Workloads schützen

NetApp Ransomware Resilience

NetApp
February 11, 2026

Inhalt

Workloads schützen

Schützen Sie Workloads mit NetApp Ransomware Resilience -Schutzstrategien

Sie können Workloads vor Ransomware-Angriffen schützen, indem Sie einen Workload-konsistenten Schutz aktivieren oder Ransomware-Schutzstrategien in NetApp Ransomware Resilience erstellen.

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Strategien zum Schutz vor Ransomware verstehen

Strategien zum Schutz vor Ransomware umfassen *Erkennung*, *Schutz* und *Replikationsrichtlinien*.

- **Erkennungsrichtlinien** identifizieren Ransomware-Bedrohungen.
- **Schutzrichtlinien** umfassen Snapshot- und Backup-Richtlinien. In einer Schutzstrategie sind Erkennungs- und Snapshot-Richtlinien erforderlich. Sicherungsrichtlinien sind optional.

  Wenn Sie zum Schutz Ihrer Workloads andere NetApp -Produkte verwenden, erkennt Ransomware Resilience diese und bietet Ihnen die Möglichkeit, entweder:

  - Verwenden Sie eine Ransomware-Erkennungsrichtlinie und nutzen Sie weiterhin die Snapshot- und Backup-Richtlinien, die von anderen NetApp -Tools erstellt wurden, oder
  - Verwenden Sie Ransomware Resilience, um Erkennung, Snapshots und Backups zu verwalten.
- **Replikationsrichtlinien** ermöglichen es Ihnen, Snapshots von Ransomware Resilience auf einen sekundären Standort zu replizieren. Replikationspläne können auf stündliche, tägliche, wöchentliche oder monatliche Frequenzen eingestellt werden.

  Derzeit können Snapshots nur auf lokalem ONTAP Speicher repliziert werden.

> Für eine verbesserte Verwaltung und Sicherung Ihres Datenbestands können Sie"Gruppendateifreigaben" um Datenmengen gemeinsam im Rahmen einer Strategie zu schützen.

Schutzrichtlinien mit anderen von NetApp verwalteten Diensten

Über Ransomware Resilience hinaus können die folgenden Dienste zur Verwaltung des Schutzes verwendet werden:

- NetApp Backup and Recovery für Dateifreigaben, VM-Dateifreigaben
- SnapCenter für VMware für VM-Datenspeicher
- SnapCenter für Oracle

Schutzinformationen dieser Dienste werden in Ransomware Resilience angezeigt. Mit Ransomware Resilience können Sie diesen Diensten Erkennungsrichtlinien hinzufügen. Das Hinzufügen einer Schutzrichtlinie mit Ransomware Resilience ersetzt die vorhandenen Schutzrichtlinien.

Wenn eine Ransomware-Erkennungsrichtlinie von Autonomous Ransomware Protection (ARP oder ARP/AI, je nach ONTAP Version) und FPolicy in ONTAP verwaltet wird, sind diese Workloads geschützt und werden weiterhin von ARP und FPolicy verwaltet.

> Für Workloads in Amazon FSx for NetApp ONTAP sind keine Sicherungsziele verfügbar. Führen Sie Sicherungsvorgänge mit dem FSx for ONTAP -Sicherungsdienst durch. Sie legen Sicherungsrichtlinien für Workloads in FSx für ONTAP in AWS fest, nicht in Ransomware Resilience. Die Sicherungsrichtlinien werden in Ransomware Resilience angezeigt und bleiben gegenüber AWS unverändert.

Schutzrichtlinien für Workloads, die nicht durch NetApp -Anwendungen geschützt sind

Wenn Ihre Arbeitslast nicht von Backup and Recovery, Ransomware Resilience, SnapCenter oder SnapCenter Plug-in for VMware vSphere verwaltet wird, werden möglicherweise Snapshots als Teil von ONTAP oder anderen Produkten erstellt. Wenn der ONTAP FPolicy-Schutz vorhanden ist, können Sie den FPolicy-Schutz mit ONTAP ändern.

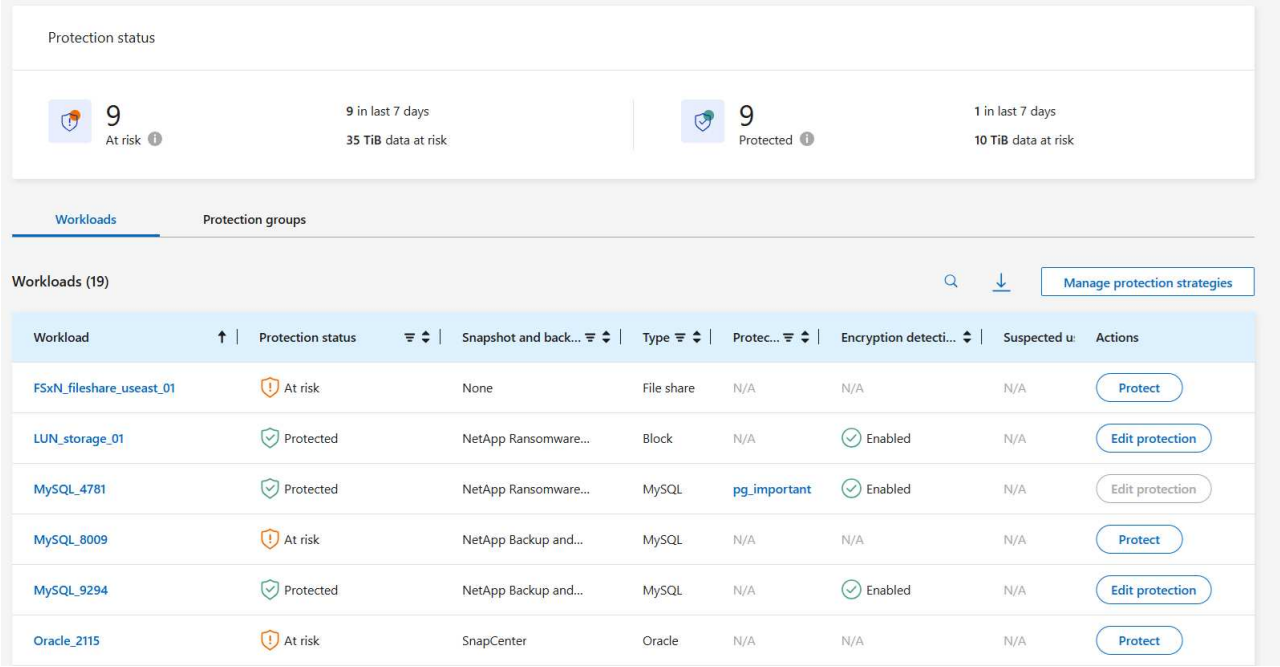
Anzeigen des Ransomware-Schutzes für eine Arbeitslast

Einer der ersten Schritte zum Schutz von Workloads besteht darin, Ihre aktuellen Workloads und deren Schutzstatus anzuzeigen. Sie können die folgenden Arten von Workloads sehen:

- Anwendungs-Workloads
- Blockieren von Workloads
- Dateifreigabe-Workloads
- VM-Workloads

Schritte

1. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz**.
2. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie im Bereich „Datenschutz“ des Dashboards die Option „Alle anzeigen“ aus.
    - Wählen Sie im Menü **Schutz** aus.



3. Auf dieser Seite können Sie Schutzdetails für die Arbeitslast anzeigen und ändern.

> Sehen"Fügen Sie eine Ransomware-Schutzstrategie hinzu" um mehr über die Verwendung von Ransomware Resilience zu erfahren, wenn eine bestehende Schutzrichtlinie mit SnapCenter oder Backup and Recovery vorhanden ist.

Die Seite „Schutz verstehen“

Auf der Seite „Schutz“ werden die folgenden Informationen zum Workload-Schutz angezeigt:

Schutzstatus: Eine Arbeitslast kann einen der folgenden Schutzstatus aufweisen, um anzugeben, ob eine Richtlinie angewendet wird oder nicht:

- **Geschützt**: Eine Richtlinie wird angewendet. ARP (oder ARP/AI, je nach ONTAP Version) ist auf allen mit der Arbeitslast verbundenen Volumes aktiviert.
- **Gefährdet**: Es wird keine Richtlinie angewendet. Wenn für einen Workload keine primäre Erkennungsrichtlinie aktiviert ist, ist er „gefährdet“, auch wenn für ihn eine Snapshot- und Backup-Richtlinie aktiviert ist.
- **In Bearbeitung**: Eine Richtlinie wird angewendet, ist aber noch nicht abgeschlossen.
- **Fehlgeschlagen**: Eine Richtlinie wird angewendet, funktioniert aber nicht.

Erkennungsstatus: Eine Arbeitslast kann einen der folgenden Ransomware-Erkennungsstatus aufweisen:

- **Lernen**: Der Arbeitslast wurde vor Kurzem eine Richtlinie zur Ransomware-Erkennung zugewiesen und Ransomware Resilience scannt die Arbeitslasten.
- **Aktiv**: Eine Schutzrichtlinie zur Ransomware-Erkennung ist zugewiesen.
- **Nicht festgelegt**: Es ist keine Schutzrichtlinie zur Ransomware-Erkennung zugewiesen.
- **Fehler**: Eine Ransomware-Erkennungsrichtlinie wurde zugewiesen, aber Ransomware Resilience hat einen Fehler festgestellt.

