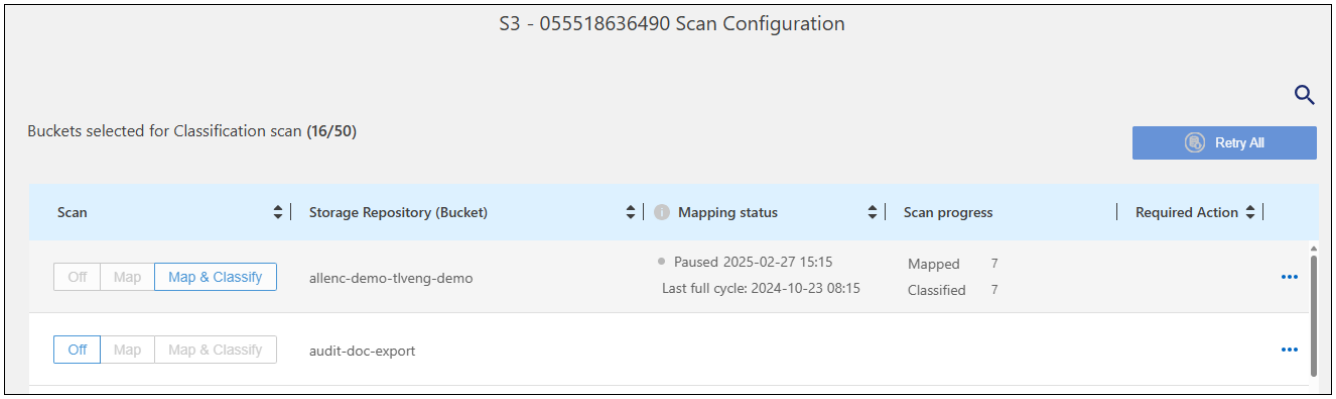
- **Not Scanning**: Die Volumenkonfiguration von "Off" wurde ausgewählt und das System scannt nicht das Volume.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.



2. Wählen Sie auf der Registerkarte Konfiguration die Schaltfläche **Konfiguration** für die Arbeitsumgebung aus.
3. Zeigen Sie auf der Seite Scankonfiguration die Scaneinstellungen für alle Repositorys an.



4. Bewegen Sie den Mauszeiger über das Diagramm in der Spalte *Mapping Status*, um die Anzahl der Dateien anzuzeigen, die in jedem Repository (Bucket in diesem Beispiel) noch zugeordnet oder klassifiziert werden sollen.

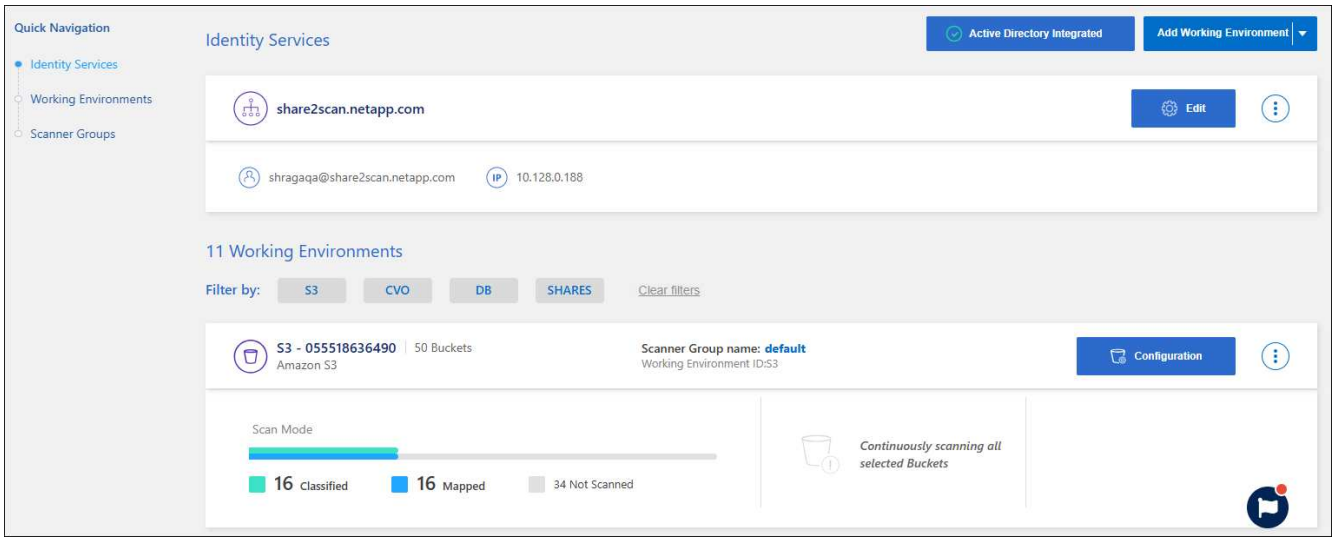
Ändern Sie den Typ der Suche nach einem Repository