Wenn der Schutz in Ransomware Resilience aktiviert ist, beginnt die Erkennung und Meldung von Warnungen, nachdem sich der Status der Ransomware-Erkennungsrichtlinie vom Lernmodus in den aktiven Modus geändert hat.

Verdächtige Benutzeraktivitäten und Aktivitäten im Zusammenhang mit FPolicy (verdächtige Dateierweiterungen) werden getrennt vom Erkennungsstatus aufgeführt.

Erkennungsrichtlinie: Der Name der Ransomware-Erkennungsrichtlinie wird angezeigt, sofern eine zugewiesen wurde. Wenn die Erkennungsrichtlinie nicht zugewiesen wurde, wird „N/A“ angezeigt.

Replikationsziel: Wenn Sie die Snapshot-Replikation konfiguriert haben, werden die Namen der Ziel-Speicher-VMs und -Systeme aufgelistet. Wenn keine Replikation vorliegt, wird in diesem Feld „Keine“ angezeigt.

Snapshot- und Backup-Richtlinien: Diese Spalte zeigt die auf die Arbeitslast angewendeten Snapshot- und Backup-Richtlinien und das Produkt oder den Dienst, das bzw. der diese Richtlinien verwaltet.

- Verwaltet von SnapCenter
- Verwaltet durch SnapCenter Plug-in for VMware vSphere
- Verwaltet durch Backup und Wiederherstellung
- Name der Ransomware-Schutzrichtlinie, die Snapshots und Backups regelt
- Keine

Arbeitsbelastungsbedeutung

Ransomware Resilience weist jedem Workload während der Erkennung basierend auf einer Analyse jedes Workloads eine Wichtigkeit oder Priorität zu. Die Workload-Wichtigkeit wird durch die folgenden Snapshot-Häufigkeiten bestimmt:

- **Kritisch**: Es werden mehr als eine Snapshot-Kopie pro Stunde erstellt (sehr aggressiver Schutzplan).
- **Wichtig**: Snapshot-Kopien werden seltener als stündlich, aber häufiger als täglich erstellt.
- **Standard**: Es werden mehrmals täglich Momentaufnahmen erstellt.

Vordefinierte Erkennungsrichtlinien

Sie können eine der folgenden vordefinierten Ransomware-Resilience-Richtlinien auswählen, die auf die Wichtigkeit der Arbeitslast abgestimmt sind.

Die Richtlinie **Encryption-Benutzererweiterung** ist die einzige vordefinierte Richtlinie, die die Erkennung verdächtigen Benutzerverhaltens unterstützt.

+ Die **kritische Replikationsrichtlinie** ist die einzige vordefinierte Richtlinie, die die Replikation von Snapshots nach ONTAP unterstützt.

Richtlinie nebene	Schnappschuss	Frequenz	Aufbewahrungsdauer (Tage)	Anzahl der Snapshot-Kopien	Maximale Anzahl von Snapshot-Kopien
Richtlinie für kritische Arbeitslast	Viertelstündlich	Alle 15 Minuten	3	288	309
	Täglich	Jeden 1 Tag	14	14	309
	Wöchentlich	Jede Woche	35	5	309
	Monatlich	Alle 30 Tage	60	2	309
Wichtige Arbeitsbelastungsrichtlinie	Viertelstündlich	Alle 30 Minuten	3	144	165
	Täglich	Jeden 1 Tag	14	14	165
	Wöchentlich	Jede Woche	35	5	165
	Monatlich	Alle 30 Tage	60	2	165
Standard-Arbeitslastrichtlinie	Viertelstündlich	Alle 30 Minuten	3	72	93
	Täglich	Jeden 1 Tag	14	14	93
	Wöchentlich	Jede Woche	35	5	93
	Monatlich	Alle 30 Tage	60	2	93
Verschlüsselungsbenutzererweiterung	Viertelstündlich	Alle 30 Minuten	3	72	93
	Täglich	Jeden 1 Tag	14	14	93
	Wöchentlich	Jede Woche	35	5	93
	Monatlich	Alle 30 Tage	60	2	93
Verschlüsselungsbenutzererweiterung	Viertelstündlich	Alle 30 Minuten	3	72	93
	Täglich	Jeden 1 Tag	14	14	93
	Wöchentlich	Jede Woche	35	5	93
	Monatlich	Alle 30 Tage	60	2	93

Richtlinie nebene	Schnappschuss	Frequenz	Aufbewahrungsdauer (Tage)	Anzahl der Snapshot-Kopien	Maximale Anzahl von Snapshot-Kopien
Richtlinie zur kritischen Replikation	Viertelstündlich	Alle 15 Minuten	3	288	309
	Täglich	Jeden 1 Tag	14	14	309
	Wöchentlich	Jede Woche	35	5	309
	Monatlich	Alle 30 Tage	60	2	309

Aktivieren Sie anwendungs- oder VM-konsistenten Schutz mit SnapCenter

Durch die Aktivierung des anwendungs- oder VM-konsistenten Schutzes können Sie Ihre Anwendungs- oder VM-Workloads auf konsistente Weise schützen und einen ruhigen und konsistenten Zustand erreichen, um einen möglichen späteren Datenverlust zu vermeiden, falls eine Wiederherstellung erforderlich ist.

Dieser Prozess leitet die Registrierung des SnapCenter Software Servers für Anwendungen oder des SnapCenter Plug-in for VMware vSphere für VMs mit Backup und Recovery ein.

Nachdem Sie den Workload-konsistenten Schutz aktiviert haben, können Sie Schutzstrategien in Ransomware Resilience verwalten. Die Schutzstrategie umfasst die an anderer Stelle verwalteten Snapshot- und Backup-Richtlinien sowie eine in Ransomware Resilience verwaltete Ransomware-Erkennungsrichtlinie.

Informationen zum Registrieren von SnapCenter oder SnapCenter Plug-in for VMware vSphere mithilfe von Backup und Recovery finden Sie in den folgenden Informationen:

- "Registrieren der SnapCenter Server-Software"
- "Registrieren Sie das SnapCenter Plug-in for VMware vSphere"

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Dashboard“ aus.
2. Suchen Sie im Bereich „Empfehlungen“ eine der folgenden Empfehlungen und wählen Sie „Überprüfen und beheben“ aus:
   - Verfügbaren SnapCenter Server mit der NetApp Console registrieren
   - Verfügbares SnapCenter Plug-in for VMware vSphere (SCV) mit der NetApp Console registrieren
3. Befolgen Sie die Informationen, um das SnapCenter oder SnapCenter Plug-in for VMware vSphere Host mithilfe von Backup und Recovery zu registrieren.
4. Zurück zur Ransomware-Resilienz.
5. Navigieren Sie von Ransomware Resilience zum Dashboard und starten Sie den Erkennungsprozess erneut.
6. Wählen Sie unter „Ransomware-Resilienz“ **Schutz** aus, um die Seite „Schutz“ anzuzeigen.
7. Überprüfen Sie die Details in der Spalte „Snapshot- und Sicherungsrichtlinien“ auf der Seite „Schutz“, um sicherzustellen, dass die Richtlinien an anderer Stelle verwaltet werden.

Fügen Sie eine Ransomware-Schutzstrategie hinzu

Es gibt drei Ansätze zum Hinzufügen einer Ransomware-Schutzstrategie:

- **Erstellen Sie eine Ransomware-Schutzstrategie, wenn Sie keine Snapshot- oder Backup-Richtlinien haben.**

  Die Ransomware-Schutzstrategie umfasst:

  - Snapshot-Richtlinie
  - Richtlinie zur Ransomware-Erkennung
  - Sicherungsrichtlinie

- **Ersetzen Sie die vorhandenen Snapshot- oder Backup-Richtlinien von SnapCenter oder Backup and Recovery Protection durch Schutzstrategien, die von Ransomware Resilience verwaltet werden.**

  Die Ransomware-Schutzstrategie umfasst:

  - Snapshot-Richtlinie
  - Richtlinie zur Ransomware-Erkennung
  - Sicherungsrichtlinie

- **Erstellen Sie eine Erkennungsrichtlinie für Workloads mit vorhandenen Snapshot- und Backup-Richtlinien, die in anderen NetApp -Produkten oder -Services verwaltet werden.**

  Die Erkennungsrichtlinie ändert nicht die in anderen Produkten verwalteten Richtlinien.

  Die Erkennungsrichtlinie aktiviert den autonomen Ransomware-Schutz und den FPolicy-Schutz, wenn diese bereits in anderen Diensten aktiviert sind. Erfahren Sie mehr über"Autonomer Ransomware-Schutz" ,"Sicherung und Wiederherstellung" , Und"ONTAP FPolicy" .

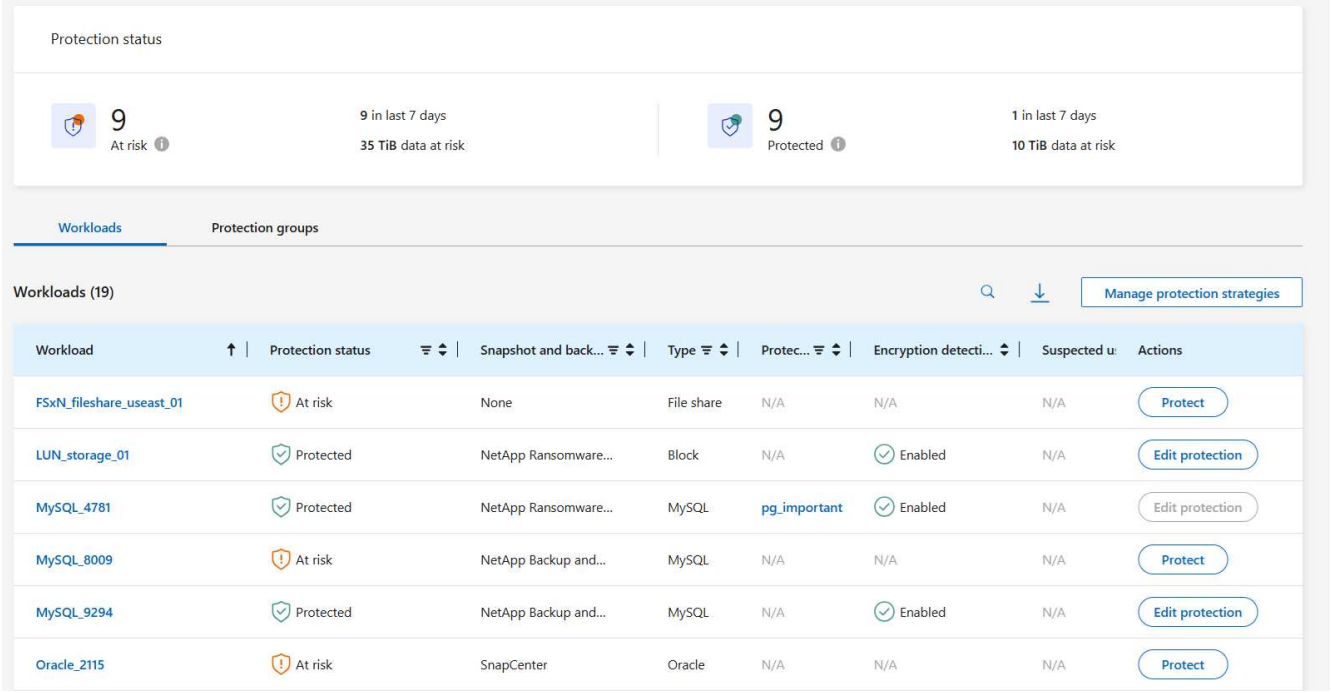
Erstellen Sie eine Ransomware-Schutzstrategie (wenn Sie keine Snapshot- oder Backup-Richtlinien haben)

Wenn für die Arbeitslast keine Snapshot- oder Sicherungsrichtlinien vorhanden sind, können Sie eine Ransomware-Schutzstrategie erstellen, die die folgenden Richtlinien enthalten kann, die Sie in Ransomware Resilience erstellen:

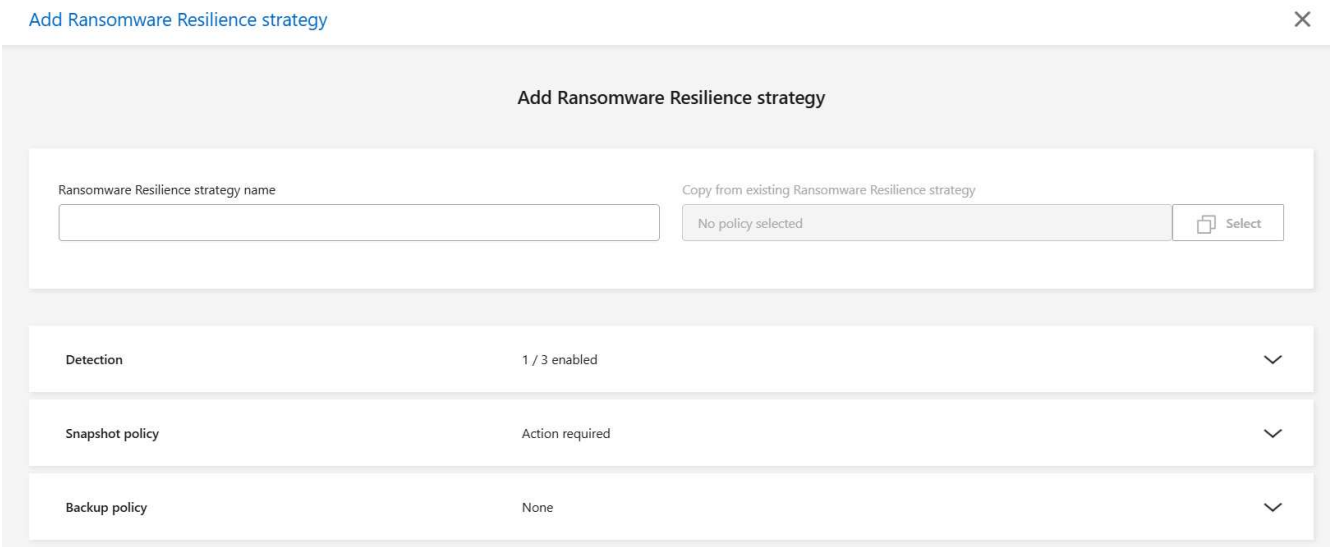
- Snapshot-Richtlinie
- Sicherungsrichtlinie
- Richtlinie zur Ransomware-Erkennung
- Sekundäre Replikation zu ONTAP

Schritte zum Erstellen einer Ransomware-Schutzstrategie

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



2. Wählen Sie auf der Seite „Schutz“ eine Arbeitslast aus und klicken Sie dann auf **Schützen**.
3. Wählen Sie auf der Seite „Ransomware-Schutzstrategien“ **Hinzufügen** aus.



4. Geben Sie einen neuen Strategienamen ein oder geben Sie einen vorhandenen Namen ein, um ihn zu kopieren. Wenn Sie einen vorhandenen Namen eingeben, wählen Sie aus, welchen Sie kopieren möchten, und wählen Sie **Kopieren**.

> Wenn Sie eine vorhandene Strategie kopieren und ändern möchten, hängt Ransomware Resilience „_copy“ an den ursprünglichen Namen an. Sie sollten den Namen und mindestens eine Einstellung ändern, um es eindeutig zu machen.

5. Wählen Sie für jedes Element den **Abwärtspfeil** aus.
   - **Erkennungsrichtlinie**:
     - **Richtlinie**: Wählen Sie eine der vordefinierten Erkennungsrichtlinien.

- **Primäre Erkennung**: Aktivieren Sie die Ransomware-Resilienz, um potenzielle Ransomware-Angriffe zu erkennen.
- **Erkennung verdächtigen Benutzerverhaltens**: Aktivieren Sie die Erkennung des Benutzerverhaltens, um Benutzeraktivitätsereignisse an Ransomware Resilience zu übertragen und verdächtige Ereignisse wie Datenverletzungen zu erkennen.
- **Dateierweiterungen blockieren**: Aktivieren Sie die Ransomware-Resilienz, um bekannte verdächtige Dateierweiterungen zu blockieren. Ransomware Resilience erstellt automatisch Snapshot-Kopien, wenn die primäre Erkennung aktiviert ist.

  Wenn Sie die blockierten Dateierweiterungen ändern möchten, bearbeiten Sie sie im System Manager.

◦ **Snapshot-Richtlinie**:

- **Basisname der Snapshot-Richtlinie**: Wählen Sie eine Richtlinie aus oder wählen Sie **Erstellen** und geben Sie einen Namen für die Snapshot-Richtlinie ein.
- **Snapshot-Sperre**: Aktivieren Sie diese Option, um die Snapshot-Kopien auf dem primären Speicher zu sperren, sodass sie für einen bestimmten Zeitraum nicht geändert oder gelöscht werden können, selbst wenn ein Ransomware-Angriff den Weg zum Sicherungsspeicherziel findet. Dies wird auch als *unveränderlicher Speicher* bezeichnet. Dies ermöglicht eine schnellere Wiederherstellung.

  Wenn ein Snapshot gesperrt ist, wird die Ablaufzeit des Volumes auf die Ablaufzeit der Snapshot-Kopie eingestellt.

Die Snapshot-Kopiersperre ist mit ONTAP 9.12.1 und höher verfügbar. Weitere Informationen zu SnapLock finden Sie unter "SnapLock in ONTAP" .

◦ **Schnappschuss-Zeitpläne**: Wählen Sie Zeitplanoptionen und die Anzahl der aufzubewahrenden Schnappschusskopien aus und aktivieren Sie den Zeitplan.

- **Replikationsrichtlinie**:

◦ **Basisname der Replikationsrichtlinie**: Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen aus. Der Basisname ist das Präfix, das an alle Snapshots angehängt wird.

◦ **Replikationszeitpläne**: Aktivieren Sie die gewünschten Replikationsfrequenzen (stündlich, täglich, wöchentlich oder monatlich) und legen Sie für jeden aktivierten Zeitplan den Aufbewahrungswert (die Anzahl der aufzubewahrenden replizierten Snapshots) fest.

- **Backup-Richtlinie**:

◦ **Basisname der Sicherungsrichtlinie**: Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Namen.

◦ **Sicherungszeitpläne**: Wählen Sie Zeitplanoptionen für den sekundären Speicher und aktivieren Sie den Zeitplan.