Sie können jederzeit auf der Konfigurationsseite Scans oder Scans von nur-Zuordnungen oder Klassifizierungen in einer Arbeitsumgebung starten oder stoppen. Sie können auch von mappingonly Scans zu Mapping- und Klassifizierungsscans und umgekehrt wechseln.

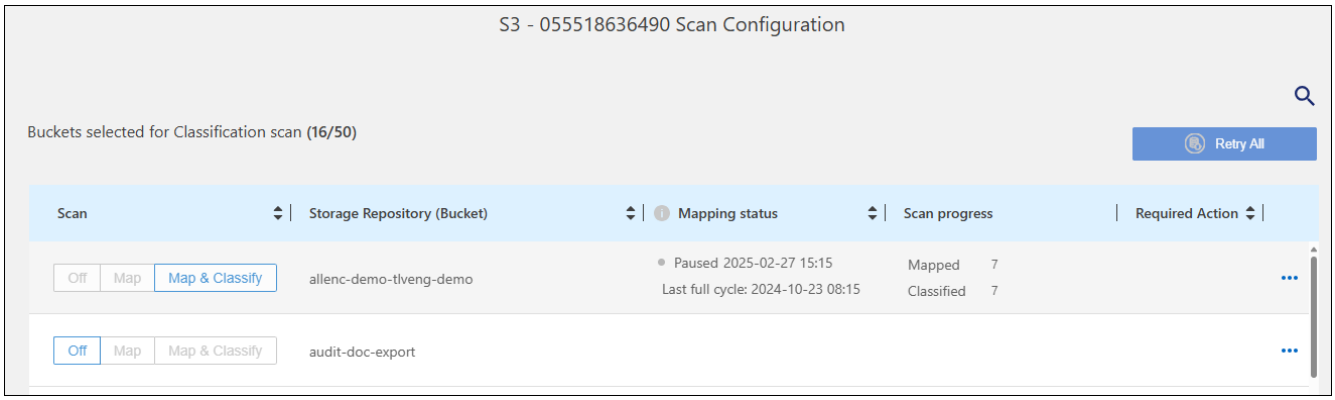
Datenbanken können nicht auf mapping-only Scans gesetzt werden. Das Scannen von Datenbanken kann deaktiviert oder aktiviert sein; wobei ein dem Kartenwert und Klassifizieren entspricht.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Registerkarte Konfiguration die Schaltfläche **Konfiguration** für die Arbeitsumgebung aus.

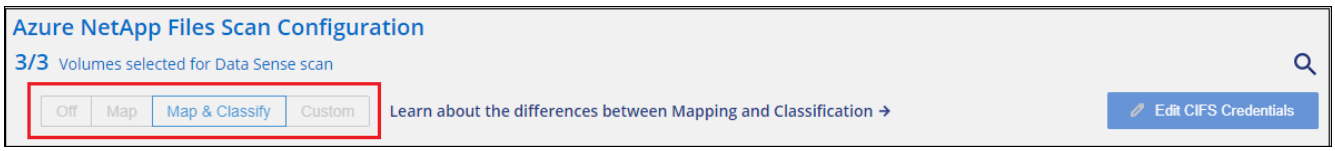


3. Ändern Sie auf der Seite Scankonfiguration eines der Repositories (in diesem Beispiel Buckets), um **Map** oder **Map & Classify**-Scans durchzuführen.



Bestimmte Arbeitsumgebungen ermöglichen es Ihnen, den Scantyp global für alle Repositories über eine Tastenleiste oben auf der Seite zu ändern. Dies gilt für Cloud Volumes ONTAP, On-Premises ONTAP, Azure NetApp Files und Amazon FSX für ONTAP Systeme.

Das folgende Beispiel zeigt diese Tastenleiste für ein Azure NetApp Files System.