Um die Sicherungssperre auf dem sekundären Speicher zu aktivieren, konfigurieren Sie Ihre Sicherungsziele mit der Option **Einstellungen**. Weitere Informationen finden Sie unter "Konfigurieren der Einstellungen" .

6. Wählen Sie **Hinzufügen**.

Fügen Sie Workloads mit vorhandenen Snapshot- und Backup-Richtlinien, die von SnapCenter oder Backup and Recovery verwaltet werden, eine Erkennungsrichtlinie hinzu

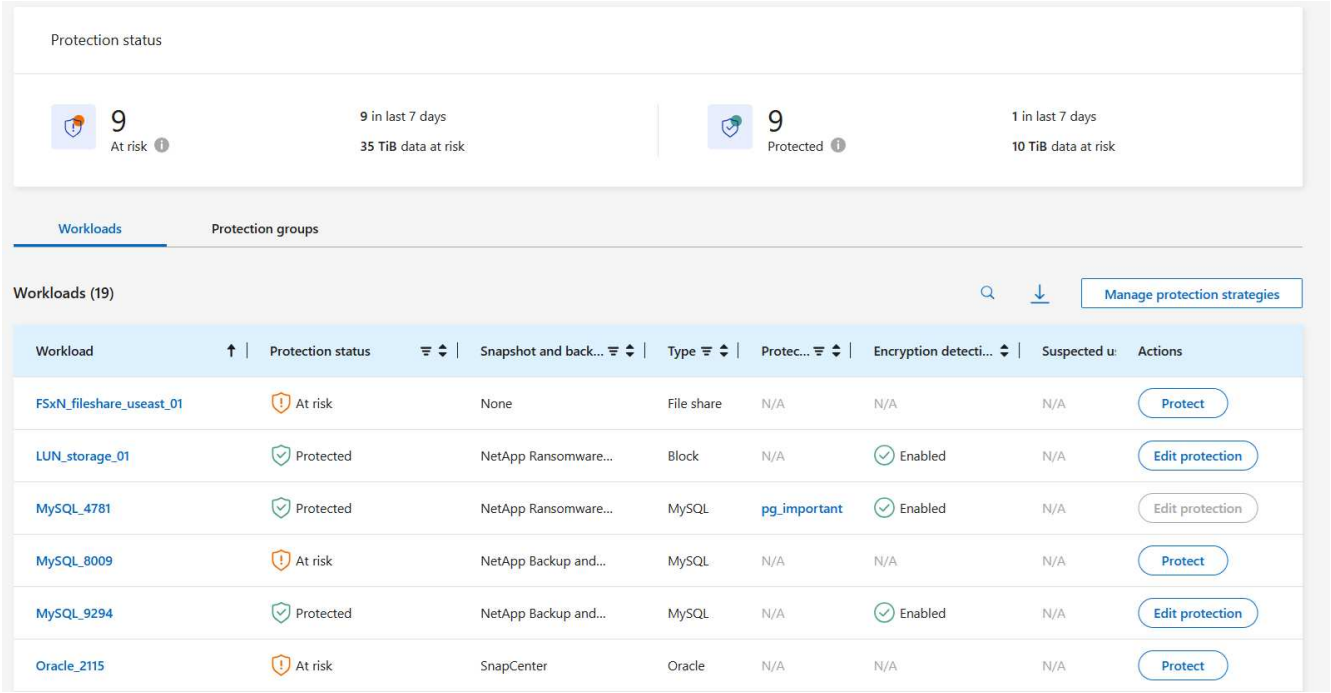
Mit Ransomware Resilience können Sie Workloads mit vorhandenem Snapshot- und Backup-Schutz, der in anderen NetApp -Produkten oder -Services verwaltet wird, entweder eine Erkennungsrichtlinie oder eine Schutzrichtlinie zuweisen. Andere Dienste wie Backup and Recovery und SnapCenter verwenden Richtlinien, die Snapshots, die Replikation auf sekundären Speicher oder Backups auf Objektspeicher regeln.

Hinzufügen einer Erkennungsrichtlinie zu Workloads mit vorhandenen Sicherungs- oder Snapshot-Richtlinien

Wenn Sie über vorhandene Snapshot- oder Backup-Richtlinien mit Backup and Recovery oder SnapCenter verfügen, können Sie eine Richtlinie zum Erkennen von Ransomware-Angriffen hinzufügen. Informationen zum Verwalten von Schutz und Erkennung mit Ransomware Resilience finden Sie unterSchutz durch Ransomware-Resilienz .

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



2. Wählen Sie auf der Seite „Schutz“ eine Arbeitslast aus und wählen Sie dann **Schützen**.
3. Ransomware Resilience erkennt, ob aktive SnapCenter oder Backup- und Recovery-Richtlinien vorhanden sind.
4. Um Ihre vorhandenen Backup- und Recovery- oder SnapCenter -Richtlinien beizubehalten und nur eine _Erkennungs_richtlinie anzuwenden, lassen Sie das Kontrollkästchen **Vorhandene Richtlinien ersetzen** deaktiviert.
5. Um Details zu den SnapCenter -Richtlinien anzuzeigen, wählen Sie den **Abwärtspfeil**.
6. Wählen Sie die gewünschten Erkennungseinstellungen: **Verschlüsselungserkennung Erkennung verdächtigen Benutzerverhaltens Blockieren verdächtiger Dateierweiterungen**
7. Wählen Sie **Weiter**.
8. Wenn Sie **Erkennung verdächtigen Nutzerverhaltens** als Erkennungseinstellung ausgewählt haben, wählen Sie den User activity agent oder "oder erstellen Sie ein".

Der Benutzeraktivitätsagent hostet die neuen Datensammler. Ransomware Resilience erstellt den Datensammler automatisch, um Benutzeraktivitätsereignisse an Ransomware Resilience zu übertragen und so anomales Benutzerverhalten zu erkennen.

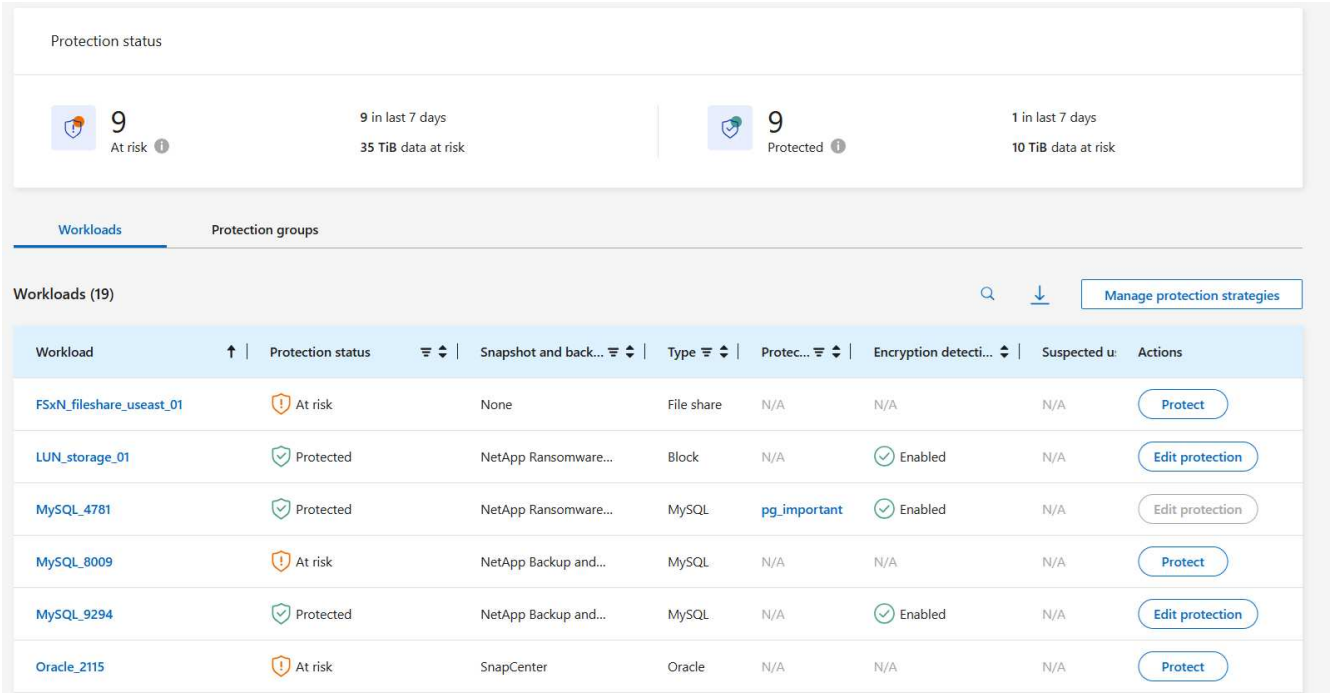
9. Wählen Sie **Weiter**.
10. Überprüfen Sie Ihre Auswahl. Wählen Sie **Erstellen**, um die Erkennung zu aktivieren.
11. Überprüfen Sie auf der Seite „Schutz“ den **Erkennungsstatus**, um zu bestätigen, dass die Erkennung aktiv ist.

Ersetzen Sie vorhandene Backup- oder Snapshot-Richtlinien durch eine Ransomware-Schutzstrategie

Sie können Ihre vorhandenen Backup- oder Snapshot-Richtlinien durch eine Ransomware-Schutzstrategie ersetzen. Dieser Ansatz entfernt Ihren extern verwalteten Schutz und konfiguriert Erkennung und Schutz in Ransomware Resilience.

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



2. Wählen Sie auf der Seite „Schutz“ eine Arbeitslast aus und wählen Sie dann **Schützen**.
3. Ransomware Resilience erkennt, ob aktive Backup- und Recovery- oder SnapCenter -Richtlinien vorhanden sind. Um die vorhandenen Backup- und Recovery- oder SnapCenter -Richtlinien zu ersetzen, aktivieren Sie das Kontrollkästchen **Vorhandene Richtlinien ersetzen**. Wenn Sie das Kontrollkästchen aktivieren, ersetzt Ransomware Resilience die Liste der Erkennungsrichtlinien durch Erkennungsrichtlinien.
4. Wählen Sie eine Schutzrichtlinie. Wenn keine Schutzrichtlinie vorhanden ist, wählen Sie **Hinzufügen**, um eine neue Richtlinie zu erstellen. Informationen zum Erstellen einer Richtlinie finden Sie unterErstellen einer Schutzrichtlinie . Wählen Sie **Weiter**.
5. Wenn Ihre Strategie die Replikation beinhaltet, wählen Sie das **Zielsystem** und die **Zielspeicher-VM** aus. Wählen Sie **Weiter**.
6. Wählen Sie ein Sicherungsziel aus oder erstellen Sie ein neues. Wählen Sie **Weiter**.
   a. Wenn Ihre Schutzstrategie die Erkennung des Benutzerverhaltens umfasst, wählen Sie in Ihrer

Umgebung einen Benutzeraktivitätsagenten aus, um die neuen Datensammler zu hosten. Ransomware Resilience erstellt den Datensammler automatisch, um Benutzeraktivitätsereignisse an Ransomware Resilience zu übertragen und so anomales Benutzerverhalten zu erkennen.

7. Überprüfen Sie die neue Schutzstrategie und wählen Sie dann **Schützen** aus, um sie anzuwenden.
8. Überprüfen Sie auf der Seite „Schutz“ den **Erkennungsstatus**, um zu bestätigen, dass die Erkennung aktiv ist.

Zuweisen einer anderen Richtlinie

Sie können die bestehende Richtlinie durch eine andere ersetzen.

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ in der Workload-Zeile die Option „Schutz bearbeiten“ aus.
3. Wenn für die Arbeitslast eine vorhandene Backup- und Wiederherstellungs- oder SnapCenter -Richtlinie vorhanden ist, die Sie beibehalten möchten, deaktivieren Sie **Vorhandene Richtlinien ersetzen**. Um die vorhandenen Richtlinien zu ersetzen, aktivieren Sie **Vorhandene Richtlinien ersetzen**.
4. Wählen Sie auf der Seite „Richtlinien“ den Abwärtspfeil für die Richtlinie aus, die Sie zuweisen möchten, um die Details zu überprüfen.
5. Wählen Sie die Richtlinie aus, die Sie zuweisen möchten.
6. Wählen Sie **Schützen**, um die Änderung abzuschließen.

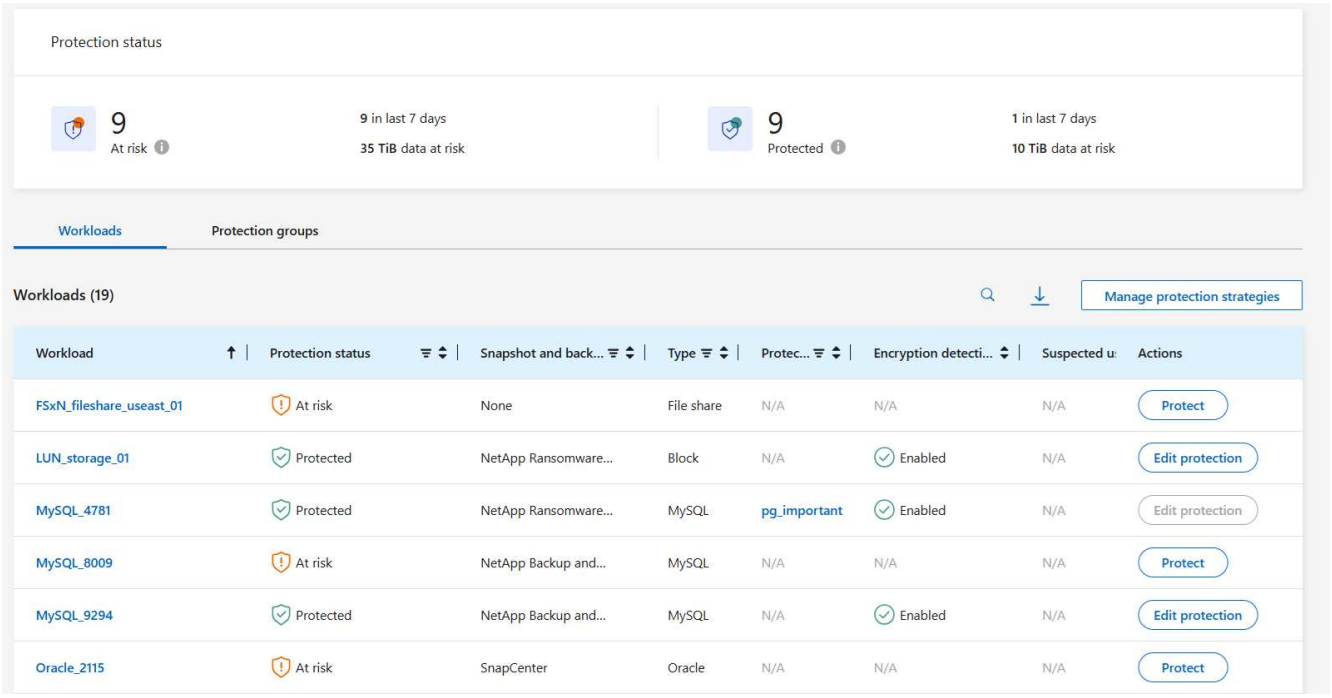
Erstellen einer Schutzgruppe

Durch die Gruppierung von Dateifreigaben in einer Schutzgruppe können Sie Ihren Datenbestand leichter schützen. Ransomware Resilience kann alle Volumes in einer Gruppe gleichzeitig schützen, anstatt jedes Volume einzeln zu schützen.

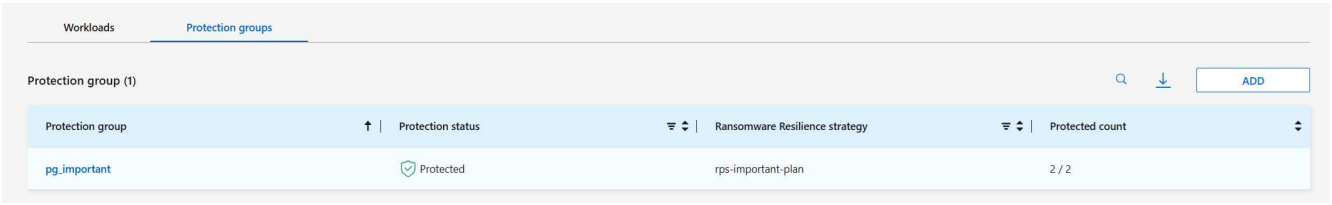
Sie können Gruppen unabhängig von ihrem Schutzstatus erstellen (d. h. nicht geschützte Gruppen und geschützte Gruppen). Wenn Sie einer Schutzgruppe eine Schutzrichtlinie hinzufügen, ersetzt die neue Schutzrichtlinie alle vorhandenen Richtlinien, einschließlich der von SnapCenter und NetApp Backup and Recovery verwalteten Richtlinien.

Schritte

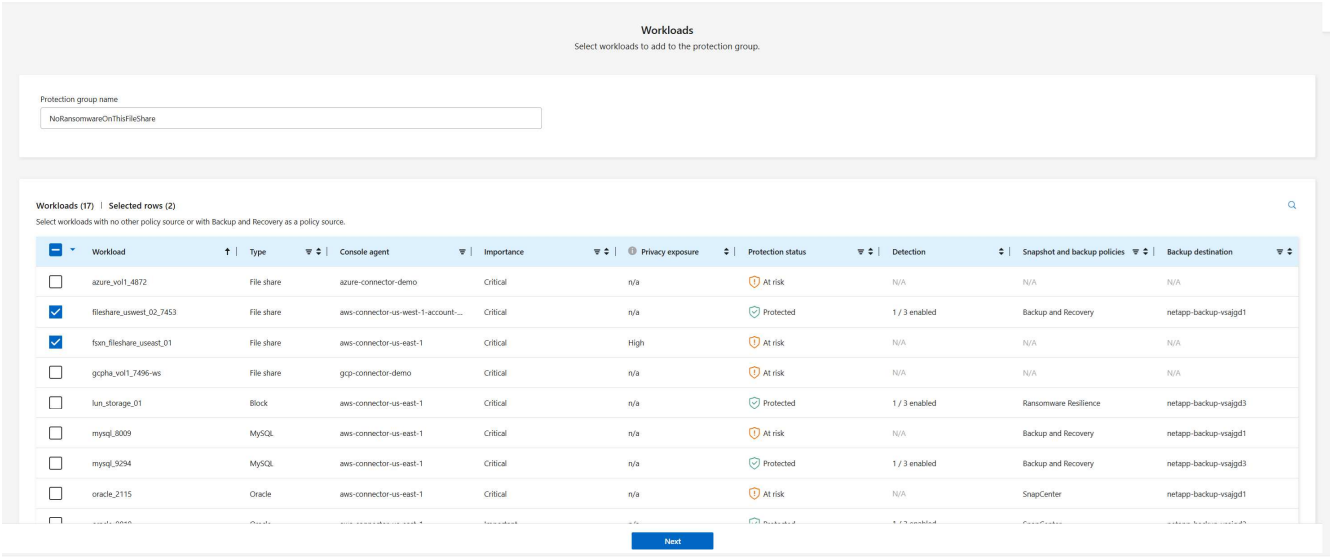
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