Priorisieren Sie Scans

Sie können die wichtigsten nur-Mapping-Scans priorisieren oder Scans zuordnen und klassifizieren, um sicherzustellen, dass Scans mit hoher Priorität zuerst abgeschlossen werden.

Standardmäßig werden Scans basierend auf der Reihenfolge, in der sie initiiert werden, in die Warteschlange gestellt. Mit der Möglichkeit, Scans zu priorisieren, können Sie Scans an die Vorderseite der Warteschlange verschieben. Mehrere Scans können priorisiert werden. Die Priorität wird in der Reihenfolge „First-in“, „First-Out“ festgelegt. Das bedeutet, dass der erste von Ihnen priorisierte Scan an den Anfang der Warteschlange geht. Der zweite priorisierte Scan wird in der Warteschlange und so weiter.

Die Prioritätsachse wird einmalig vergeben. Automatische Neuscans von Zuordnungsdaten erfolgen in der Standardreihenfolge.

Schritte

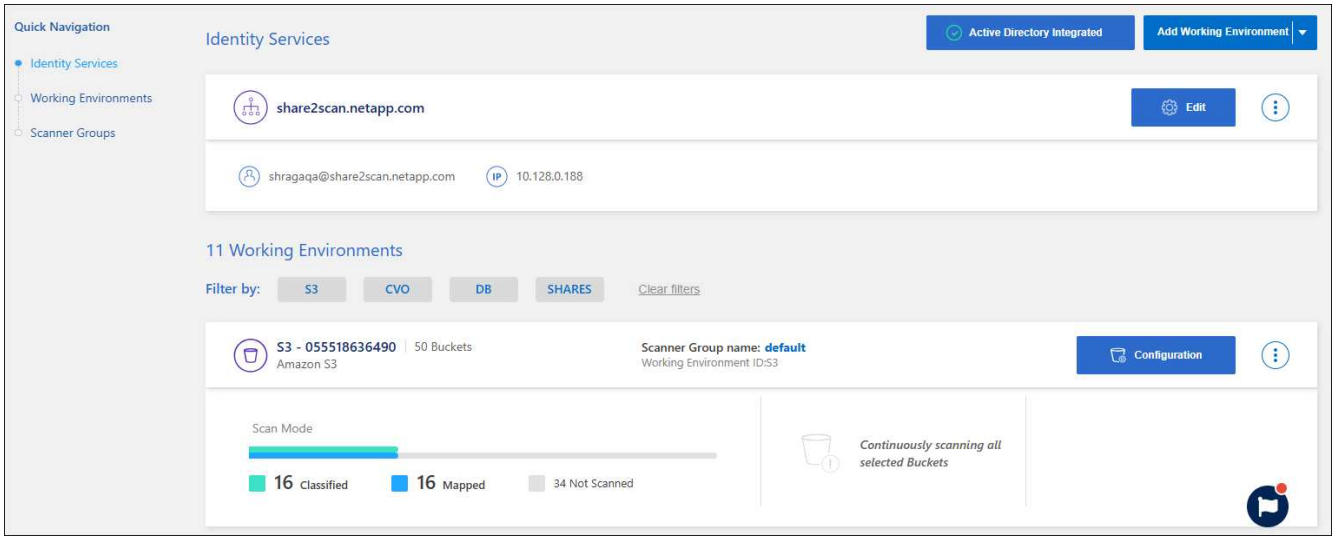
1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie die Ressourcen aus, die Sie priorisieren möchten.
3. Wählen Sie aus der Option Aktionen … die Option **priorisiere Scan**.