2. Wählen Sie auf der Seite „Schutz“ die Registerkarte „Schutzgruppen“ aus.



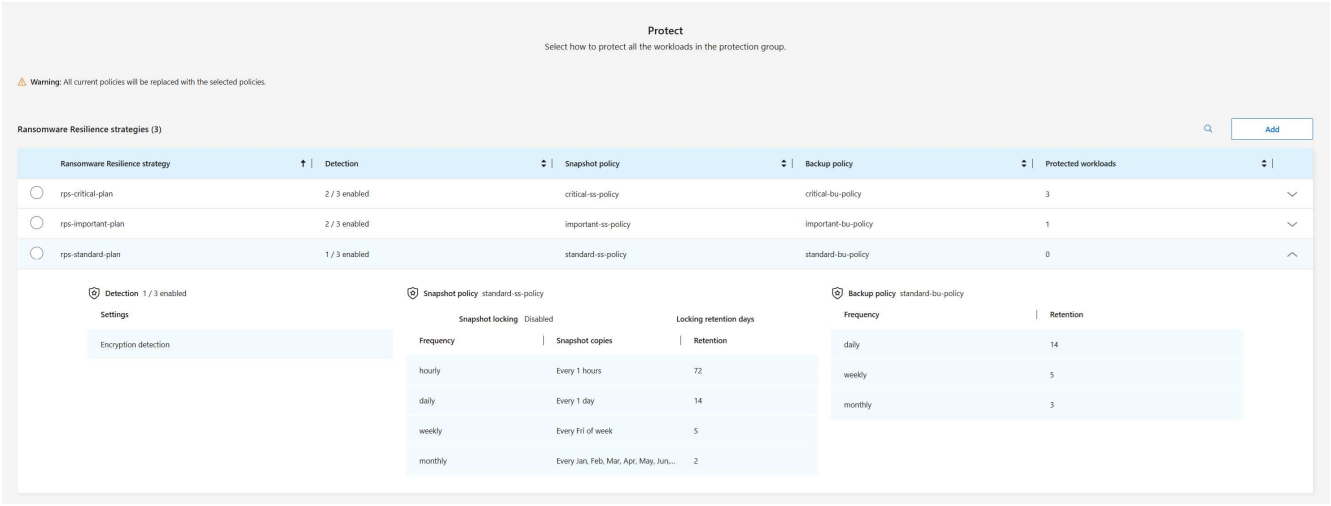
3. Wählen Sie **Hinzufügen**.



4. Geben Sie einen Namen für die Schutzgruppe ein.
5. Wählen Sie die Workloads aus, die der Gruppe hinzugefügt werden sollen.

Um weitere Details zu den Arbeitslasten anzuzeigen, scrollen Sie nach rechts.

6. Wählen Sie **Weiter**.



7. Wählen Sie die Richtlinie aus, die den Schutz für diese Gruppe regelt. Wählen Sie zur Bestätigung **Weiter**.
8. Wenn die Schutzstrategie die Replikation umfasst, überprüfen Sie die Replikationseinstellungen.
   a. Um alle Snapshots am selben Zielort zu replizieren, aktivieren Sie **Für jede Arbeitslast das gleiche Ziel verwenden**. Wählen Sie im Abschnitt „Konsolenagent“ ein **Zielsystem** und eine **Zielspeicher-VM** für die Workloads aus. + Um andere Ziele zu verwenden, deaktivieren Sie dieses Kästchen. Überprüfen Sie alle Workloads unter jedem Console-Agenten und weisen Sie jedem Workload ein **Zielsystem** und eine **Zielspeicher-VM** zu. Wählen Sie **Weiter**.
9. Um eine Sicherungsrichtlinie zu konfigurieren, wählen Sie eine aus und klicken Sie dann auf **Weiter**.
10. Wenn Ihre Erkennungsrichtlinie die Erkennung des Benutzerverhaltens umfasst, wählen Sie den Datensammler aus, den Sie verwenden möchten, und klicken Sie dann auf **Weiter**.
11. Überprüfen Sie die Auswahl für die Schutzgruppe.
12. Um die Erstellung der Schutzgruppe abzuschließen, wählen Sie **Hinzufügen**.

Gruppenschutz bearbeiten

Sie können die Erkennungsrichtlinie für eine vorhandene Gruppe ändern.

Schritte

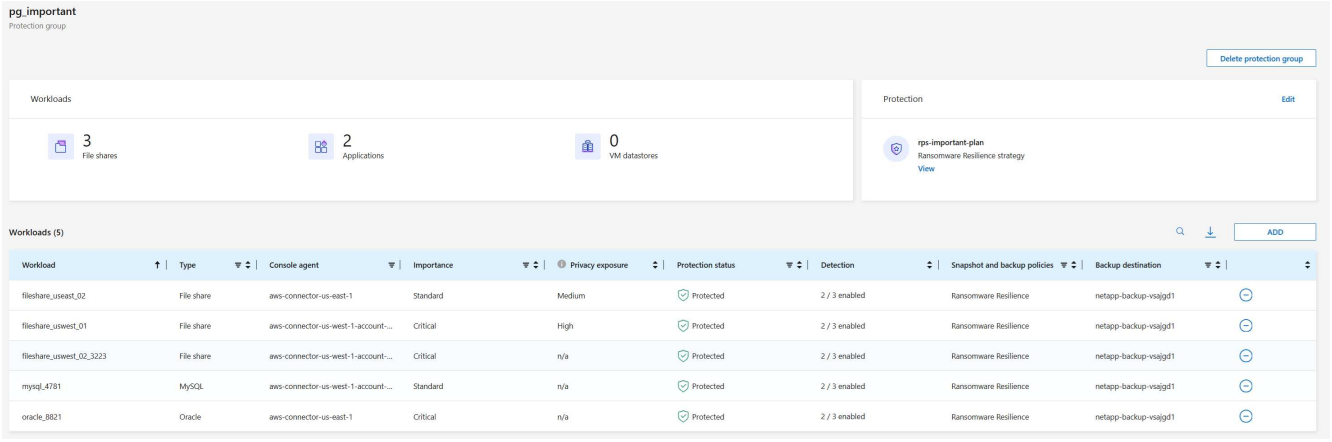
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Registerkarte **Schutzgruppen** und dann die Gruppe aus, deren Richtlinie Sie ändern möchten.
3. Wählen Sie auf der Übersichtsseite der Schutzgruppe **Schutz bearbeiten** aus.
4. Wählen Sie eine vorhandene Schutzrichtlinie aus, die angewendet werden soll, oder wählen Sie **Hinzufügen**, um eine neue Schutzrichtlinie zu erstellen. Weitere Informationen zum Hinzufügen einer Schutzrichtlinie finden Sie unterErstellen einer Schutzrichtlinie . Wählen Sie dann **Speichern**.
5. Wählen Sie in der Übersicht der Sicherungsziele ein vorhandenes Sicherungsziel aus oder **fügen Sie ein neues Sicherungsziel hinzu**.
6. Wählen Sie **Weiter** aus, um Ihre Änderungen zu überprüfen.

Entfernen von Workloads aus einer Gruppe

Möglicherweise müssen Sie später Arbeitslasten aus einer vorhandenen Gruppe entfernen.

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Registerkarte „Schutzgruppen“ aus.
3. Wählen Sie die Gruppe aus, aus der Sie eine oder mehrere Workloads entfernen möchten.



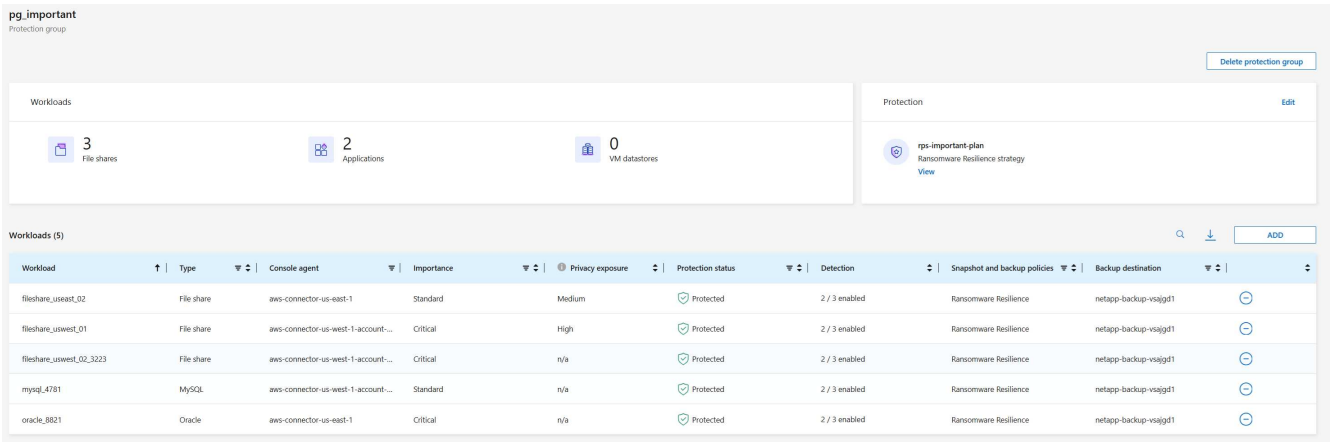
4. Wählen Sie auf der Seite der ausgewählten Schutzgruppe die Arbeitslast aus, die Sie aus der Gruppe entfernen möchten, und wählen Sie die *Aktionen*••• Option.
5. Wählen Sie im Menü „Aktionen“ die Option „Arbeitslast entfernen“ aus.
6. Bestätigen Sie, dass Sie die Arbeitslast entfernen möchten, und wählen Sie **Entfernen**.

Löschen der Schutzgruppe

Durch das Löschen der Schutzgruppe werden die Gruppe und ihr Schutz entfernt, die einzelnen Workloads werden jedoch nicht entfernt.

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Registerkarte „Schutzgruppen“ aus.
3. Wählen Sie die Gruppe aus, aus der Sie eine oder mehrere Workloads entfernen möchten.



4. Wählen Sie auf der Seite mit der ausgewählten Schutzgruppe oben rechts **Schutzgruppe löschen** aus.
5. Bestätigen Sie, dass Sie die Gruppe löschen möchten, und wählen Sie **Löschen**.

Verwalten Sie Strategien zum Schutz vor Ransomware

Sie können eine Ransomware-Strategie löschen.

Durch eine Ransomware-Schutzstrategie geschützte Workloads anzeigen

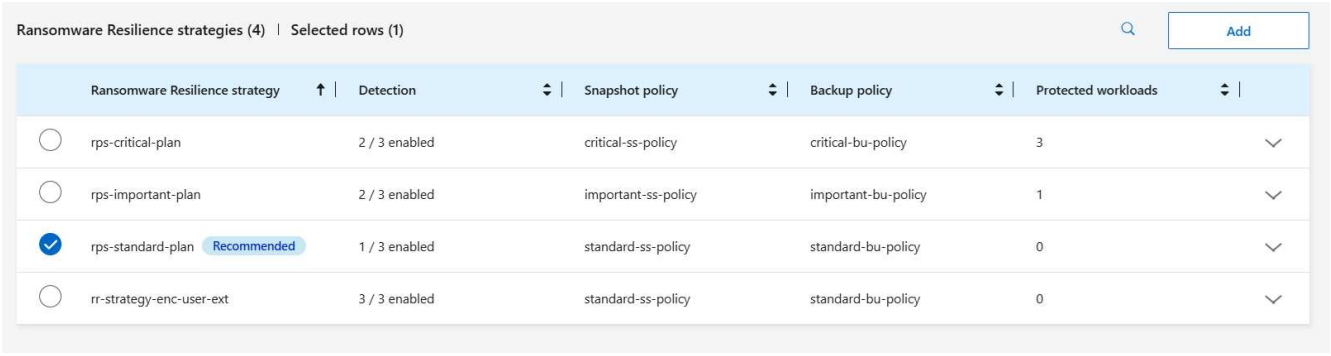
Bevor Sie eine Ransomware-Schutzstrategie löschen, möchten Sie möglicherweise prüfen, welche Workloads durch diese Strategie geschützt sind.

Sie können die Arbeitslasten aus der Liste der Strategien oder beim Bearbeiten einer bestimmten Strategie anzeigen.

Schritte zum Anzeigen von Strategien

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Option „Schutzstrategien verwalten“ aus.

   Auf der Seite mit den Ransomware-Schutzstrategien wird eine Liste mit Strategien angezeigt.



3. Wählen Sie auf der Seite „Ransomware-Schutzstrategien“ in der Spalte „Geschützte Workloads“ den Abwärtspfeil am Ende der Zeile aus.

Löschen einer Ransomware-Schutzstrategie

Sie können eine Schutzstrategie löschen, die derzeit keinen Workloads zugeordnet ist.

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Option „Schutzstrategien verwalten“ aus.
3. Wählen Sie auf der Seite „Strategien verwalten“ die Option „Aktionen“ aus. ••• Option für die Strategie, die Sie löschen möchten.
4. Wählen Sie im Menü „Aktionen“ die Option „Richtlinie löschen“ aus.

Scannen Sie mit NetApp Data Classification in Ransomware Resilience nach personenbezogenen Daten

Innerhalb von NetApp Ransomware Resilience können Sie NetApp Data Classification

verwenden, um die Daten in einer Dateifreigabe-Workload zu scannen und zu klassifizieren. Durch die Klassifizierung von Daten können Sie feststellen, ob der Datensatz personenbezogene Daten (PII) enthält, die das Sicherheitsrisiko erhöhen können. Die Datenklassifizierung ist eine Kernkomponente der NetApp Console und ohne zusätzliche Kosten verfügbar.

"Datenklassifizierung"nutzt KI-gesteuerte natürliche Sprachverarbeitung für die kontextbezogene Datenanalyse und -kategorisierung und bietet umsetzbare Einblicke in Ihre Daten, um Compliance-Anforderungen zu erfüllen, Sicherheitslücken zu erkennen, Kosten zu optimieren und die Migration zu beschleunigen.

Dieser Prozess kann sich auf die Wichtigkeit der Arbeitslast auswirken, um sicherzustellen, dass Sie über den entsprechenden Schutz verfügen.

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Identifizieren Sie Datenschutzrisiken mithilfe der Datenklassifizierung

Bevor Sie die Datenklassifizierung innerhalb von Ransomware Resilience verwenden, benötigen Sie"um die Datenklassifizierung zum Scannen Ihrer Daten zu aktivieren" .

Sie können die Datenklassifizierung auf der Schutzseite von Ransomware Resilience bereitstellen. Befolgen Sie die Schritte zur Ermittlung der Datenschutzrisiken. Wenn Sie **Exposure identifizieren** auswählen und die Datenklassifizierung noch nicht bereitgestellt haben, können Sie sie in einem Dialogfeld aktivieren.

Weitere Informationen zur Datenklassifizierung finden Sie unter:

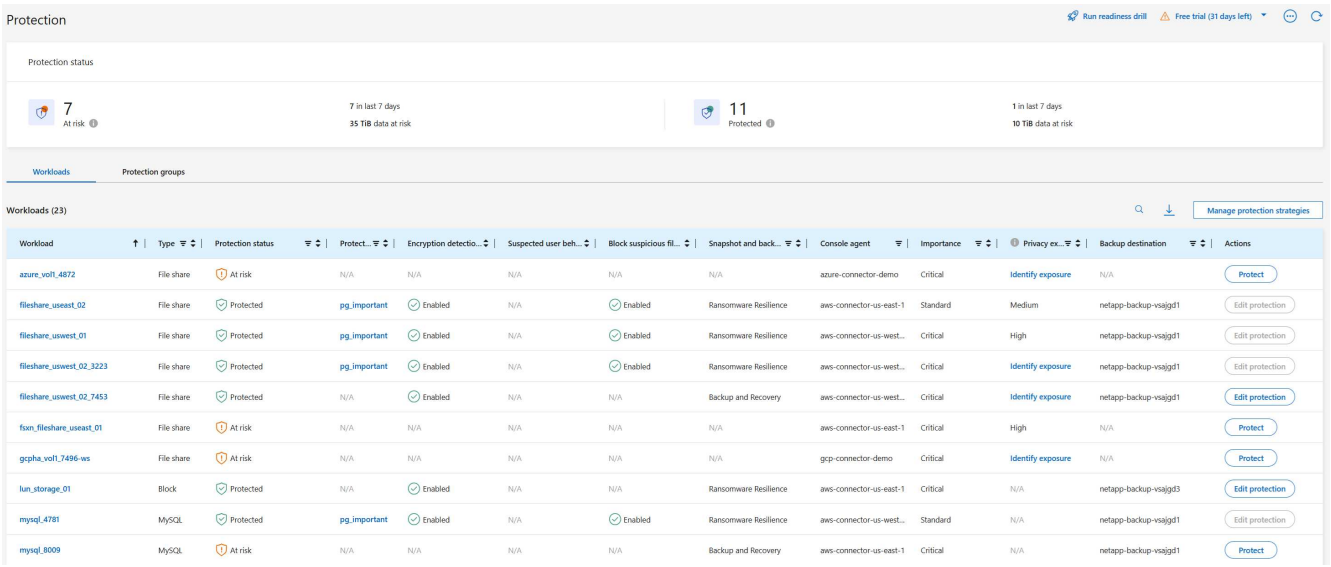
- "Erfahren Sie mehr über die Datenklassifizierung"
- "Kategorien personenbezogener Daten"
- "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten"

Bevor Sie beginnen

Das Scannen nach PII-Daten in Ransomware Resilience ist verfügbar, wenn Sie"bereitgestellte Datenklassifizierung" . Die Datenklassifizierung ist als Teil der Konsole ohne zusätzliche Kosten verfügbar und kann vor Ort oder in der Kunden-Cloud bereitgestellt werden.