Beenden Sie die Suche nach einem Repository

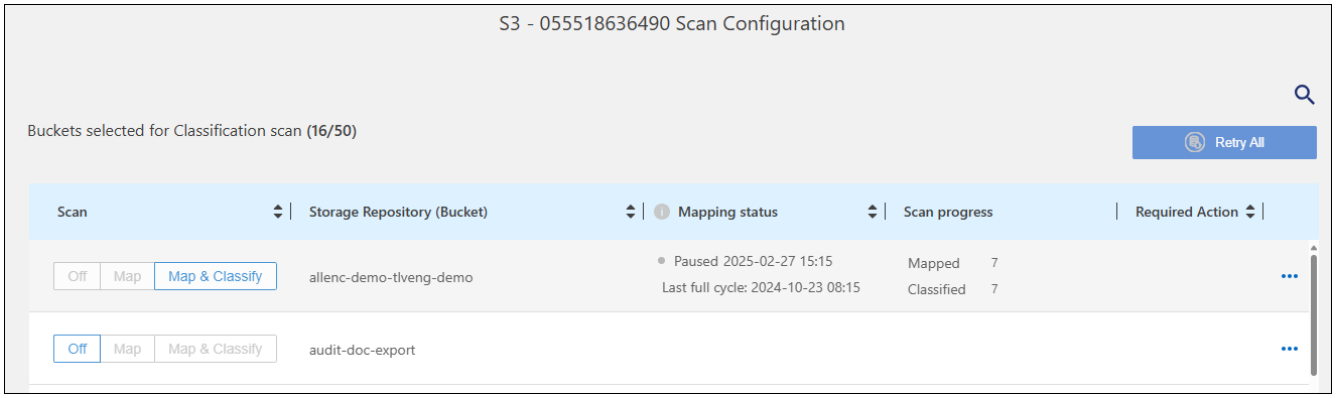
Sie können das Scannen eines Repositorys (z. B. eines Volumes) beenden, wenn Sie es nicht mehr auf Compliance-Anforderungen überwachen müssen. Dazu schalten Sie das Scannen aus. Wenn der Scanvorgang deaktiviert ist, werden alle Indexierungen und Informationen zu diesem Volumen aus dem System entfernt, und der Ladevorgang zum Scannen der Daten wird angehalten.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Registerkarte Konfiguration die Schaltfläche **Konfiguration** für die Arbeitsumgebung aus.



3. Wählen Sie auf der Seite Scankonfiguration die Option **aus**, um die Suche nach einem bestimmten Bucket zu beenden.



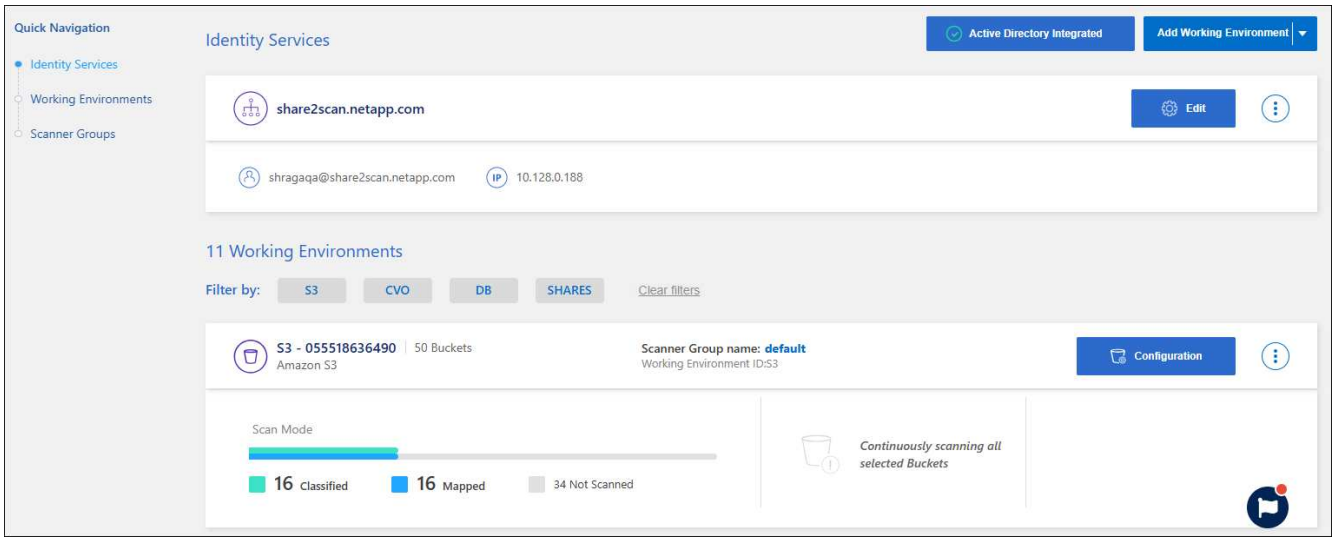
Halten Sie die Suche nach einem Repository an und setzen Sie sie fort

Sie können das Scannen in einem Repository „anhalten“, wenn Sie vorübergehend das Scannen bestimmter Inhalte beenden möchten. Das Anhalten des Scans bedeutet, dass die BlueXP Klassifizierung keine zukünftigen Scans nach Änderungen oder Ergänzungen des Repositorys durchführt, sondern dass alle aktuellen Ergebnisse weiterhin im System angezeigt werden. Das Anhalten des Scanvorgangs stoppt nicht den Ladevorgang für die gescannten Daten, da die Daten noch vorhanden sind.

Sie können den Scanvorgang jederzeit fortsetzen.

Schritte

1. Wählen Sie im BlueXP -Klassifizierungsmenü **Konfiguration**.
2. Wählen Sie auf der Registerkarte Konfiguration die Schaltfläche **Konfiguration** für die Arbeitsumgebung aus.



3. Wählen Sie auf der Seite Scankonfiguration das Symbol Aktionen ••• aus.
4. Wählen Sie **Pause**, um die Suche nach einem Volume anzuhalten, oder wählen Sie **Fortsetzen**, um die Suche nach einem Volume fortzusetzen, das zuvor angehalten wurde.

Anzeigen von Compliance-Berichten zur BlueXP - Klassifizierung

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 nur Daten für einige Arbeitsumgebungen enthalten, können Sie nach Filtern filtern, um nur diese anzuzeigen.

- 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.

Die folgenden Berichte sind für die BlueXP Klassifizierung verfügbar:

- **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.
- **Data Mapping Report**: Liefert Informationen über die Größe und Anzahl der Dateien in Ihren Arbeitsumgebungen. Dazu zählen Nutzungskapazität, Alter der Daten, Größe der Daten und Dateitypen.
- **Data Subject Access Request Report**: Ermöglicht es Ihnen, einen Bericht aller Dateien zu extrahieren, die Informationen über den spezifischen Namen oder die persönliche Kennung einer betroffenen Person enthalten.
- **HIPAA-Bericht**: Hilft Ihnen, die Verteilung von Gesundheitsinformationen in Ihren Dateien zu identifizieren.
- **PCI DSS-Bericht**: Hilft Ihnen, die Verteilung von Kreditkarteninformationen in Ihren Dateien zu identifizieren.
- **Privacy Risk Assessment Report**: Bietet Einblicke in den Datenschutz aus Ihren Daten und eine Bewertung des Datenschutzrisikos.
- **Berichte über einen bestimmten Informationstyp**: Es sind Berichte verfügbar, die Angaben zu den identifizierten Dateien enthalten, die personenbezogene Daten und sensible personenbezogene Daten enthalten. Sie können auch Dateien nach Kategorie und Dateityp aufgeschlüsselt sehen.

Wählen Sie die Arbeitsumgebungen für Berichte aus

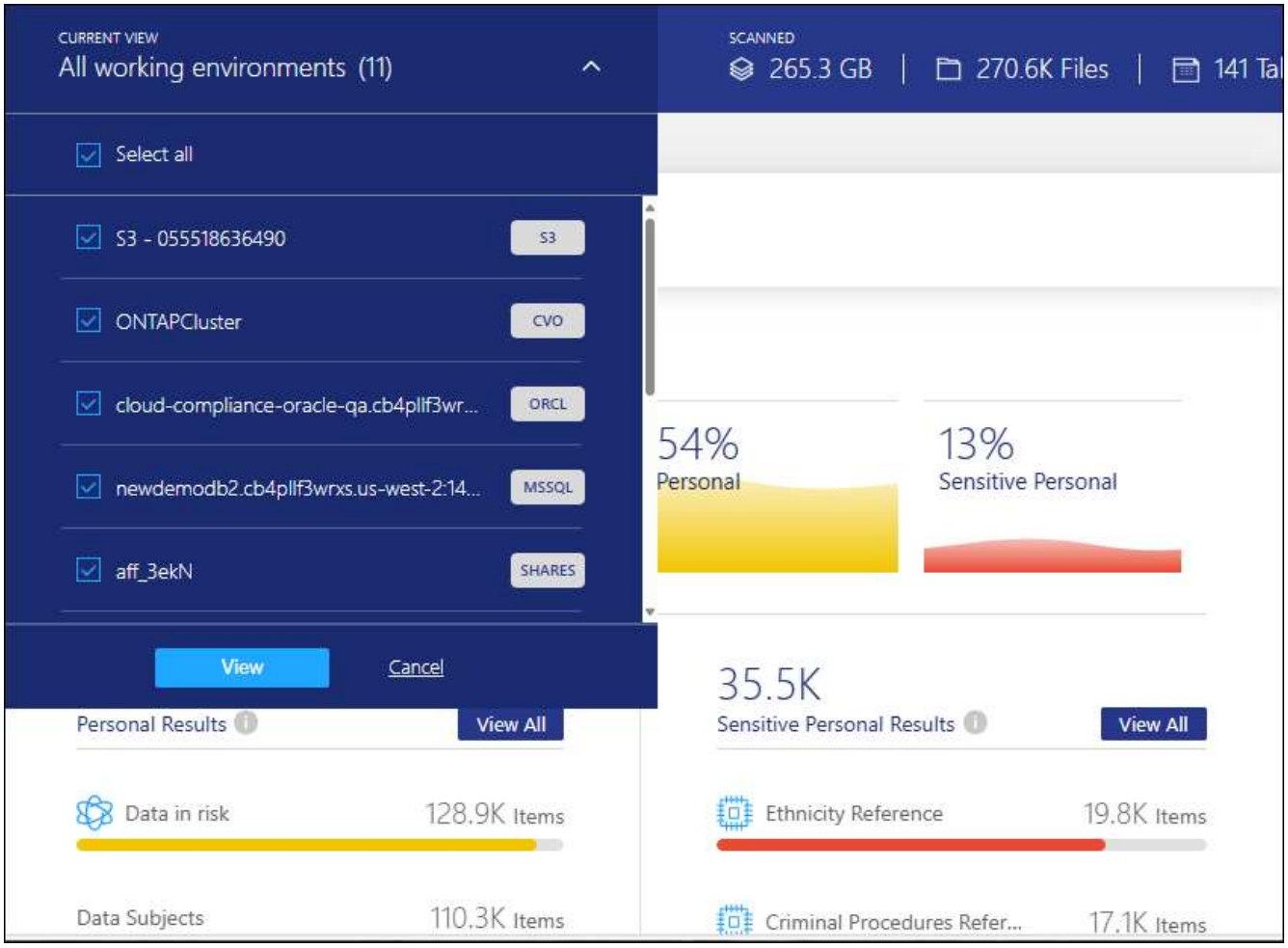
Sie können die Inhalte des BlueXP Klassifizierungs-Compliance-Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen einzusehen.

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

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option „**Compliance**“.

2. Wählen Sie die Dropdown-Liste Arbeitsumgebungen aus, und wählen Sie die Arbeitsumgebungen aus.
3. Wählen Sie **Ansicht**.



Zugriffsanfrage Für Betroffene

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 Datensubjekten und Download von Berichten

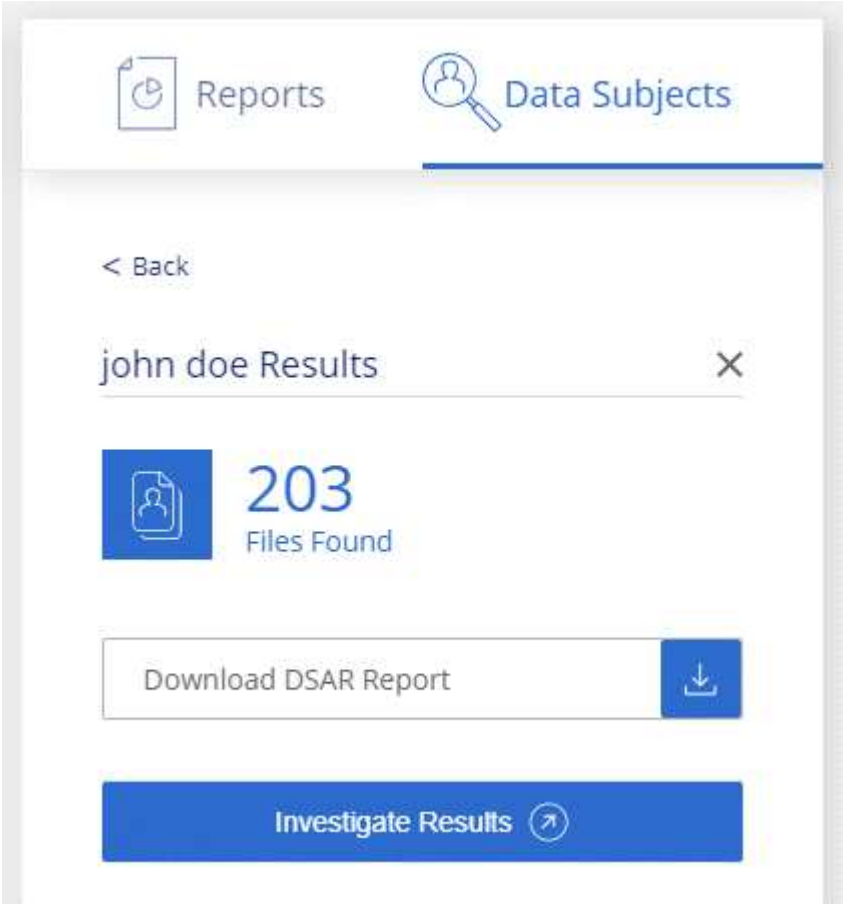
Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Sie können nach suchen"Alle persönlichen Informationstypen".

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. Wählen Sie im Menü BlueXP -Klassifizierung die Option „**Compliance**“.
2. Scrollen Sie auf der Compliance-Seite nach unten und wählen Sie **Data Subjects** aus.
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.

Bericht zum Health Insurance Portability and Accountability Act (HIPAA)

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:

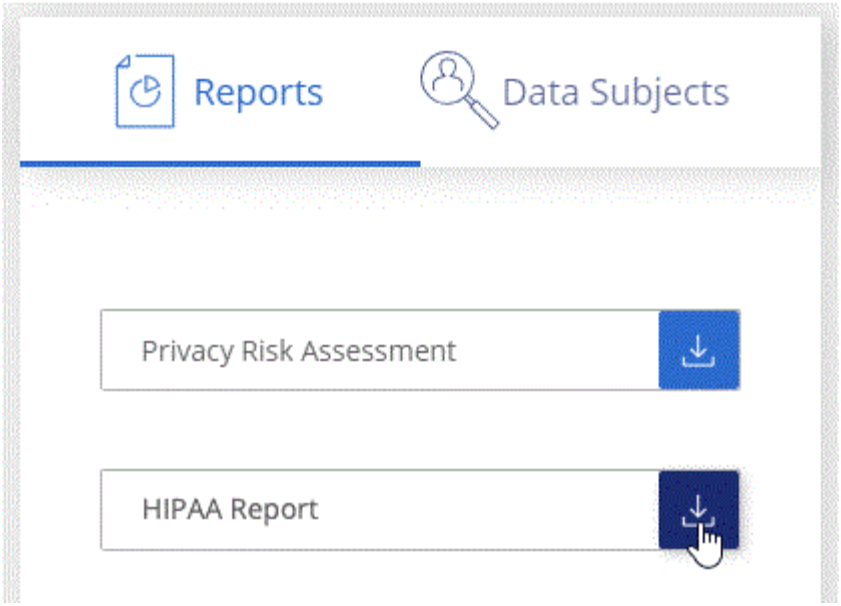
- Übersicht: Wie viele Dateien Gesundheitsinformationen enthalten und in welchen Arbeitsumgebungen.
- Verschlüsselung: Der Prozentsatz der Dateien, die Gesundheitsinformationen enthalten, die sich in verschlüsselten oder unverschlüsselten Arbeitsumgebungen befinden. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.
- Ransomware-Schutz: Der Prozentsatz an Dateien, die Gesundheitsinformationen enthalten und sich in Arbeitsumgebungen befinden, in denen 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 Gesundheitsinformationen nicht länger aufbewahren sollten, als Sie sie verarbeiten müssen.
- Verteilung von Gesundheitsinformationen: Die Arbeitsumgebungen, in denen die Gesundheitsinformationen 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. Wählen Sie im Menü BlueXP -Klassifizierung die Option „**Compliance**“.
2. Scrollen Sie nach unten und suchen Sie den Bereich **Reports**.
3. Klicken Sie auf das Download-Symbol neben **HIPAA Report**.



Ergebnis

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

Bericht zum Payment Card Industry Data Security Standard (PCI DSS)

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:

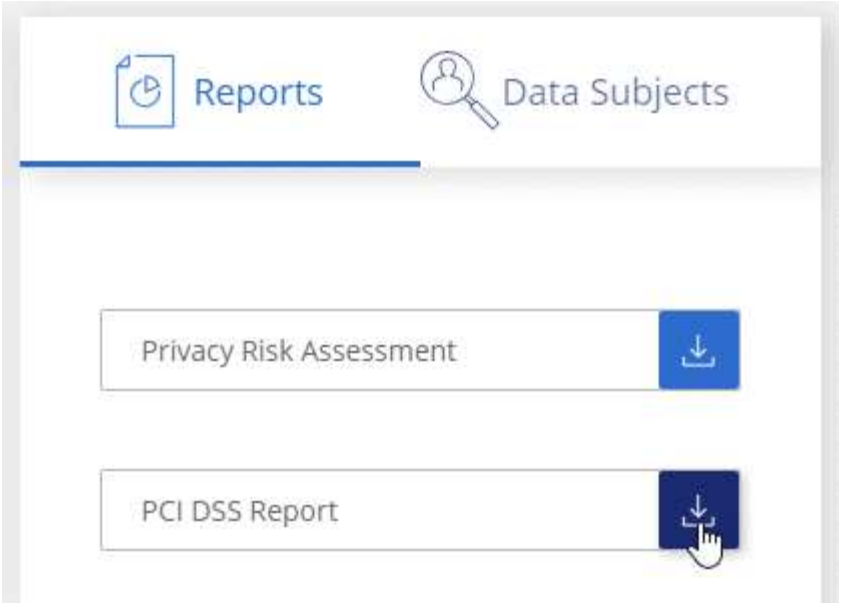
- Übersicht: Wie viele Dateien Kreditkarteninformationen enthalten und in welchen Arbeitsumgebungen.
- Verschlüsselung: Der Prozentsatz der Dateien, die Kreditkarteninformationen enthalten, die in verschlüsselten oder unverschlüsselten Arbeitsumgebungen gespeichert sind. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.
- Ransomware-Schutz: Der Prozentsatz an Dateien, die Kreditkarteninformationen enthalten und sich in Arbeitsumgebungen befinden, 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 Ihre Kreditkartendaten nicht länger aufbewahren sollten, als Sie sie bearbeiten müssen.
- Verteilung von Kreditkarteninformationen: Die Arbeitsumgebungen, in denen Kreditkarteninformationen gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

Generieren Sie den PCI DSS Report

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option „**Compliance**“.
2. Scrollen Sie nach unten und suchen Sie den Bereich **Reports**.
3. Wählen Sie das Download-Symbol neben **PCI DSS Report**.



Ergebnis

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

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:

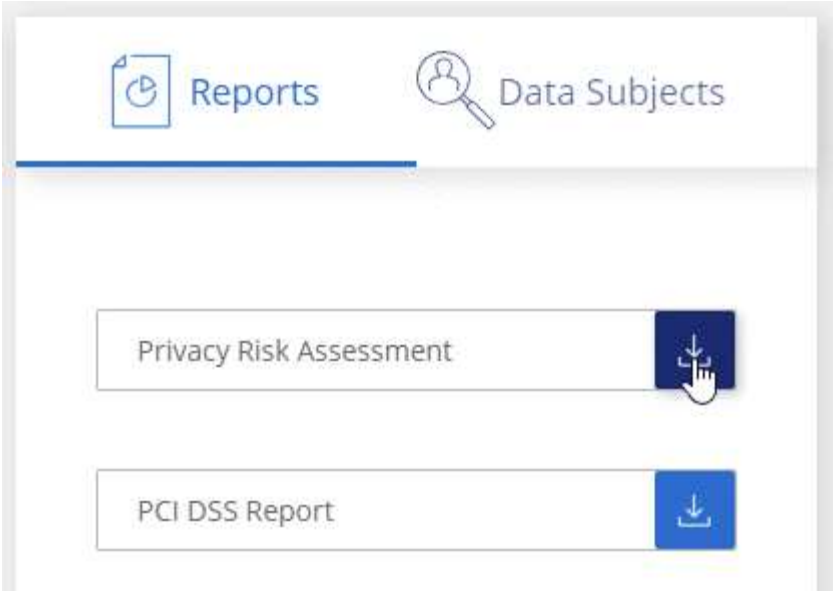
- Compliance-Status: Bewertung des Schweregrads und Verteilung von Daten – egal, ob es sich um nicht sensible, persönliche oder sensible Personen handelt.
- Bewertungsübersicht: Eine Aufschlüsselung der gefundenen personenbezogenen Daten sowie der Datenkategorien.
- Betroffene in dieser Bewertung: Die Anzahl der Personen, nach Standort, für die nationale Kennungen gefunden wurden.

Generieren Sie den Privacy Risk Assessment Report

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Wählen Sie im Menü BlueXP -Klassifizierung die Option „**Compliance**“.
2. Scrollen Sie nach unten und suchen Sie den Bereich **Reports**.
3. Klicken Sie auf das Download-Symbol neben **Privacy Risk Assessment**.



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 %

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.