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Suchen Sie auf der Seite „Schutz“ in der Spalte „Arbeitslast“ nach einer Arbeitslast für die Dateifreigabe.



3. Um die Datenklassifizierung zu aktivieren und Ihre Daten auf PII zu scannen, wählen Sie in der Spalte **Datenschutzgefährdung** die Option **Gefährdung identifizieren** aus.

> Wenn Sie die Datenklassifizierung nicht bereitgestellt haben, wird durch Auswahl von **Exposure identifizieren** ein Dialogfeld zum Bereitstellen der Datenklassifizierung geöffnet. Wählen Sie **Bereitstellen**. Nachdem Sie die Datenklassifizierung bereitgestellt haben, können Sie zur Seite „Schutz“ zurückkehren und dann „Gefährdung identifizieren“ auswählen.

Ergebnis

Das Scannen kann je nach Größe und Anzahl der Dateien mehrere Minuten dauern. Während des Scans zeigt die Seite „Schutz“ an, dass Dateien identifiziert werden, und stellt eine Dateianzahl bereit. Wenn der Scanvorgang abgeschlossen ist, wird in der Spalte „Datenschutzgefährdung“ die Gefährdungsstufe als „Niedrig“, „Mittel“ oder „Hoch“ eingestuft.

Überprüfen Sie die Datenschutzbestimmungen

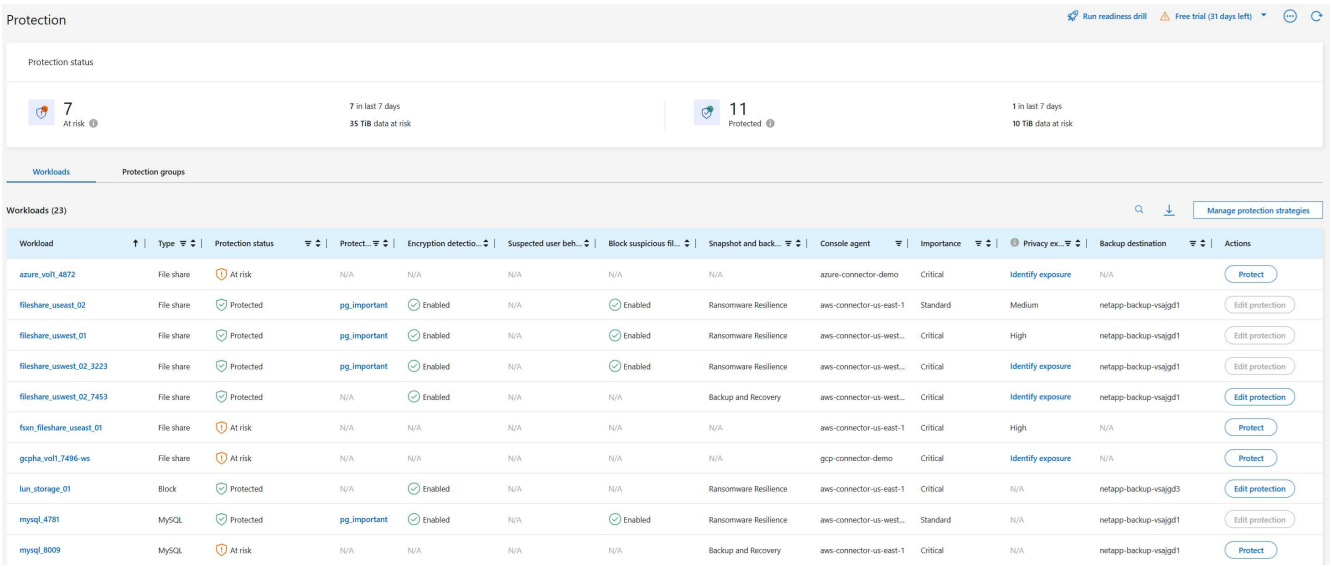
Bewerten Sie das Risiko, nachdem die Datenklassifizierung nach PII gesucht hat.

PII-Daten werden einer von drei Kategorien zugeordnet:

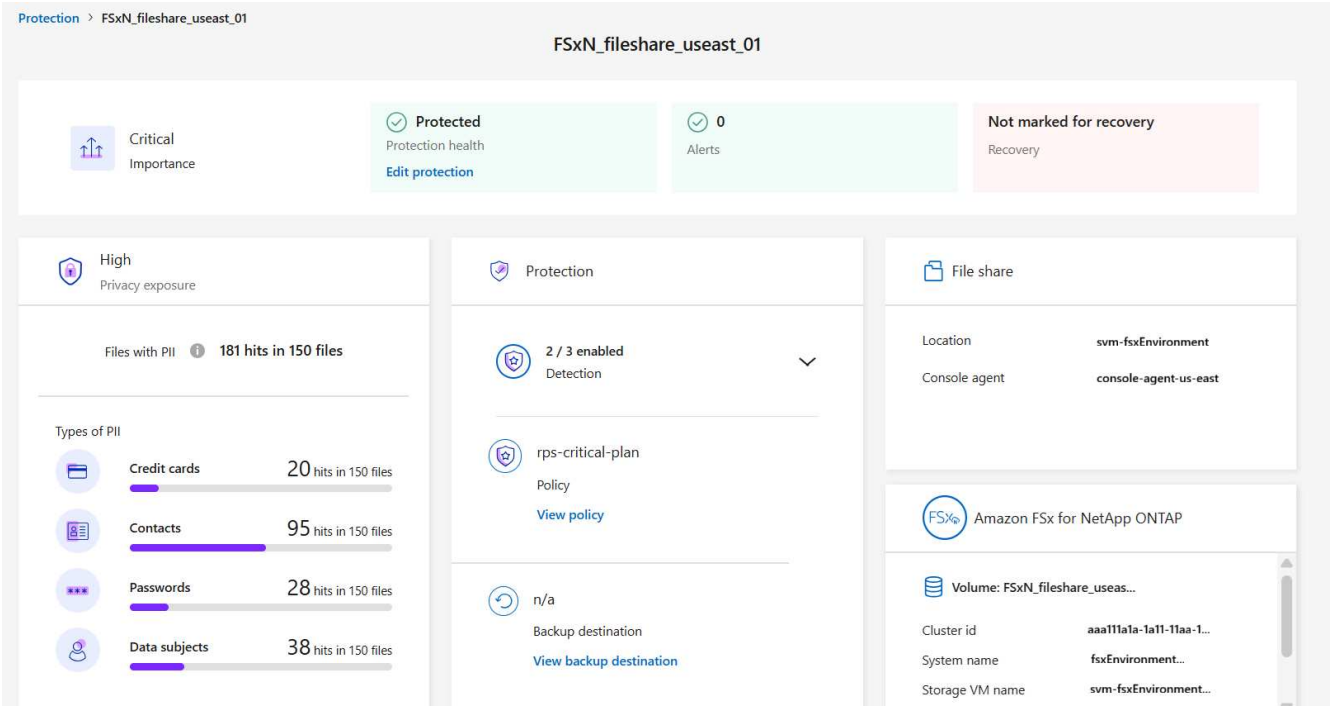
- **Hoch**: Mehr als 70 % der Dateien enthalten PII
- **Mittel**: Mehr als 30 % und weniger als 70 % der Dateien enthalten PII
- **Niedrig**: Mehr als 0 % und weniger als 30 % der Dateien enthalten PII

Schritte

1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Suchen Sie auf der Seite „Schutz“ in der Spalte „Arbeitslast“ nach der Arbeitslast der Dateifreigabe, die in der Spalte „Datenschutzgefährdung“ einen Status anzeigt.



3. Wählen Sie den Workload-Link in der Workload-Spalte aus, um Details zum Workload anzuzeigen.



4. Sehen Sie sich auf der Seite „Workloaddetails“ die Details in der Kachel „Datenschutzgefährdung“ an.

Auswirkungen der Offenlegung der Privatsphäre auf die Bedeutung der Arbeitsbelastung

Änderungen der Datenschutzbelastung können sich auf die Arbeitsbelastung auswirken.

Bei Offenlegung der Privatsphäre:	Aus dieser Datenschutzbelehrung:	Zu dieser Datenschutzbeeinträchtigung:	Dann bewirkt die Arbeitslastwichtigkeit Folgendes: .
Abnahme	Hoch, Mittel oder Niedrig	Mittel, Niedrig oder Keine	Bleibt gleich

Bei Offenlegung der Privatsphäre:	Aus dieser Datenschutzbelehrung:	Zu dieser Datenschutzbeeinträchtigung:	Dann bewirkt die Arbeitslastwichtigkeit Folgendes: .
Erhöht	Keine	Niedrig	Bleibt beim Standard
	Niedrig	Medium	Änderungen von Standard zu Wichtig
	Niedrig oder Mittel	Hoch	Änderungen von Standard oder Wichtig zu Kritisch

Weitere Informationen

Einzelheiten zur Datenklassifizierung finden Sie in der Dokumentation zur Datenklassifizierung:

- "Erfahren Sie mehr über die Datenklassifizierung"
- "Kategorien personenbezogener Daten"
- "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten"