Nutzen Sie Ransomware-Resilienz

NetApp Ransomware Resilience

NetApp
February 17, 2026

Inhalt

Nutzen Sie Ransomware-Resilienz . . . 1
Überwachen Sie den Workload-Zustand mit dem NetApp Ransomware Resilience Dashboard . . . 1
Überprüfen des Workload-Zustands mithilfe des Dashboards . . . 1
Überprüfen Sie die Schutzempfehlungen auf dem Dashboard . . . 2
Exportieren Sie Schutzdaten in CSV-Dateien . . . 4
Zugriff auf die technische Dokumentation . . . 5
Workloads schützen . . . 5
Schützen Sie Workloads mit NetApp Ransomware Resilience -Schutzstrategien . . . 5
Scannen Sie mit NetApp Data Classification in Ransomware Resilience nach personenbezogenen Daten . . . 21
Warnmeldungen in NetApp Ransomware Resilience verwalten . . . 24
Warnungen anzeigen . . . 26
Auf eine Warn-E-Mail antworten . . . 26
Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten . . . 27
Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden). . . . 28
Vorfälle abweisen, bei denen es sich nicht um potenzielle Angriffe handelt . . . 29
Liste der betroffenen Dateien anzeigen . . . 31
Wiederherstellung nach einem Ransomware-Angriff (nachdem die Vorfälle neutralisiert wurden) mit NetApp Ransomware Resilience . . . 32
Anzeigen von Workloads, die zur Wiederherstellung bereit sind . . . 33
Wiederherstellen einer von SnapCenter verwalteten Arbeitslast . . . 34
Wiederherstellen einer Arbeitslast, die nicht von SnapCenter verwaltet wird . . . 34
Berichte in NetApp Ransomware Resilience herunterladen . . . 42

Nutzen Sie Ransomware-Resilienz

Überwachen Sie den Workload-Zustand mit dem NetApp Ransomware Resilience Dashboard

Das NetApp Ransomware Resilience Dashboard bietet auf einen Blick Informationen zum Schutzzustand Ihrer Workloads. Sie können schnell feststellen, welche Workloads gefährdet oder geschützt sind, welche Workloads von einem Vorfall betroffen sind oder sich in der Wiederherstellung befinden und den Umfang des Schutzes einschätzen, indem Sie sich ansehen, wie viel Speicher geschützt oder gefährdet ist.

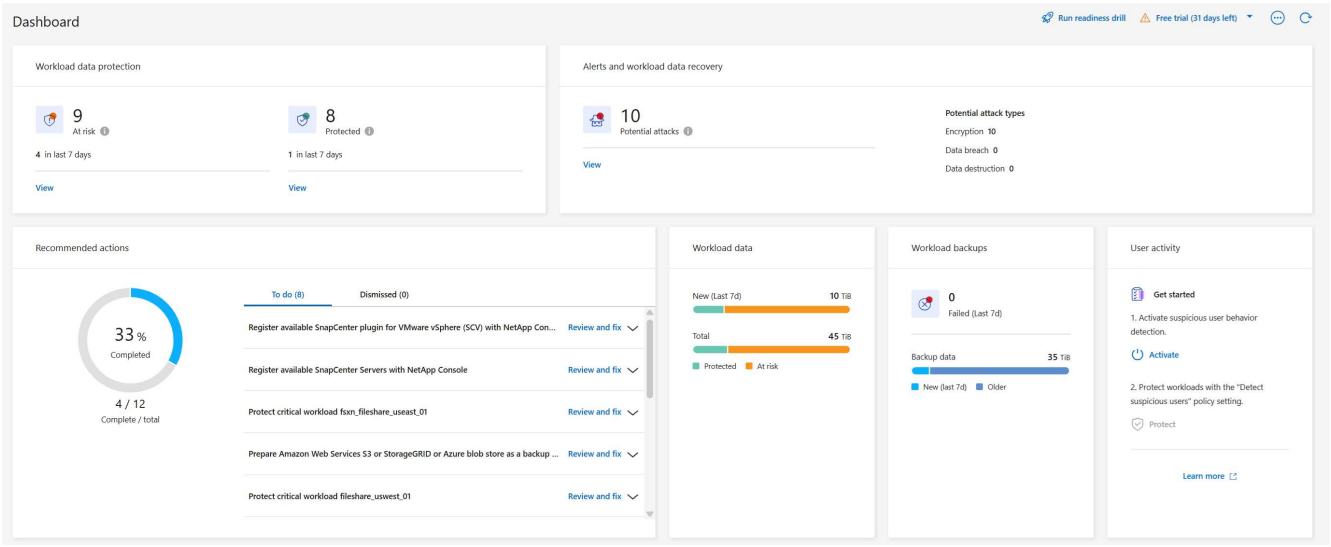
Über das Dashboard können Sie Schutzvorschläge einsehen, Einstellungen ändern und Berichte herunterladen.

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

Überprüfen des Workload-Zustands mithilfe des Dashboards

Schritte

1. Nachdem die Konsole Ihre Workloads erkannt hat, zeigt das Ransomware Resilience-Dashboard den Datenschutzstatus der Workloads an.



2. Vom Dashboard aus können Sie in jedem Bereich die folgenden Aktionen ausführen:

   - **Schutz von Workload-Daten**: Wählen Sie **Alle anzeigen** aus, um auf der Seite „Schutz“ alle gefährdeten oder geschützten Workloads anzuzeigen. Wenn die Schutzstufen nicht mit einer Schutzrichtlinie übereinstimmen, sind Workloads gefährdet. Weitere Informationen finden Sie unter "Workloads schützen" .

Wählen Sie den Tooltip „i“ aus, um Tipps zu diesen Daten anzuzeigen. Um das Arbeitslastlimit zu erhöhen, wählen Sie in dieser Notiz **Arbeitslastlimit erhöhen** aus. Wenn Sie diese Option auswählen, gelangen Sie zur Seite „Konsolensupport“, auf der Sie ein Fallticket erstellen können.

- **Warnungen und Wiederherstellung von Workload-Daten**: Wählen Sie **Alle anzeigen** aus, um aktive Vorfälle anzuzeigen, die sich auf Ihren Workload ausgewirkt haben, nach der Neutralisierung der Vorfälle zur Wiederherstellung bereit sind oder sich in der Wiederherstellung befinden. Weitere Informationen finden Sie unter "Auf eine erkannte Warnung reagieren" .
  - Ein Vorfall wird in einen der folgenden Zustände eingeteilt:
    - Neu
    - Entlassen
    - Abweisen
    - Gelöst
  - Eine Warnung kann einen der folgenden Status haben:
    - Neu
    - Inaktiv
  - Ein Workload kann einen der folgenden Wiederherstellungsstatus haben:
    - Wiederherstellung erforderlich
    - Im Gange
    - Restauriert
    - Fehlgeschlagen
- **Empfohlene Maßnahmen**: Um den Schutz zu erhöhen, überprüfen Sie jede Empfehlung und wählen Sie dann **Überprüfen und beheben**.

  Sehen "Überprüfen Sie die Schutzvorschläge auf dem Dashboard" oder "Workloads schützen" .

  Ransomware Resilience zeigt 24 Stunden lang neue Empfehlungen seit Ihrem letzten Besuch des Dashboards mit dem Tag „Neu“ an. Die Aktionen werden in der Reihenfolge ihrer Priorität angezeigt, wobei die wichtigsten ganz oben stehen. Überprüfen Sie jede Empfehlung, setzen Sie sie um oder verwerfen Sie sie.

In der Gesamtzahl der Aktionen sind die von Ihnen abgelehnten Aktionen nicht enthalten.

- **Arbeitslastdaten**: Überwachen Sie Änderungen im Schutzumfang der letzten 7 Tage.
- **Workload-Backups**: Überwachen Sie Änderungen an Workload-Backups, die von Ransomware Resilience erstellt wurden und in den letzten 7 Tagen fehlgeschlagen oder erfolgreich abgeschlossen wurden.

Überprüfen Sie die Schutzempfehlungen auf dem Dashboard

Ransomware Resilience bewertet den Schutz Ihrer Workloads und empfiehlt Maßnahmen zur Verbesserung dieses Schutzes.

Sie können eine Empfehlung prüfen und darauf reagieren, wodurch sich der Status der Empfehlung in „Abgeschlossen“ ändert. Oder Sie können es verwerfen, wenn Sie später darauf reagieren möchten. Durch das Ablehnen einer Aktion wird die Empfehlung in eine Liste abgelehnter Aktionen verschoben, die Sie später

überprüfen können.

Hier ist eine Auswahl der Empfehlungen von Ransomware Resilience.

Empfehlung	Beschreibung	So lösen Sie
Fügen Sie eine Ransomware-Schutzrichtlinie hinzu.	Die Arbeitslast ist derzeit nicht geschützt.	Weisen Sie der Arbeitslast eine Richtlinie zu. Weitere Informationen finden Sie unter "Schützen Sie Workloads vor Ransomware-Angriffen" .
Stellen Sie eine Verbindung zu SIEM her, um Bedrohungen zu melden.	Senden Sie Daten zur Bedrohungsanalyse und -erkennung an ein Sicherheits- und Ereignismanagementsystem (SIEM).	Geben Sie die SIEM/XDR-Serverdetails ein, um die Bedrohungserkennung zu aktivieren. Weitere Informationen finden Sie unter "Konfigurieren der Schutzeinstellungen" .
Aktivieren Sie Workload-konsistenten Schutz für Anwendungen oder VMware.	Diese Workloads werden nicht von der SnapCenter -Software oder dem SnapCenter Plug-in for VMware vSphere verwaltet.	Aktivieren Sie den Workload-konsistenten Schutz, damit sie von SnapCenter verwaltet werden. Weitere Informationen finden Sie unter "Schützen Sie Ihre Workload vor Ransomware-Angriffen" .
Verbessern Sie die Sicherheitslage des Systems	NetApp Digital Advisor hat mindestens ein hohes oder kritisches Sicherheitsrisiko identifiziert.	Überprüfen Sie alle Sicherheitsrisiken im NetApp Digital Advisor. Siehe "Digital Advisor -Dokumentation" .
Machen Sie eine Politik stärker.	Einige Workloads sind möglicherweise nicht ausreichend geschützt. Stärken Sie den Schutz von Workloads mit einer Richtlinie.	Erhöhen Sie die Aufbewahrung, fügen Sie Backups hinzu, erzwingen Sie unveränderliche Backups, blockieren Sie verdächtige Dateierweiterungen, aktivieren Sie die Erkennung auf sekundärem Speicher und mehr. Weitere Informationen finden Sie unter "Schützen Sie Workloads vor Ransomware-Angriffen" .
Bereiten Sie <Sicherungsanbieter> als Sicherungsziel vor, um Ihre Workload-Daten zu sichern.	Die Arbeitslast hat derzeit keine Sicherungsziele.	Fügen Sie diesem Workload Sicherungsziele hinzu, um ihn zu schützen. Weitere Informationen finden Sie unter "Konfigurieren der Schutzeinstellungen" .
Schützen Sie kritische oder sehr wichtige Anwendungs-Workloads vor Ransomware.	Auf der Seite „Schützen“ werden kritische oder sehr wichtige (je nach zugewiesener Prioritätsstufe) Anwendungs-Workloads angezeigt, die nicht geschützt sind.	Weisen Sie diesen Workloads eine Richtlinie zu. Weitere Informationen finden Sie unter "Schützen Sie Workloads vor Ransomware-Angriffen" .

Empfehlung	Beschreibung	So lösen Sie
Schützen Sie kritische oder sehr wichtige Dateifreigabe-Workloads vor Ransomware.	Auf der Seite „Schutz“ werden kritische oder sehr wichtige Workloads vom Typ „Dateifreigabe“ oder „Datenspeicher“ angezeigt, die nicht geschützt sind.	Weisen Sie jeder Arbeitslast eine Richtlinie zu. Weitere Informationen finden Sie unter "Schützen Sie Workloads vor Ransomware-Angriffen" .
Verfügbares SnapCenter Plugin für VMware vSphere (SCV) mit der Konsole registrieren	Eine VM-Workload ist nicht geschützt.	Weisen Sie der VM-Workload VM-konsistenten Schutz zu, indem Sie das SnapCenter -Plugin für VMware vSphere aktivieren. Weitere Informationen finden Sie unter "Schützen Sie Workloads vor Ransomware-Angriffen" .
Verfügbaren SnapCenter -Server mit der Konsole registrieren	Eine Anwendung ist nicht geschützt.	Weisen Sie der Arbeitslast anwendungskonsistenten Schutz zu, indem Sie SnapCenter Server aktivieren. Weitere Informationen finden Sie unter "Schützen Sie Workloads vor Ransomware-Angriffen" .
Überprüfen Sie neue Warnungen.	Es liegen neue Warnungen vor.	Überprüfen Sie die neuen Warnungen. Weitere Informationen finden Sie unter "Reagieren Sie auf eine erkannte Ransomware-Warnung" .

Schritte

1. Wählen Sie im Bereich „Empfohlene Aktionen“ in Ransomware Resilience eine Empfehlung aus und klicken Sie dann auf **Überprüfen und beheben**.
2. Um die Aktion auf einen späteren Zeitpunkt zu verschieben, wählen Sie **Verwerfen**.

   Die Empfehlung wird aus der Aufgabenliste gelöscht und erscheint in der Liste „Abgelehnt“.

   Sie können einen abgelehnten Eintrag später in einen Aufgabeneintrag ändern. Wenn Sie ein Element als erledigt markieren oder ein verworfenes Element in eine zu erledigende Aktion ändern, erhöht sich die Gesamtzahl der Aktionen um 1.

3. Um Informationen zum Umsetzen der Empfehlungen anzuzeigen, wählen Sie das Symbol **Informationen** aus.

Exportieren Sie Schutzdaten in CSV-Dateien

Sie können Daten exportieren und CSV-Dateien herunterladen, die Details zu Schutz, Warnungen und Wiederherstellung enthalten.

Sie können CSV-Dateien von jeder der Hauptmenüoptionen herunterladen:

- **Schutz**: Enthält den Status und die Details aller Workloads, einschließlich der Gesamtzahl der Workloads, die Ransomware Resilience als geschützt oder gefährdet kennzeichnet.
- **Warnungen**: Enthält den Status und die Details aller Warnungen, einschließlich der Gesamtzahl der

Warnungen und automatisierten Snapshots.

- **Wiederherstellung**: Enthält den Status und die Details aller Workloads, die wiederhergestellt werden müssen, einschließlich der Gesamtzahl der Workloads, die Ransomware Resilience als „Wiederherstellung erforderlich“, „In Bearbeitung“, „Wiederherstellung fehlgeschlagen“ und „Erfolgreich wiederhergestellt“ kennzeichnet.

Beim Herunterladen einer CSV-Datei von einer Seite werden nur die Daten dieser Seite enthalten.

Die CSV-Dateien enthalten Daten für alle Workloads auf allen Konsolensystemen.

Schritte

1. Wählen Sie im Dashboard „Ransomware-Resilienz“ die Option **Aktualisieren**. Option oben rechts zum Aktualisieren der Daten, die in den Dateien angezeigt werden.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie auf der Seite die Option **Herunterladen** aus. Option.
   - Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Berichte“ aus.
3. Wenn Sie die Option **Berichte** ausgewählt haben, wählen Sie eine der vorkonfigurierten benannten Dateien aus und wählen Sie dann **Herunterladen (CSV)** oder **Herunterladen (JSON)**.

Zugriff auf die technische Dokumentation

Sie können auf die technische Dokumentation zu Ransomware Resilience zugreifen unter"docs.netapp.com" oder innerhalb von Ransomware Resilience.

Schritte

1. Wählen Sie im Ransomware Resilience-Dashboard die vertikale *Aktionen* Option.
2. Wählen Sie eine dieser Optionen:
   - **Was ist neu**, um Informationen zu den Funktionen in der aktuellen oder früheren Version in den Versionshinweisen anzuzeigen.
   - **Dokumentation**, um die Homepage der Ransomware Resilience-Dokumentation und diese Dokumentation anzuzeigen.

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.

Wenn Sie Schutzstrategien für Amazon FSxN für ONTAP und Azure NetApp Files konfigurieren, konsultieren Sie "die Einschränkungen für jeden Dienst".

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.

Backup-Ziele sind für Workloads in Amazon FSx for NetApp ONTAP oder Azure NetApp Files nicht verfügbar. Führen Sie Backup-Vorgänge mit dem FSx for ONTAP-Backup-Service durch. Sie legen Backup-Richtlinien für Workloads in FSx for ONTAP in AWS fest, nicht in Ransomware Resilience. Die Backup-Richtlinien 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.

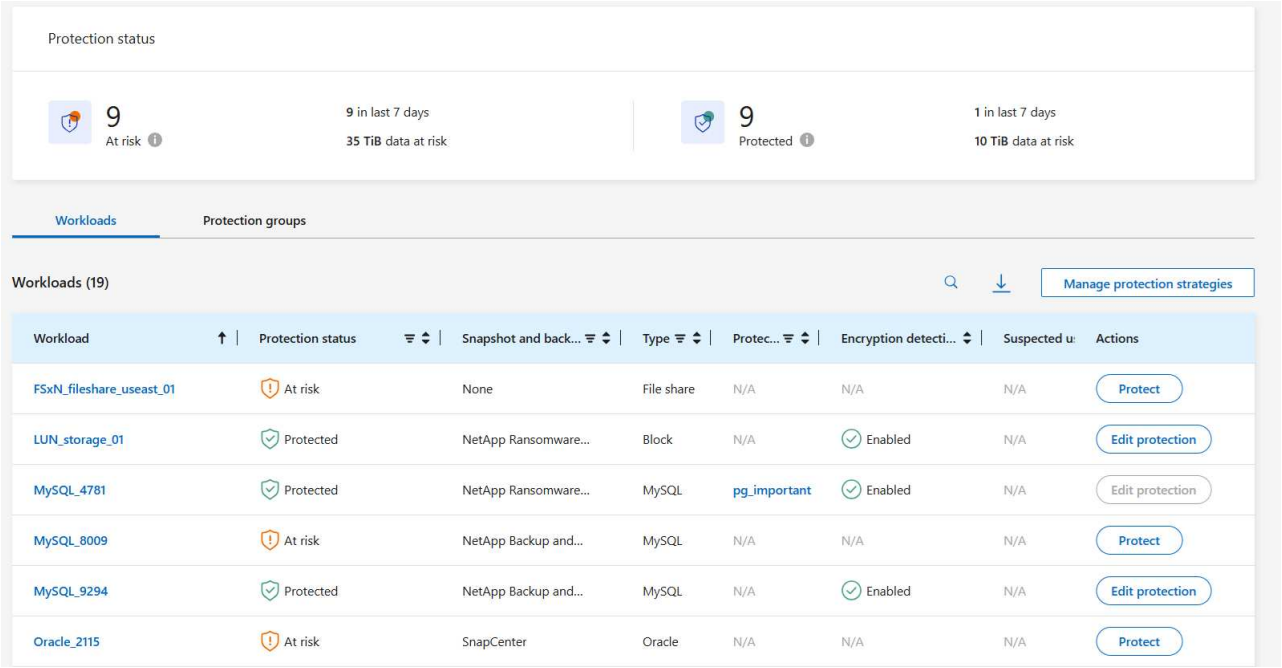
Anzeigen des Ransomware-Schutzes für eine Arbeitslast

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

Richtlinie nebene	Schnappschuss	Frequenz	Aufbewahrungsdauer (Tage)	Anzahl der Snapshot-Kopien	Maximale Anzahl von Snapshot-Kopien
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 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)

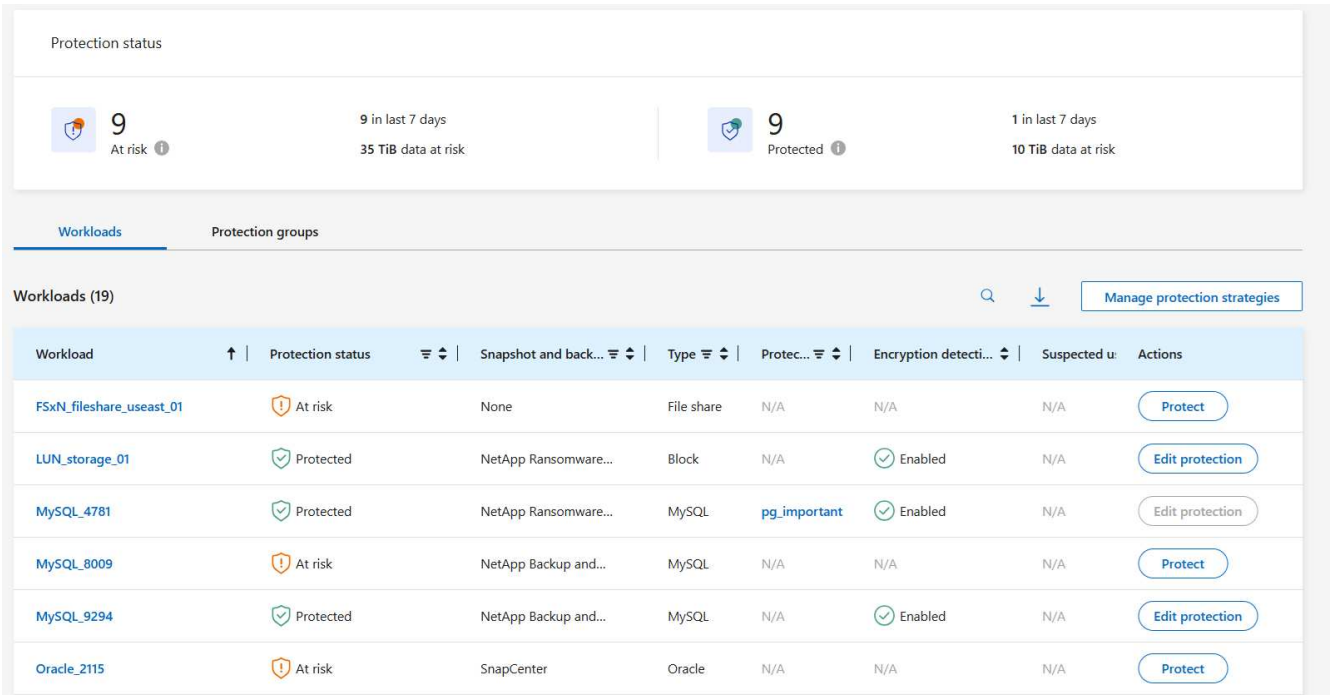
Wenn für die Arbeitslast keine Snapshot- oder Sicherungsrichtlinien vorhanden sind, können Sie eine Ransomware-Schutzstrategie erstellen, die die folgenden Richtlinien enthalten kann, die Sie in Ransomware

Resilience erstellen:

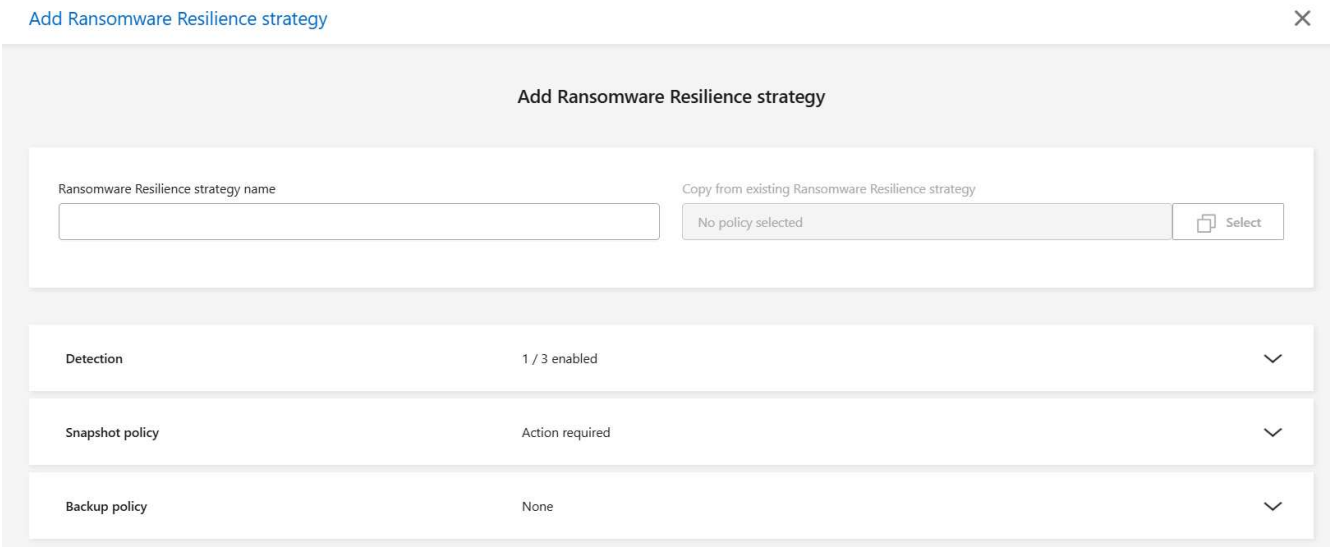
- Snapshot-Richtlinie
- Sicherungsrichtlinie
- Richtlinie zur Ransomware-Erkennung
- Sekundäre Replikation zu ONTAP

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

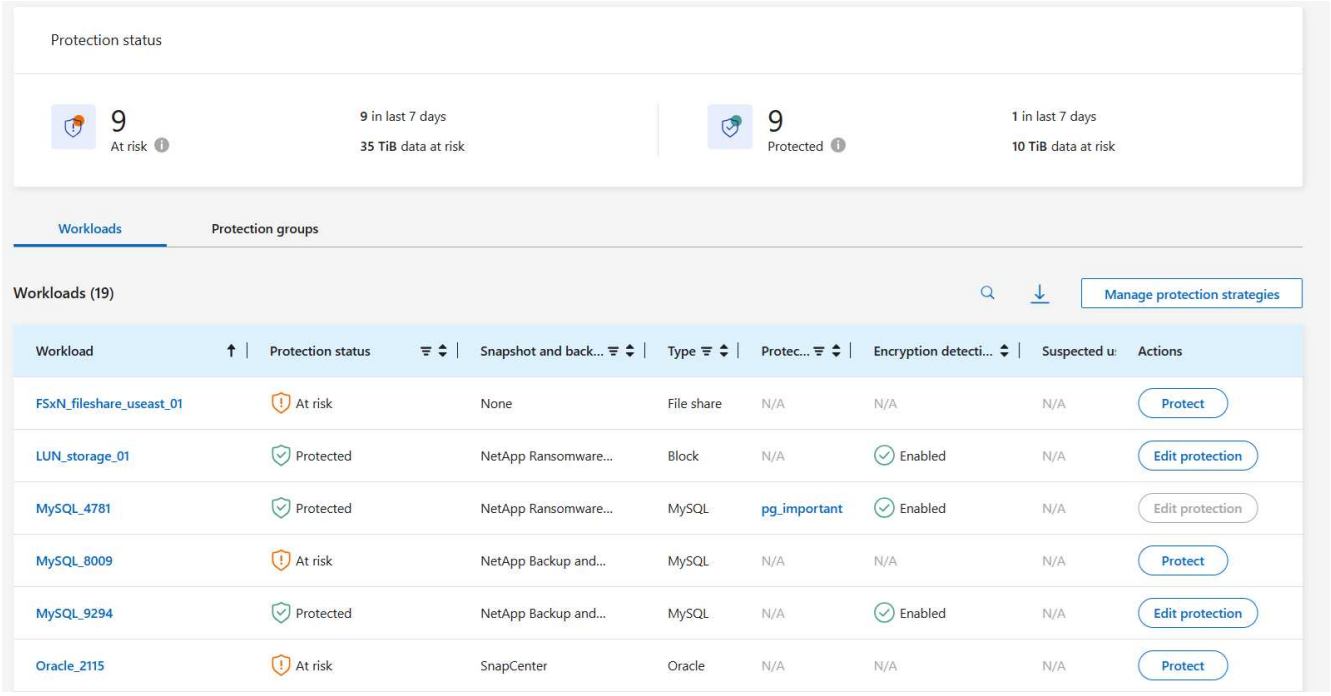
Mit Ransomware Resilience können Sie Workloads mit vorhandenem Snapshot- und Backup-Schutz, der in anderen NetApp -Produkten oder -Services verwaltet wird, entweder eine Erkennungsrichtlinie oder eine Schutzrichtlinie zuweisen. Andere Dienste wie Backup and Recovery und SnapCenter verwenden Richtlinien, 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 aus:

```
*Encryption detection*
*Suspicious user behavior detection*
*Block suspicious file extensions*
```

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.

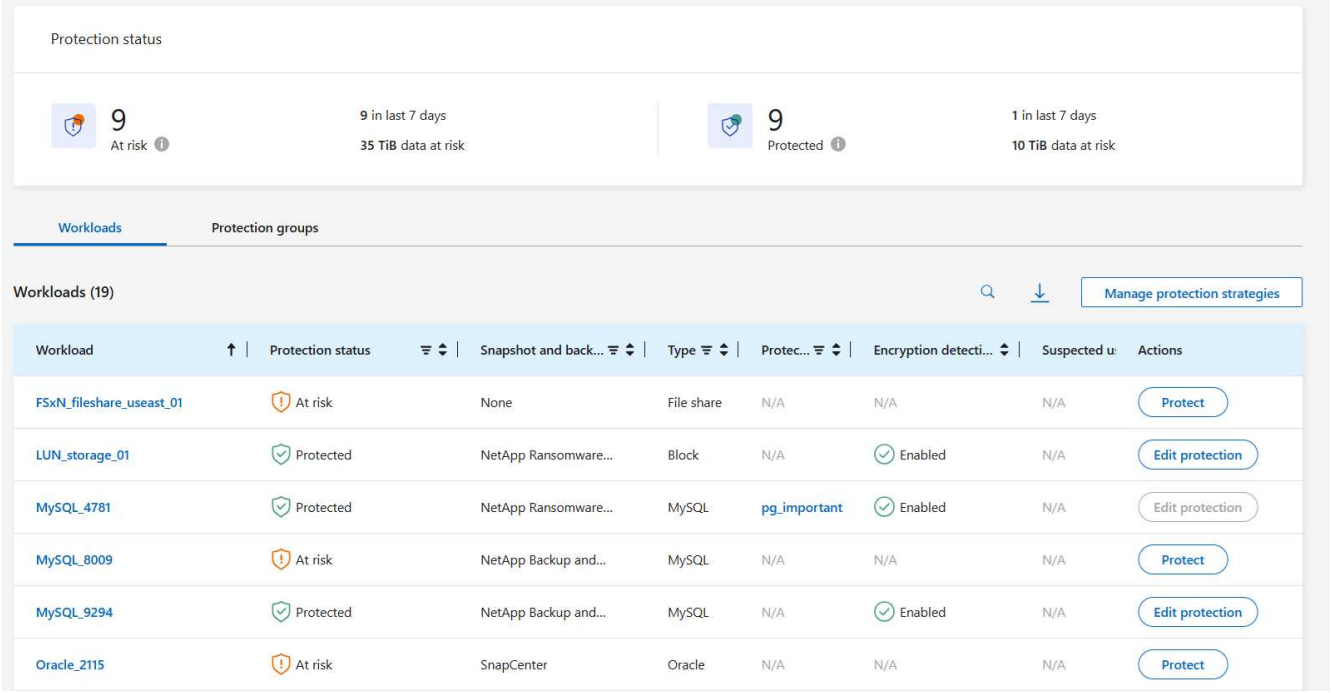
9. Wählen Sie **Weiter**.
10. Überprüfen Sie Ihre Auswahl. Wählen Sie **Erstellen**, um die Erkennung zu aktivieren.
11. Überprüfen Sie auf der Seite „Schutz“ den **Erkennungsstatus**, um zu bestätigen, dass die Erkennung aktiv ist.

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.

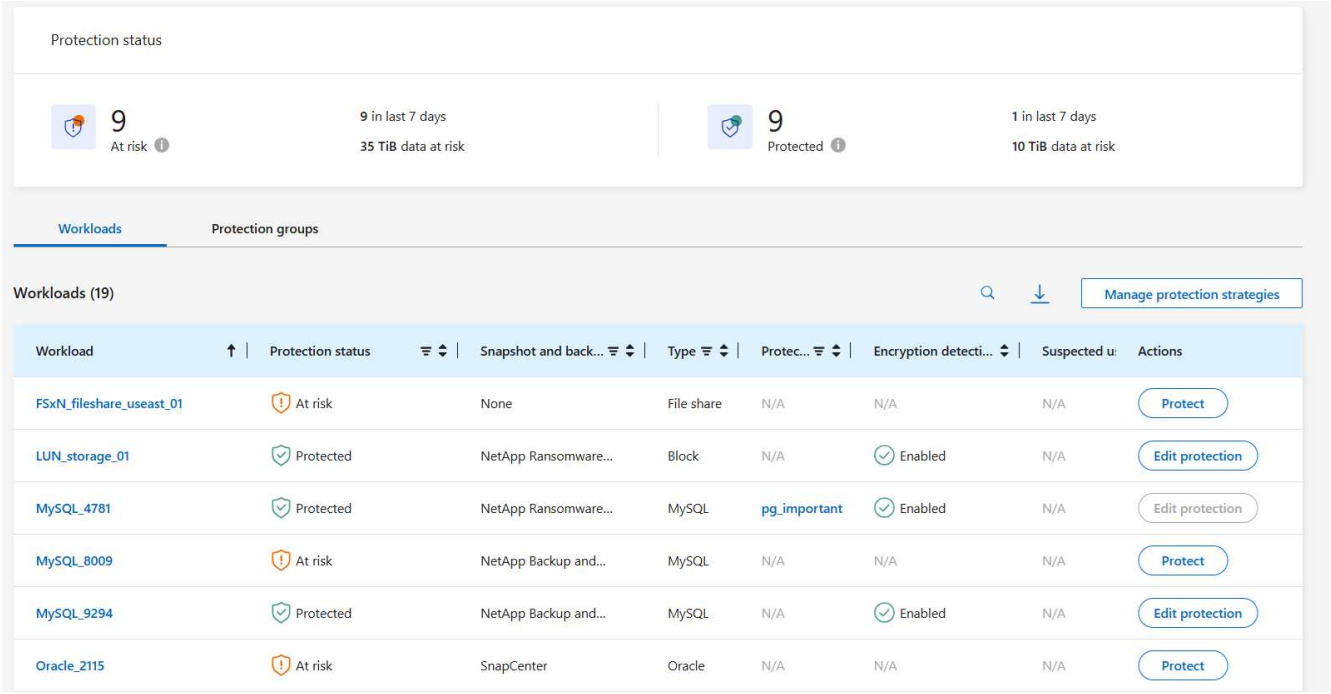
Erstellen einer Schutzgruppe

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.

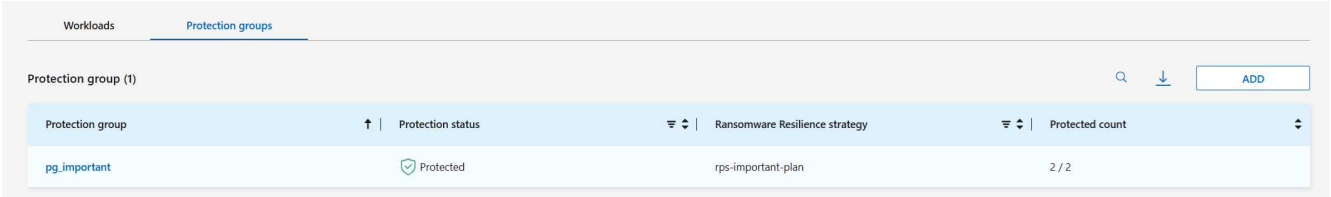
Sie können Gruppen unabhängig von ihrem Schutzstatus erstellen (d. h. nicht geschützte Gruppen und geschützte Gruppen). Wenn Sie einer Schutzgruppe eine Schutzrichtlinie hinzufügen, ersetzt die neue Schutzrichtlinie alle vorhandenen Richtlinien, einschließlich der von SnapCenter und NetApp Backup and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

Schritte

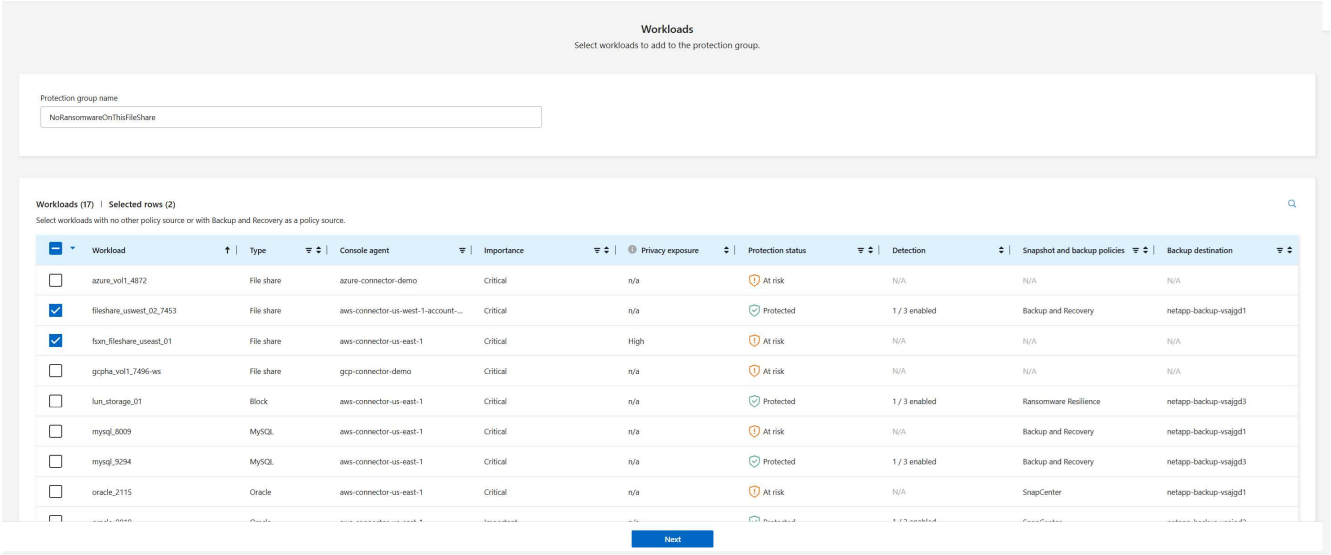
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



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



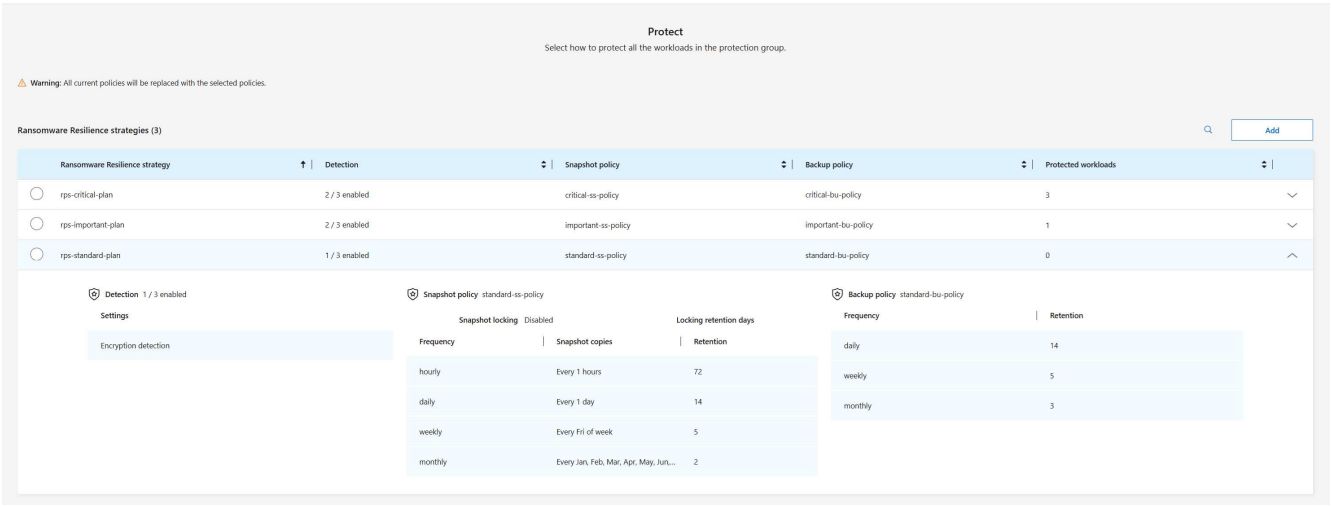
3. Wählen Sie **Hinzufügen**.



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, um den Schutz für diese Gruppe zu steuern.
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

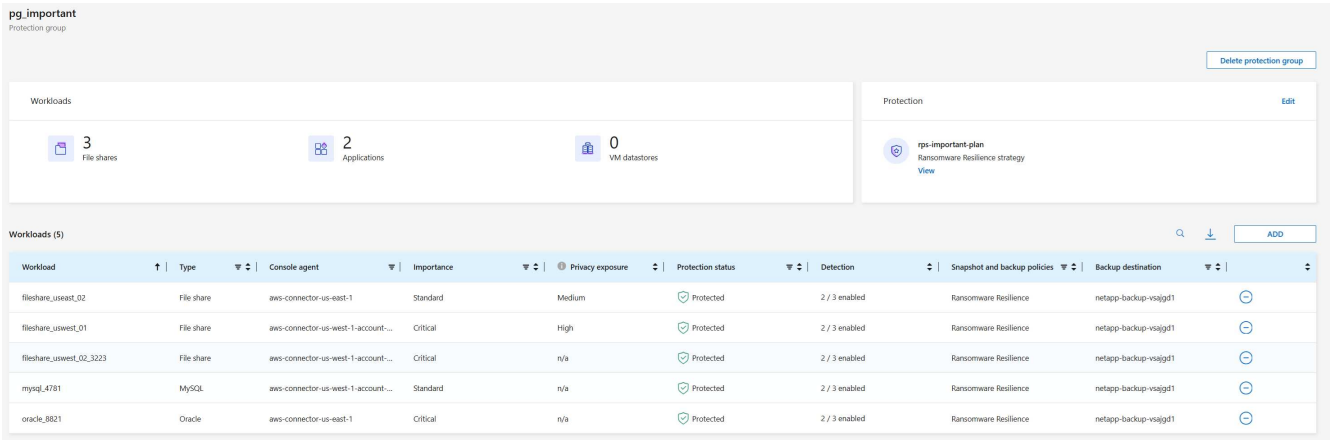
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Registerkarte **Schutzgruppen** und dann die Gruppe aus, deren Richtlinie Sie ändern möchten.
3. Wählen Sie auf der Übersichtsseite der Schutzgruppe **Schutz bearbeiten** aus.
4. Wählen Sie 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.



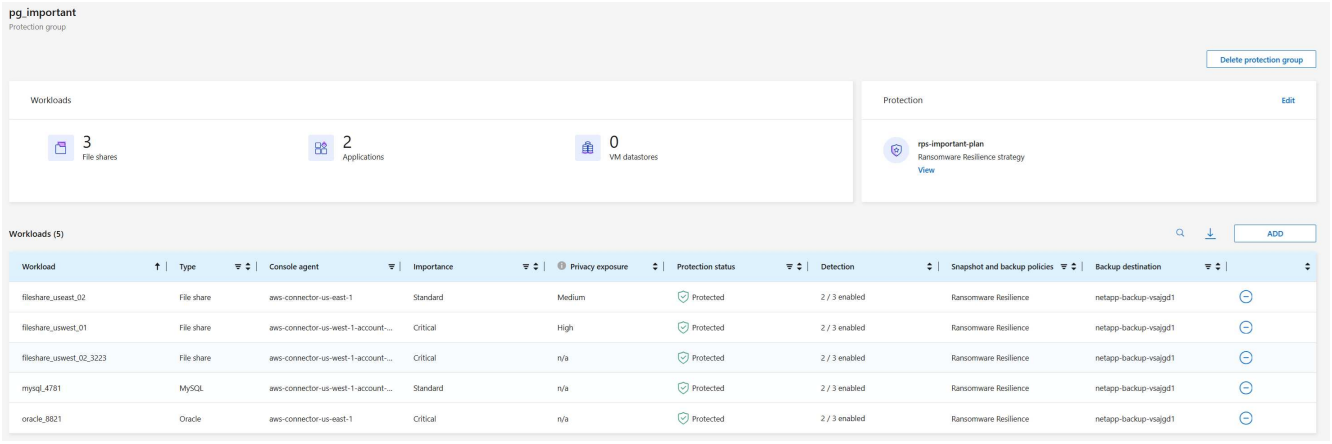
4. Wählen Sie auf der Seite der ausgewählten Schutzgruppe die Arbeitslast aus, die Sie aus der Gruppe entfernen möchten, und wählen Sie die *Aktionen*••• Option.
5. Wählen Sie im Menü „Aktionen“ die Option „Arbeitslast entfernen“ aus.
6. Bestätigen Sie, dass Sie die Arbeitslast entfernen möchten, und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

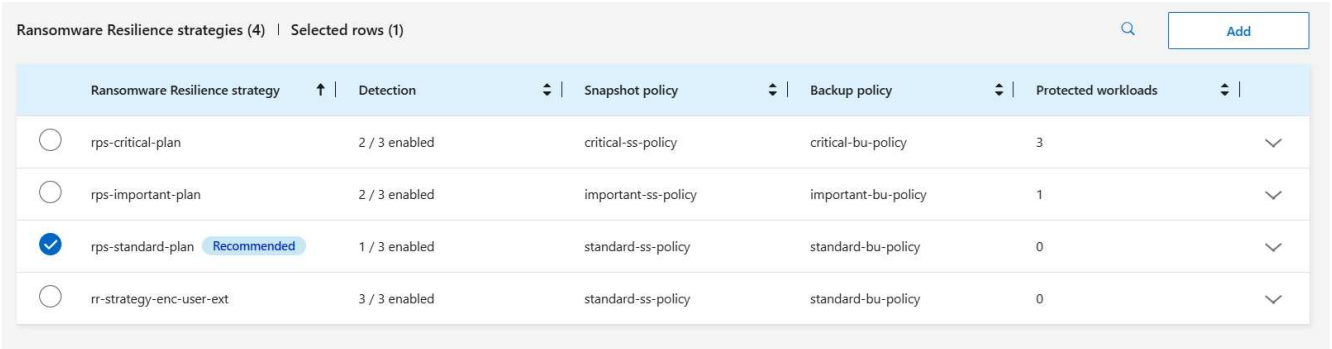
Bevor Sie eine Ransomware-Schutzstrategie löschen, möchten Sie möglicherweise prüfen, welche Workloads durch diese Strategie geschützt sind.

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:

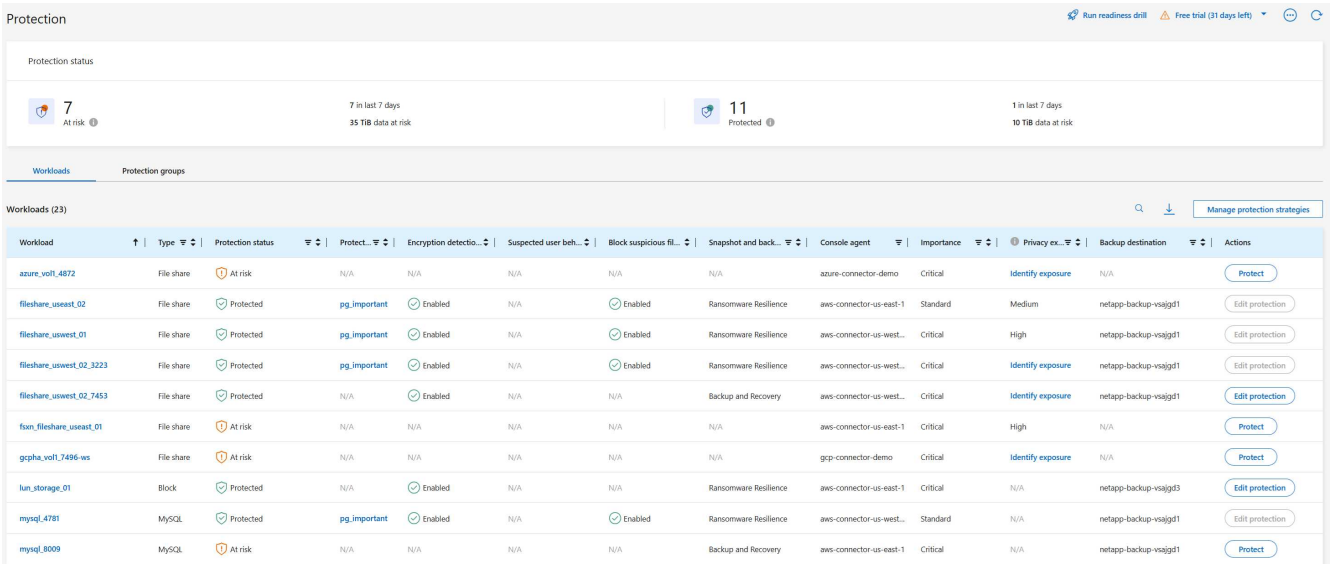
- "Erfahren Sie mehr über die Datenklassifizierung"
- "Kategorien personenbezogener Daten"
- "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten"

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.

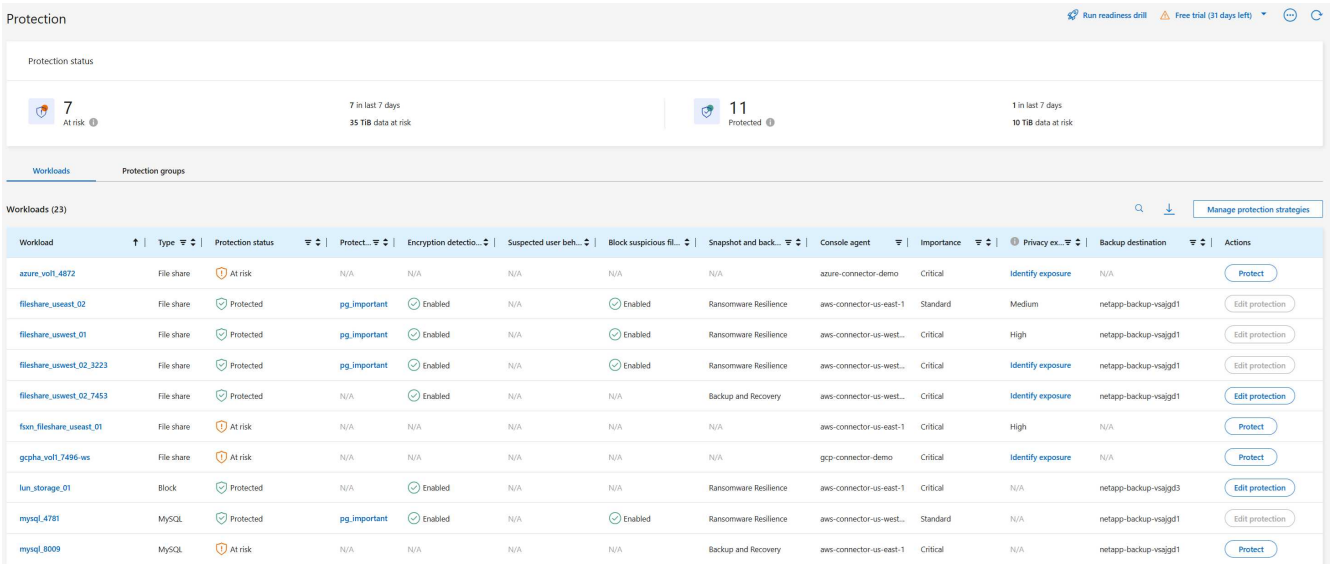
PII-Daten werden einer von drei Kategorien zugeordnet:

- **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

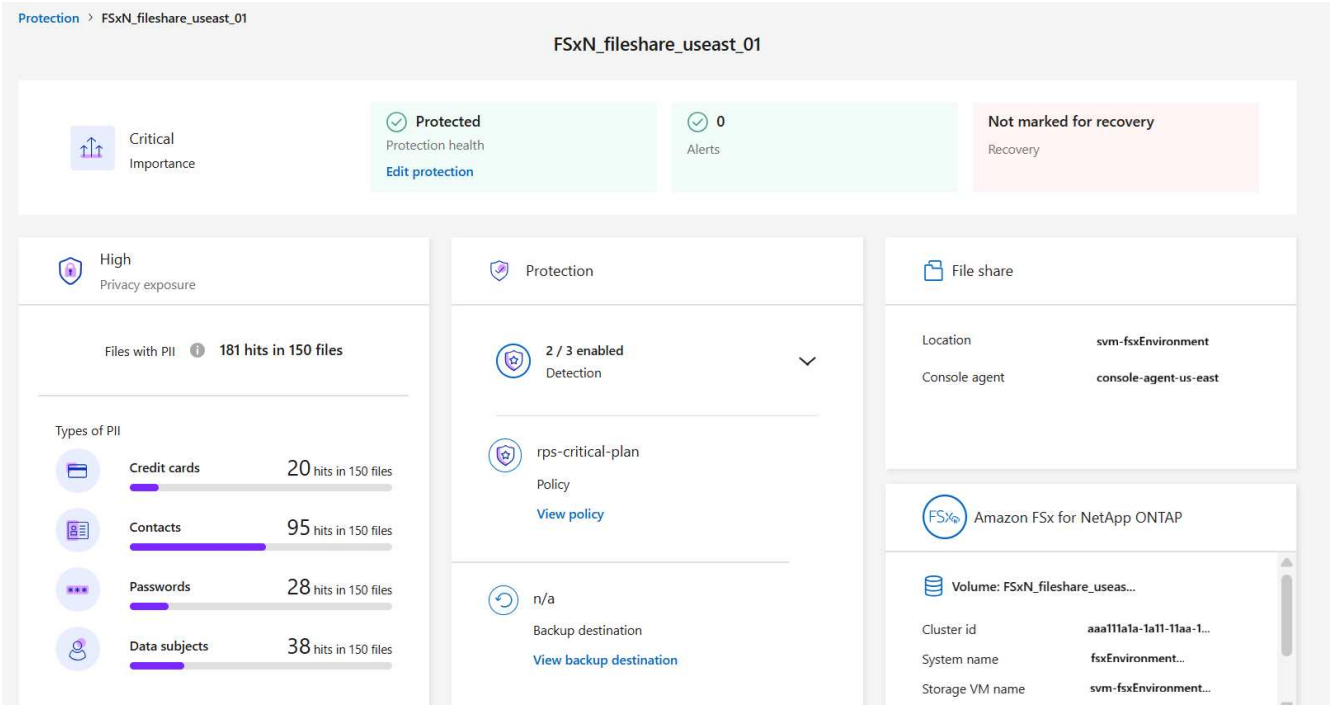
Schritte

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
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"

Warnmeldungen in NetApp Ransomware Resilience verwalten

Wenn NetApp Ransomware Resilience einen möglichen Angriff erkennt, wird eine Warnung auf dem Dashboard und im Benachrichtigungsbereich angezeigt. Ransomware Resilience erstellt sofort einen Snapshot. Überprüfen Sie das potenzielle Risiko auf der Registerkarte „Ransomware-Resilienz **Warnungen**“.

Wenn Ransomware Resilience einen möglichen Angriff erkennt, erscheint eine Benachrichtigung in den Console Notification-Einstellungen und eine E-Mail wird an die konfigurierten Adressen gesendet. Die E-Mail enthält Informationen über den Schweregrad, die betroffene Workload und einen Link zur Warnung im Tab **Alerts** von Ransomware Resilience.

Sie können Fehlalarme ignorieren oder sich für eine sofortige Wiederherstellung Ihrer Daten entscheiden.

Wenn Sie die Warnung verwerfen, lernt Ransomware Resilience dieses Verhalten, verknüpft es mit normalen Vorgängen und löst keine weitere Warnung aus.

Um mit der Wiederherstellung Ihrer Daten zu beginnen, markieren Sie die Warnung als „bereit zur Wiederherstellung“, damit Ihr Speicheradministrator mit dem Wiederherstellungsprozess beginnen kann.

Jede Warnung kann mehrere Vorfälle mit unterschiedlichem Umfang und Status umfassen. Überprüfen Sie alle Vorfälle.

Ransomware Resilience liefert sogenannte *Beweise* über die Ursache der Warnmeldung, beispielsweise die folgenden:

- Dateierweiterungen wurden erstellt oder geändert

- Dateierstellung mit einem Vergleich der erkannten und erwarteten Raten
- Dateilöschung mit einem Vergleich der erkannten und erwarteten Raten
- Bei hoher Verschlüsselung ohne Änderungen der Dateierweiterung

Eine Warnung wird wie folgt klassifiziert:

- **Potenzieller Angriff**: Eine Warnung wird ausgegeben, wenn Autonomous Ransomware Protection eine neue Erweiterung erkennt und das Vorkommen in den letzten 24 Stunden mehr als 20 Mal wiederholt wurde (Standardverhalten).
- **Warnung**: Eine Warnung erfolgt aufgrund der folgenden Verhaltensweisen:
  - Die Erkennung einer neuen Erweiterung wurde bisher nicht festgestellt und dasselbe Verhalten wiederholt sich nicht oft genug, um es als Angriff zu deklarieren.
  - Es wird eine hohe Entropie beobachtet.
  - Die Aktivität beim Lesen, Schreiben, Umbenennen oder Löschen von Dateien hat sich im Vergleich zum Normalwert verdoppelt.

Für SAN-Umgebungen basieren Warnungen ausschließlich auf hoher Entropie.

Die Beweise basieren auf Informationen von Autonomous Ransomware Protection in ONTAP. Weitere Einzelheiten finden Sie unter "Übersicht über den autonomen Ransomware-Schutz" .

Eine Warnung kann einen der folgenden Status haben:

- **Neu**
- **Inaktiv**

Ein Alarmereignis kann folgende Zustände aufweisen:

- **Neu**: Alle Vorfälle werden bei ihrer erstmaligen Erkennung als „neu“ gekennzeichnet.
- **In Bearbeitung**: Sie können einen Vorfall als „in Bearbeitung“ markieren, während Sie ihn auswerten.
- **Abgelehnt**: Wenn Sie vermuten, dass es sich bei der Aktivität nicht um einen Ransomware-Angriff handelt, können Sie den Status auf „Abgelehnt“ ändern.

Sobald Sie einen Angriff abgewiesen haben, können Sie seinen Status nicht mehr rückgängig machen. Wenn Sie eine Arbeitslast abbrechen, werden alle automatisch als Reaktion auf den potenziellen Ransomware-Angriff erstellten Snapshot-Kopien endgültig gelöscht.

- **Abweisen**: Der Vorfall wird gerade abgewiesen.
- **Gelöst**: Der Vorfall wurde behoben.
- **Automatisch gelöst**: Bei Warnungen mit niedriger Priorität wird der Vorfall automatisch gelöst, wenn innerhalb von fünf Tagen keine Maßnahmen ergriffen wurden.

Wenn Sie auf der Seite „Einstellungen“ ein Sicherheits- und Ereignisverwaltungssystem (SIEM) in Ransomware Resilience konfiguriert haben, sendet Ransomware Resilience Warndetails an Ihr SIEM-System.

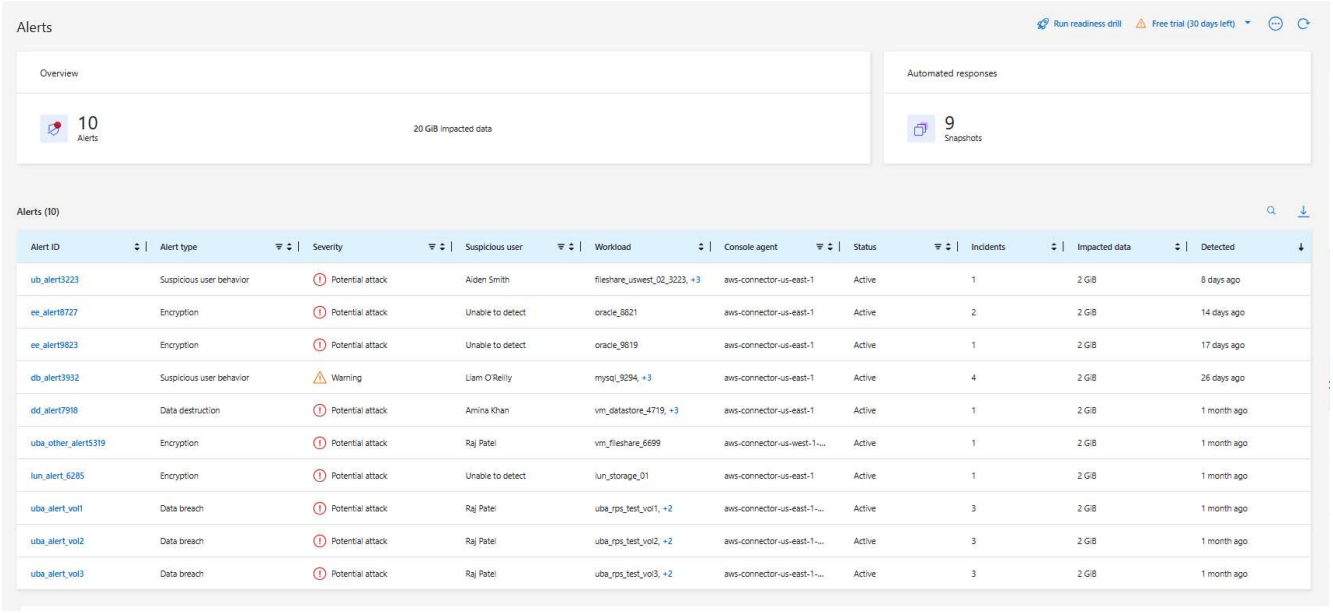
Warnungen anzeigen

Sie können über das Ransomware Resilience Dashboard oder über die Registerkarte **Warnungen** auf Warnungen zugreifen.

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

Schritte

1. Überprüfen Sie im Ransomware Resilience Dashboard den Bereich „Warnungen“.
2. Wählen Sie unter einem der Status **Alle anzeigen** aus.
3. Wählen Sie eine Warnung aus, um alle Vorfälle auf jedem Datenträger für jede Warnung zu überprüfen.
4. Um weitere Warnungen anzuzeigen, wählen Sie in der Brotkrümelnavigation oben links **Warnung** aus.
5. Überprüfen Sie die Warnungen auf der Seite „Warnungen“.



6. Fahren Sie mit einem der folgenden Schritte fort:
   - Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten .
   - Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden). .
   - bei denen es sich nicht um potenzielle Angriffe handelt .

Auf eine Warn-E-Mail antworten

Wenn Ransomware Resilience einen potenziellen Angriff erkennt, sendet es eine E-Mail-Benachrichtigung an die abonnierten Benutzer basierend auf deren Benachrichtigungseinstellungen, die in den NetApp Console-Einstellungen konfiguriert sind. Die E-Mail enthält Informationen zur Warnung, einschließlich des Schweregrads und der betroffenen Ressourcen.

Informationen zum Einrichten von E-Mail-Benachrichtigungen in der NetApp Console finden Sie unter "E-Mail-Benachrichtigungseinstellungen festlegen".

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

Schritte

1. Sehen Sie sich die E-Mail an.
2. Wählen Sie in der E-Mail **Warnung anzeigen** aus und melden Sie sich bei Ransomware Resilience an.

   Die Seite „Warnungen“ wird angezeigt.
3. Überprüfen Sie für jede Warnung alle Vorfälle auf jedem Datenträger.
4. Um weitere Warnungen anzuzeigen, klicken Sie in der Brotkrümelnavigation oben links auf **Warnung**.
5. Fahren Sie mit einem der folgenden Schritte fort:
   - Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten .
   - Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden). .
   - bei denen es sich nicht um potenzielle Angriffe handelt .

Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten

Auf der Registerkarte „Warnungen“ können Sie erkennen, ob böswillige Aktivitäten oder anomales Benutzerverhalten vorliegen.

Sie müssen einen Benutzeraktivitätsagenten konfiguriert und eine Datensicherungsstrategie mit Benutzerverhaltenserkennung aktiviert haben, um Warnungen auf Benutzerebene anzuzeigen. Die Spalte **Verdächtiger Benutzer** wird im Warnungs-Dashboard nur angezeigt, wenn die Benutzerverhaltenserkennung aktiviert ist. Um die Erkennung verdächtiger Benutzer zu aktivieren, siehe "Verdächtige Benutzeraktivität".

Anzeigen böswilliger Aktivitäten

Wenn Autonomous Ransomware Protection eine Warnung in Ransomware Resilience auslöst, können Sie die folgenden Details anzeigen:

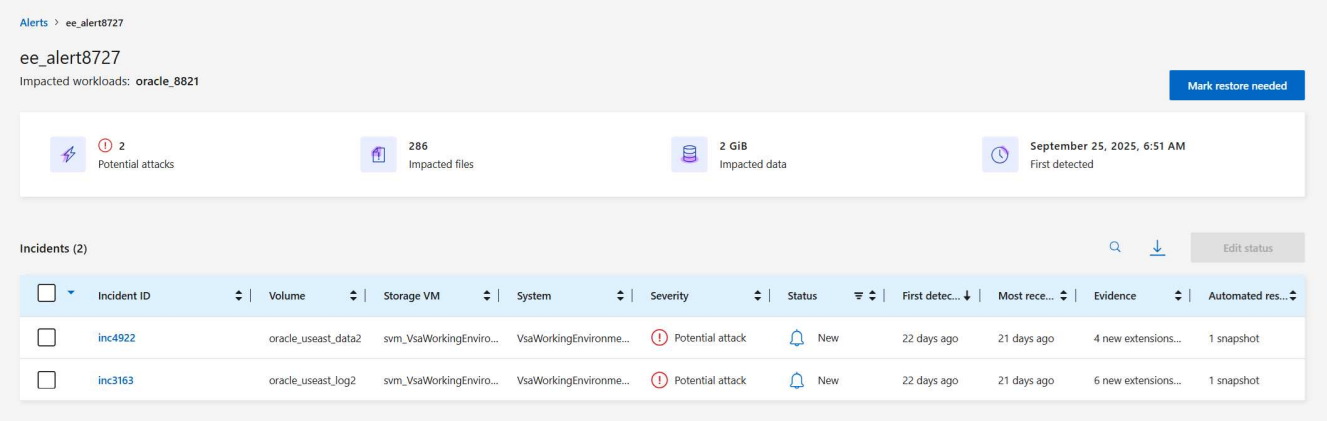
- Entropie eingehender Daten
- Erwartete Erstellungsrate neuer Dateien im Vergleich zur erkannten Rate
- Erwartete Löschrate von Dateien im Vergleich zur erkannten Rate
- Erwartete Umbenennungsrate von Dateien im Vergleich zur erkannten Rate
- Betroffene Dateien und Verzeichnisse

Diese Details sind für NAS-Workloads sichtbar. Für SAN-Umgebungen sind nur die Entropiedaten verfügbar.

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.

2. Wählen Sie eine Warnung aus.
3. Überprüfen Sie die Vorfälle in der Warnung.



4. Wählen Sie einen Vorfall aus, um die Details des Vorfalls zu überprüfen.

Anzeigen von anomalem Benutzerverhalten

Wenn Sie die Erkennung verdächtiger Benutzer zum Anzeigen anomalen Benutzerverhaltens konfiguriert haben, können Sie Daten auf Benutzerebene anzeigen und bestimmte Benutzer blockieren. Informationen zum Aktivieren der Einstellungen für verdächtige Benutzer finden Sie unter"Konfigurieren der Ransomware-Resilienzeinstellungen" .

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.
2. Wählen Sie eine Warnung aus.
3. Überprüfen Sie die Vorfälle in der Warnung.
   a. Um einen verdächtigen Benutzer in Ihrer Umgebung zu blockieren, wählen Sie **Block** neben dem Namen des Benutzers aus.
   b. Um Benachrichtigungen für einen Benutzer zu deaktivieren, der Gegenstand einer nachweislich falschen Benachrichtigung ist, wählen Sie die drei Punkte (… und anschließend **Diesen Benutzer von der Überwachung ausschließen**. Überprüfen Sie den Dialog und wählen Sie dann **Ausschließen** zur Bestätigung.

Um Benachrichtigungen für einen Benutzer wieder zu aktivieren, rufen Sie die Benachrichtigung auf. Wählen Sie die drei Punkte und dann **Diesen Benutzer in die Überwachung einbeziehen**. Sie können auch "Benutzer ausschließen" aus der Überwachung entfernen.

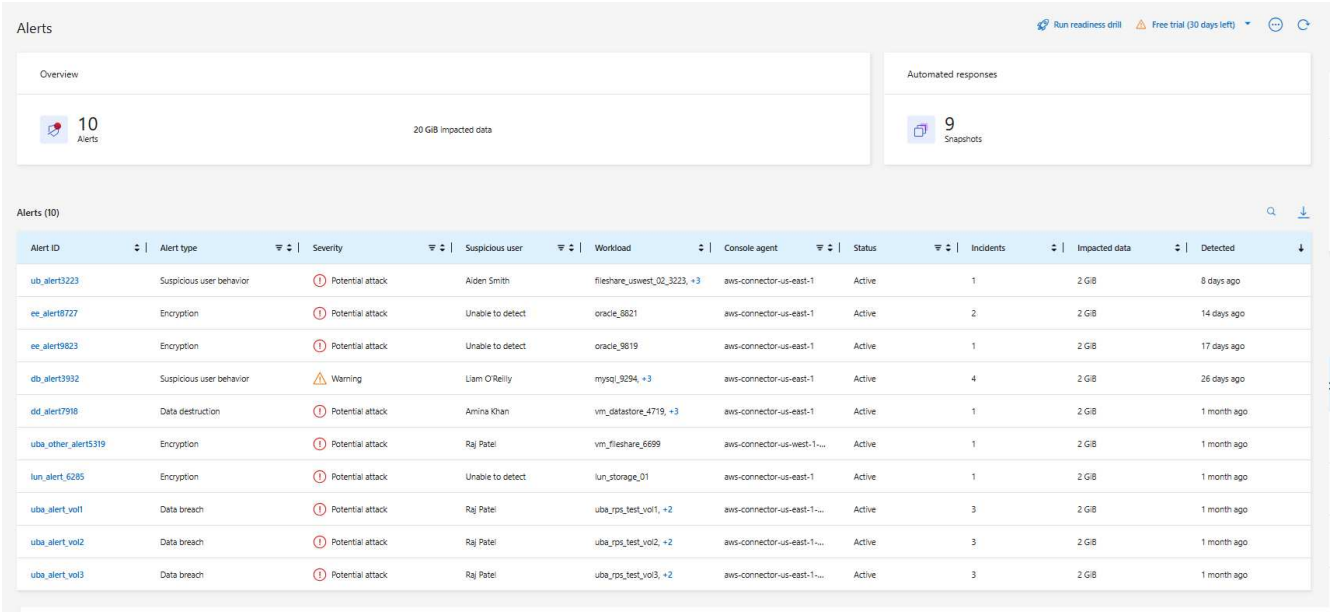
Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden).

Nachdem der Angriff gestoppt wurde, benachrichtigen Sie Ihren Storage-Administrator, dass die Daten bereit sind, damit dieser den Wiederherstellungsprozess einleiten kann.

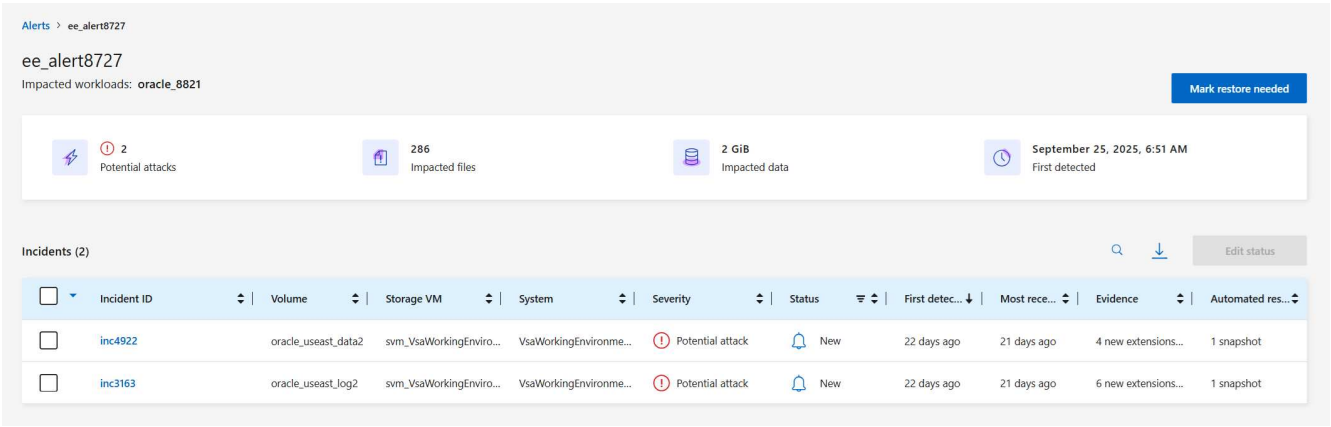
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.



2. Wählen Sie auf der Seite „Warnungen“ die Warnung aus.
3. Überprüfen Sie die Vorfälle in der Warnung.



4. Wenn Sie feststellen, dass die Vorfälle zur Wiederherstellung bereit sind, wählen Sie **Als Wiederherstellung erforderlich markieren**.
5. Bestätigen Sie die Aktion und wählen Sie **Als Wiederherstellung erforderlich markieren**.
6. Um die Workload-Wiederherstellung zu starten, wählen Sie in der Nachricht „Workload wiederherstellen“ oder wählen Sie die Registerkarte „Wiederherstellung“ aus.

Ergebnis

Nachdem die Warnung zur Wiederherstellung markiert wurde, wird sie von der Registerkarte „Warnungen“ zur Registerkarte „Wiederherstellung“ verschoben.

Vorfälle abweisen, bei denen es sich nicht um potenzielle Angriffe handelt

Nachdem Sie die Vorfälle überprüft haben, müssen Sie feststellen, ob es sich bei den Vorfällen um potenzielle Angriffe handelt. Wenn es sich nicht um tatsächliche Bedrohungen handelt, können sie als unbegründet abgetan werden.

Sie können Fehlalarme ignorieren oder sich für eine sofortige Wiederherstellung Ihrer Daten entscheiden. Wenn Sie die Warnung ignorieren, lernt Ransomware Resilience dieses Verhalten und ordnet es dem normalen Betrieb zu, sodass bei einem solchen Verhalten keine Warnung mehr ausgelöst wird.

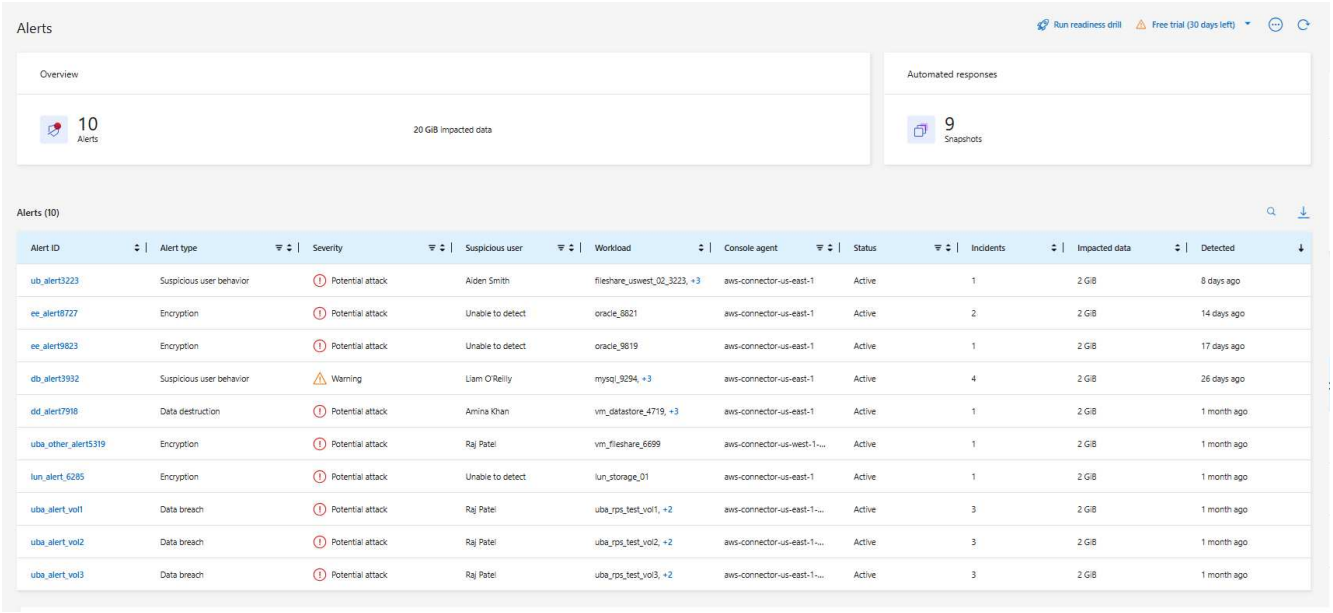
Wenn Sie eine Arbeitslast verwerfen, werden alle Snapshot-Kopien, die automatisch als Reaktion auf einen potenziellen Ransomware-Angriff erstellt wurden, dauerhaft gelöscht.

> Wenn Sie eine Warnung verwerfen, können Sie ihren Status nicht ändern oder diese Änderung rückgängig machen.

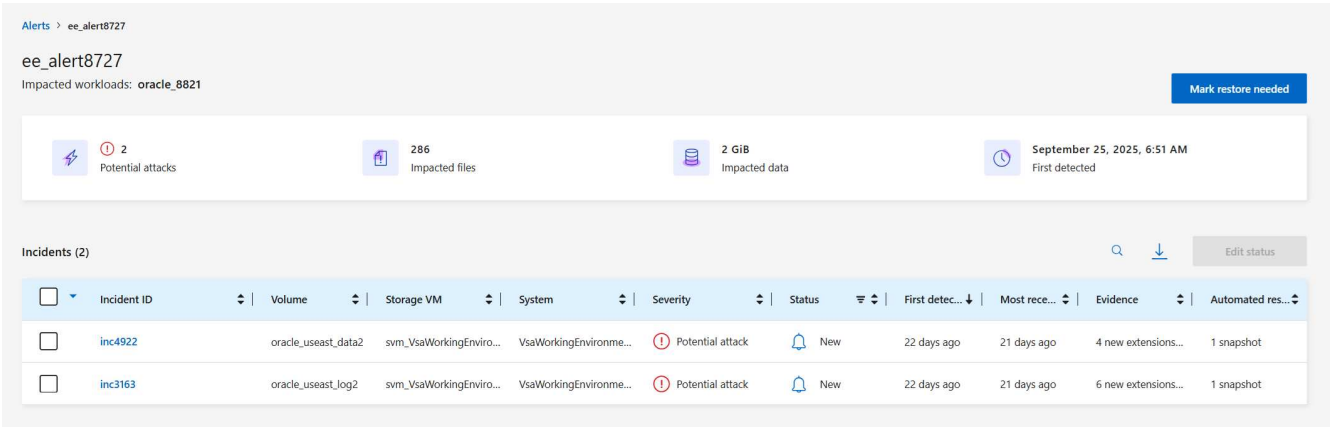
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.

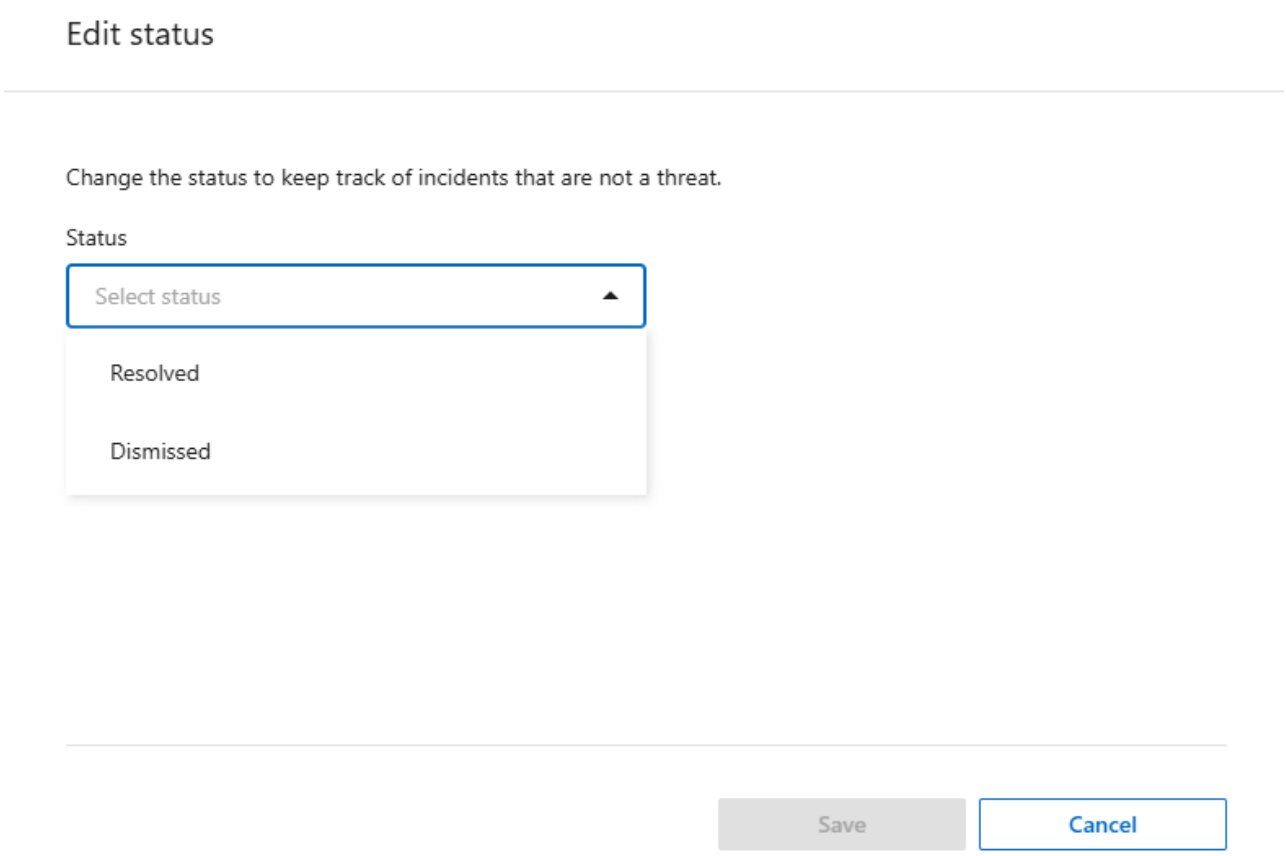


2. Wählen Sie auf der Seite „Warnungen“ die Warnung aus.



3. Wählen Sie einen oder mehrere Vorfälle aus. Alternativ können Sie alle Vorfälle auswählen, indem Sie das Feld „Vorfalls-ID“ oben links in der Tabelle anklicken.

4. Wenn Sie feststellen, dass der Vorfall keine Bedrohung darstellt, verwerfen Sie ihn als falsch-positives Ergebnis:
   - Wählen Sie den Vorfall aus.
   - Wählen Sie die Schaltfläche **Status bearbeiten** über der Tabelle.



5. Wählen Sie im Dialogfeld „Status bearbeiten“ den Status **Abgelehnt** aus.

   Es werden zusätzliche Informationen über die Arbeitslast und das Löschen der Snapshot-Kopien angezeigt.

6. Wählen Sie **Speichern**.

   Der Status des Vorfalls bzw. der Vorfälle ändert sich zu „Abgewiesen“.

Liste der betroffenen Dateien anzeigen

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie eine Liste der betroffenen Dateien anzeigen. Sie können auf die Seite „Warnungen“ zugreifen, um eine Liste der betroffenen Dateien herunterzuladen. Verwenden Sie dann die Wiederherstellungsseite, um die Liste hochzuladen und auszuwählen, welche Dateien wiederhergestellt werden sollen.

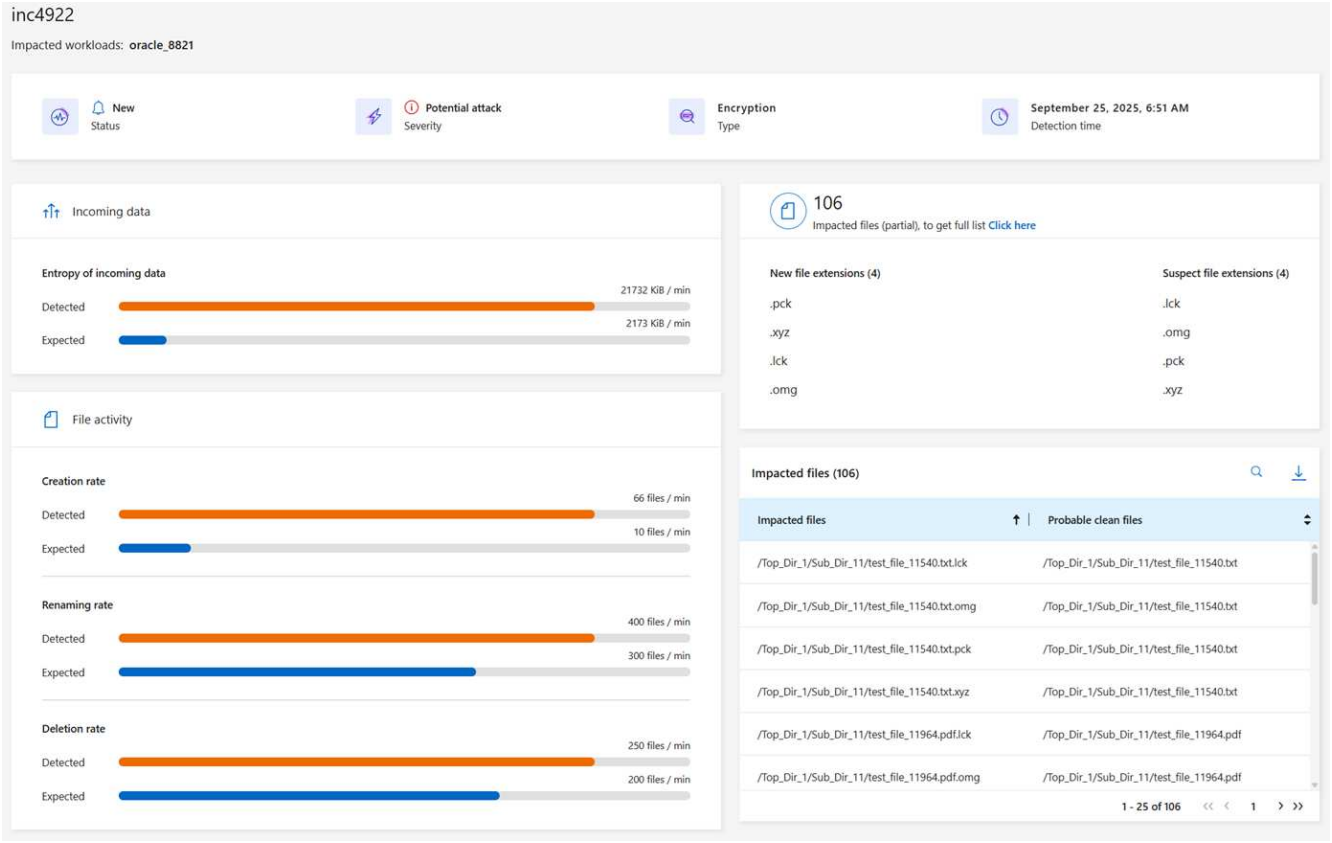
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

Verwenden Sie die Seite „Warnungen“, um die Liste der betroffenen Dateien abzurufen.

Wenn ein Volume mehrere Warnungen aufweist, müssen Sie möglicherweise für jede Warnung die CSV-Liste der betroffenen Dateien herunterladen.

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.
2. Sortieren Sie auf der Seite „Warnungen“ die Ergebnisse nach Arbeitslast, um die Warnungen für die Anwendungsarbeitslast anzuzeigen, die Sie wiederherstellen möchten.
3. Wählen Sie aus der Liste der Warnungen für diese Arbeitslast eine Warnung aus.
4. Wählen Sie für diese Warnung einen einzelnen Vorfall aus.



5. Wählen Sie für diesen Vorfall das Download-Symbol aus, um die Liste der betroffenen Dateien im CSV-Format herunterzuladen.

Wiederherstellung nach einem Ransomware-Angriff (nachdem die Vorfälle neutralisiert wurden) mit NetApp Ransomware Resilience

Nachdem Workloads als „Wiederherstellung erforderlich“ markiert wurden, empfiehlt NetApp Ransomware Resilience einen tatsächlichen Wiederherstellungspunkt (RPA) und orchestriert den Workflow für eine absturzsichere Wiederherstellung.

- Wenn die Anwendung oder VM von SnapCenter verwaltet wird, stellt Ransomware Resilience die Anwendung oder VM mithilfe des anwendungskonsistenten oder VM-konsistenten Prozesses in ihren

vorherigen Zustand und die letzte Transaktion zurück. Bei der anwendungs- oder VM-konsistenten Wiederherstellung werden alle Daten, die nicht in den Speicher gelangt sind (z. B. Daten im Cache oder in einem E/A-Vorgang), den Daten im Volume hinzugefügt.

- Wenn die Anwendung oder VM *nicht* von SnapCenter , sondern von NetApp Backup and Recovery oder Ransomware Resilience verwaltet wird, führt Ransomware Resilience eine absturzkonsistente Wiederherstellung durch, bei der alle Daten, die sich zum gleichen Zeitpunkt auf dem Volume befanden, wiederhergestellt werden, beispielsweise wenn das System abgestürzt ist.

  Sie können die Arbeitslast wiederherstellen, indem Sie alle Volumes, bestimmte Volumes oder bestimmte Dateien auswählen.

Die Wiederherstellung der Arbeitslast kann sich auf laufende Arbeitslasten auswirken. Sie sollten die Wiederherstellungsprozesse mit den entsprechenden Beteiligten koordinieren.

Ein Workload kann einen der folgenden Wiederherstellungsstatus haben:

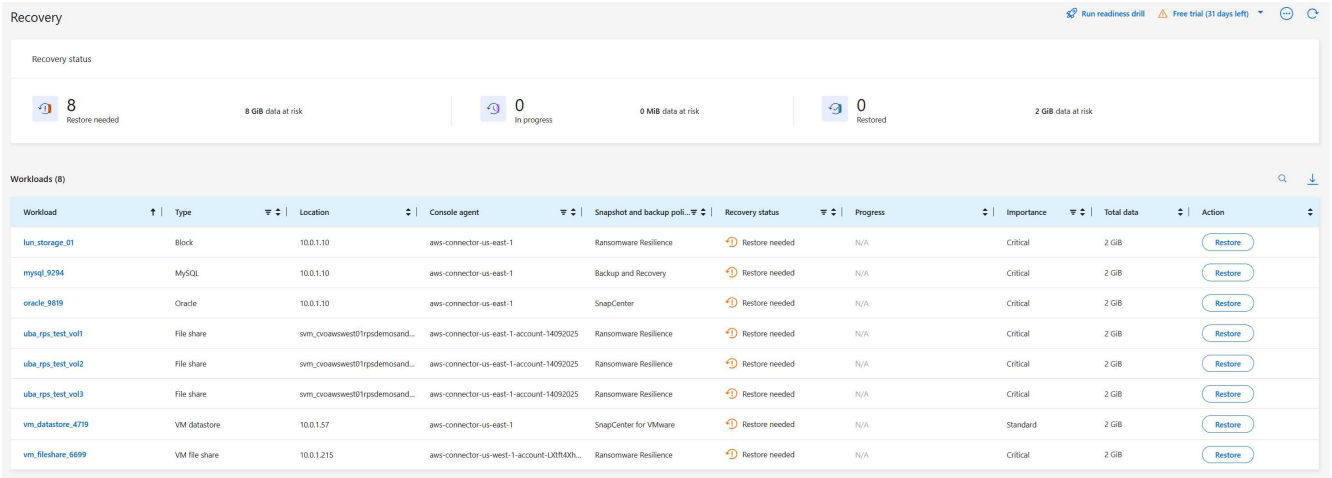
- **Wiederherstellung erforderlich**: Die Arbeitslast muss wiederhergestellt werden.
- **In Bearbeitung**: Der Wiederherstellungsvorgang ist derzeit im Gange.
- **Wiederhergestellt**: Die Arbeitslast wurde wiederhergestellt.
- **Fehlgeschlagen**: Der Workload-Wiederherstellungsprozess konnte nicht abgeschlossen werden.

Anzeigen von Workloads, die zur Wiederherstellung bereit sind

Überprüfen Sie die Workloads, die sich im Wiederherstellungsstatus „Wiederherstellung erforderlich“ befinden.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Überprüfen Sie im Dashboard die Gesamtsummen „Wiederherstellung erforderlich“ im Bereich „Warnungen“ und wählen Sie „Alle anzeigen“ aus.
   - Wählen Sie im Menü **Wiederherstellung** aus.
2. Überprüfen Sie die Arbeitslastinformationen auf der Seite **Wiederherstellung**.



Wiederherstellen einer von SnapCenter verwalteten Arbeitslast

Mithilfe von Ransomware Resilience kann der Speicheradministrator bestimmen, wie Workloads am besten vom empfohlenen oder vom bevorzugten Wiederherstellungspunkt wiederhergestellt werden.

Der Anwendungsstatus ändert sich, falls dies für die Wiederherstellung erforderlich ist. Die Anwendung wird aus Steuerdateien in ihren vorherigen Zustand zurückversetzt, sofern diese in der Sicherung enthalten sind. Nach Abschluss der Wiederherstellung wird die Anwendung im LESE-/SCHREIBMODUS geöffnet.

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" .

Schritte

1. Wählen Sie unter „Ransomware-Resilienz“ die Option „Wiederherstellung“ aus.
2. Überprüfen Sie die Arbeitslastinformationen auf der Seite **Wiederherstellung**.
3. Wählen Sie eine Arbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.
4. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
5. **Wiederherstellungsbereich**: Anwendungskonsistent (oder für SnapCenter für VMs ist der Wiederherstellungsbereich „Nach VM“)
6. **Quelle**: Wählen Sie den Abwärtspfeil neben „Quelle“, um Details anzuzeigen. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

   Ransomware Resilience identifiziert den besten Wiederherstellungspunkt als die letzte Sicherung unmittelbar vor dem Vorfall und zeigt die Anzeige „Empfohlen“ an.

7. **Ziel**: Wählen Sie den Abwärtspfeil neben „Ziel“, um Details anzuzeigen.
   a. Wählen Sie den ursprünglichen oder alternativen Speicherort aus.
   b. Wählen Sie das System aus.
   c. Wählen Sie die Speicher-VM aus.
8. Wenn am ursprünglichen Ziel nicht genügend Speicherplatz zum Wiederherstellen der Arbeitslast vorhanden ist, wird die Zeile „Temporärer Speicher“ angezeigt. Sie können den temporären Speicher auswählen, um die Workload-Daten wiederherzustellen. Die wiederhergestellten Daten werden vom temporären Speicher an den ursprünglichen Speicherort kopiert. Klicken Sie in der Zeile „Temporärer Speicher“ auf den **Abwärtspfeil** und legen Sie den Zielcluster, die Speicher-VM und die lokale Ebene fest.
9. Wählen Sie **Speichern**.
10. Wählen Sie **Weiter**.
11. Überprüfen Sie Ihre Auswahl.
12. Wählen Sie **Wiederherstellen**.
13. Wählen Sie im oberen Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Wiederherstellungsseite zu überprüfen, auf der der Status des Vorgangs durch die Zustände wechselt.

Wiederherstellen einer Arbeitslast, die nicht von SnapCenter verwaltet wird

Mithilfe von Ransomware Resilience kann der Speicheradministrator bestimmen, wie Workloads am besten vom empfohlenen oder vom bevorzugten Wiederherstellungspunkt wiederhergestellt werden.

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" .

Der Sicherheitsspeicheradministrator kann Daten auf verschiedenen Ebenen wiederherstellen:

- Wiederherstellung aller Volumes
- Stellen Sie eine Anwendung auf Volume- oder Datei- und Ordnerebene wieder her.
- Stellen Sie eine Dateifreigabe auf Volume-, Verzeichnis- oder Datei-/Ordnerebene wieder her.
- Wiederherstellung aus einem Datenspeicher auf VM-Ebene.

Der Prozess unterscheidet sich je nach Arbeitslasttyp.

Schritte

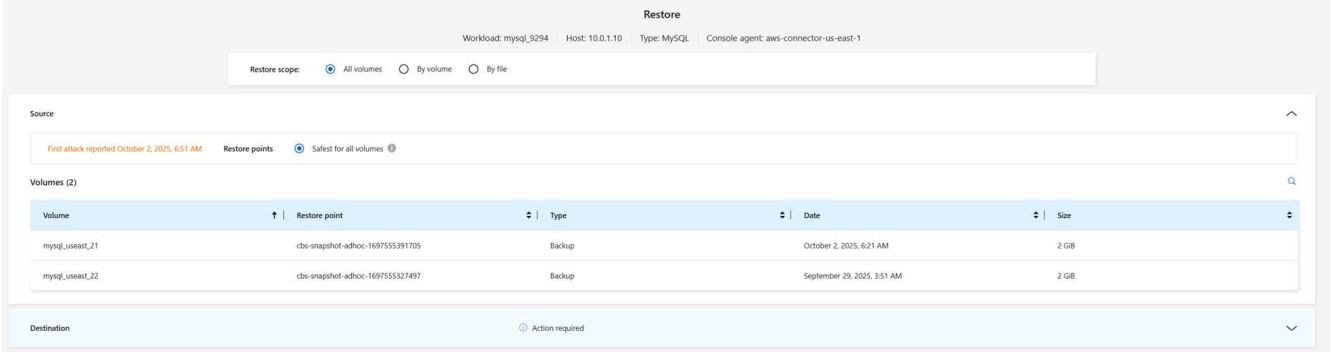
1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
2. Überprüfen Sie die Arbeitslastinformationen auf der Seite **Wiederherstellung**.
3. Wählen Sie eine Arbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.
4. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
5. **Wiederherstellungsumfang**: Wählen Sie den Wiederherstellungstyp aus, den Sie durchführen möchten:
    - Alle Bände
    - Nach Volumen
    - Nach Datei: Sie können einen Ordner oder einzelne Dateien zur Wiederherstellung angeben.

    Bei SAN-Workloads können Sie nur nach Workload wiederherstellen.

    Sie können bis zu 100 Dateien oder einen einzelnen Ordner auswählen.
6. Fahren Sie mit einem der folgenden Verfahren fort, je nachdem, ob Sie Anwendung, Volume oder Datei ausgewählt haben.

Alle Volumes wiederherstellen

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
2. Wählen Sie eine Arbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.
3. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
4. Wählen Sie auf der Seite „Wiederherstellen“ im Wiederherstellungsbereich **Alle Volumes** aus.



5. **Quelle**: Wählen Sie den Abwärtspfeil neben „Quelle“, um Details anzuzeigen.
   a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

> Ransomware Resilience identifiziert den besten Wiederherstellungspunkt als die letzte Sicherung unmittelbar vor dem Vorfall und zeigt die Meldung „Am sichersten für alle Volumes“ an. Dies bedeutet, dass alle Volumes auf eine Kopie wiederhergestellt werden, die vor dem ersten erkannten Angriff auf das erste Volume erstellt wurde.

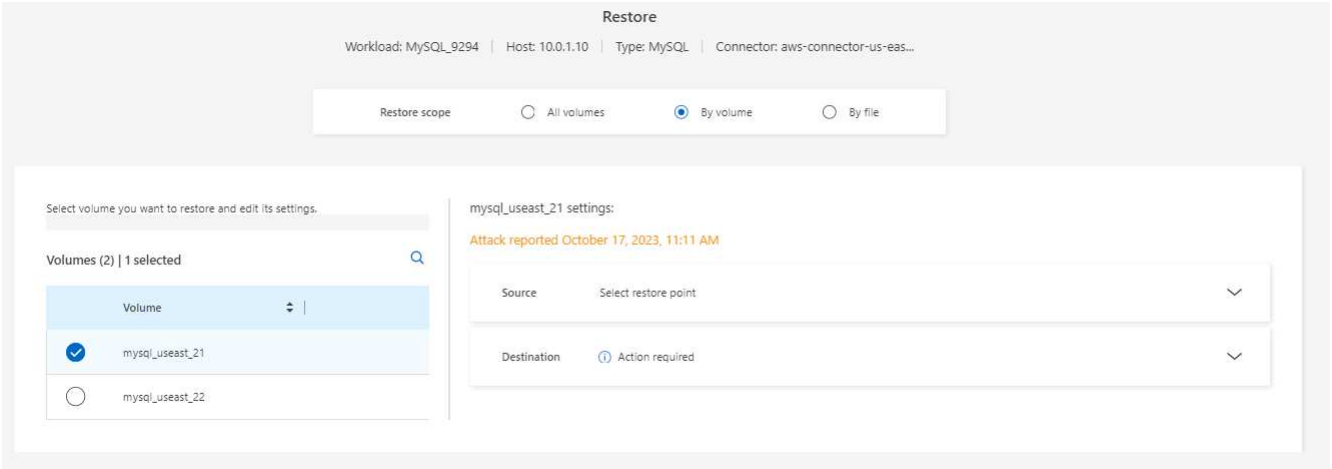
6. **Ziel**: Wählen Sie den Abwärtspfeil neben „Ziel“, um Details anzuzeigen.
   a. Wählen Sie das System aus.
   b. Wählen Sie die Speicher-VM aus.
   c. Wählen Sie das Aggregat aus.
   d. Ändern Sie das Volume-Präfix, das allen neuen Volumes vorangestellt wird.

> Der neue Datenträgername wird als Präfix + ursprünglicher Datenträgername + Sicherungsname + Sicherungsdatum angezeigt.

7. Wählen Sie **Speichern**.
8. Wählen Sie **Weiter**.
9. Überprüfen Sie Ihre Auswahl.
10. Wählen Sie **Wiederherstellen**.
11. Wählen Sie im oberen Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Wiederherstellungsseite zu überprüfen, auf der der Status des Vorgangs durch die Zustände wechselt.

Wiederherstellen einer Anwendungs-Workload auf Volume-Ebene

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
2. Wählen Sie eine Anwendungsarbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.
3. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
4. Wählen Sie auf der Seite „Wiederherstellen“ im Wiederherstellungsbereich die Option **Nach Volume** aus.



5. Wählen Sie in der Volumeliste das Volume aus, das Sie wiederherstellen möchten.

6. **Quelle**: Wählen Sie den Abwärtspfeil neben „Quelle“, um Details anzuzeigen.
   a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

> Ransomware Resilience identifiziert den besten Wiederherstellungspunkt als die letzte Sicherung unmittelbar vor dem Vorfall und zeigt die Meldung „Empfohlen“ an.

7. **Ziel**: Wählen Sie den Abwärtspfeil neben „Ziel“, um Details anzuzeigen.
   a. Wählen Sie das System aus.
   b. Wählen Sie die Speicher-VM aus.
   c. Wählen Sie das Aggregat aus.
   d. Überprüfen Sie den neuen Datenträgernamen.

> Der neue Datenträgername wird als ursprünglicher Datenträgername + Sicherungsname + Sicherungsdatum angezeigt.

8. Wählen Sie **Speichern**.
9. Wählen Sie **Weiter**.
10. Überprüfen Sie Ihre Auswahl.
11. Wählen Sie **Wiederherstellen**.
12. Wählen Sie im oberen Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Wiederherstellungsseite zu überprüfen, auf der der Status des Vorgangs durch die Zustände wechselt.

Wiederherstellen einer Anwendungs-Workload auf Dateiebene

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie eine Liste der betroffenen Dateien anzeigen. Sie können auf die Seite „Warnungen“ zugreifen, um eine Liste der betroffenen Dateien herunterzuladen. Verwenden Sie dann die Wiederherstellungsseite, um die Liste hochzuladen und auszuwählen, welche Dateien wiederhergestellt werden sollen.

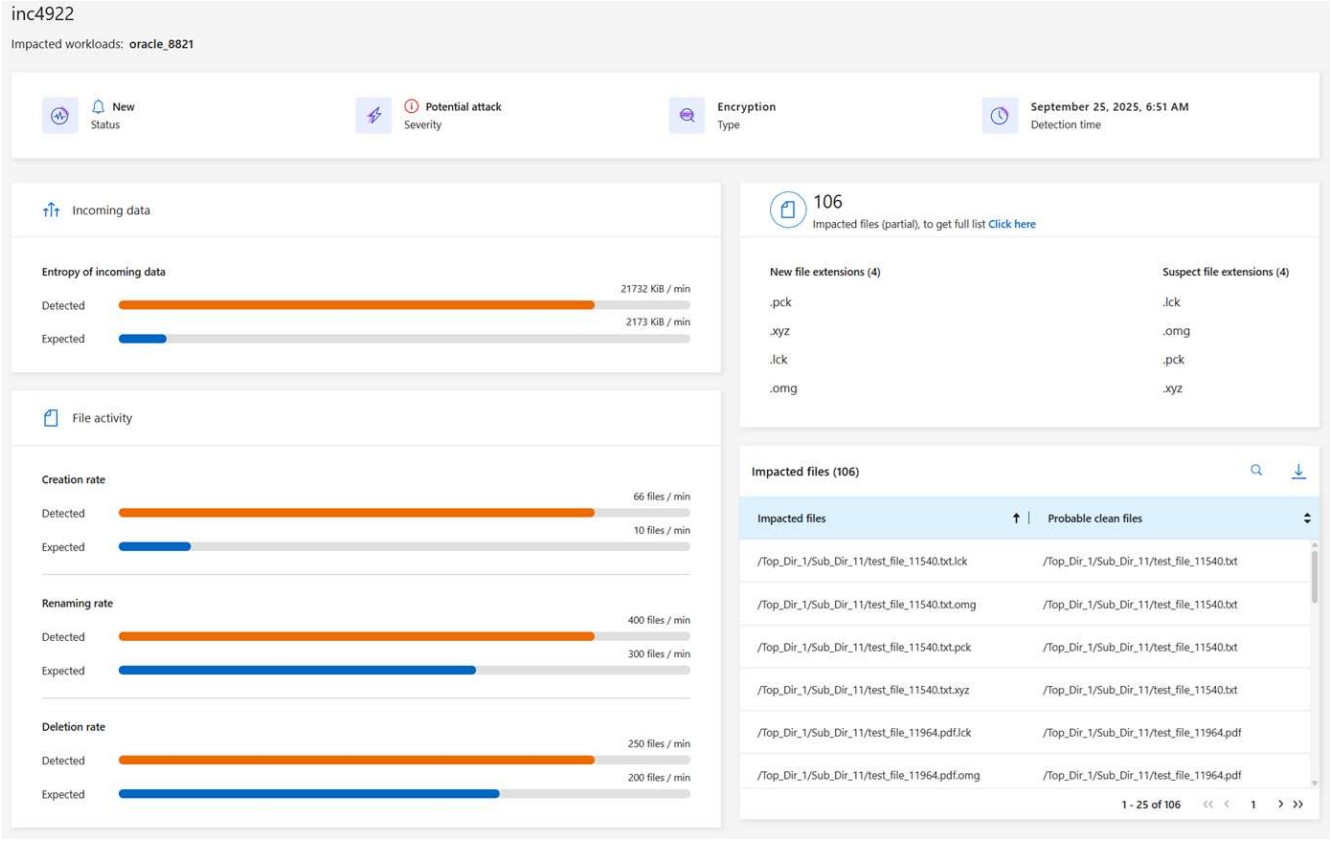
Sie können eine Anwendungs-Workload auf Dateiebene auf demselben oder einem anderen System wiederherstellen.

Schritte zum Abrufen der Liste der betroffenen Dateien

Verwenden Sie die Seite „Warnungen“, um die Liste der betroffenen Dateien abzurufen.

> Wenn ein Volume mehrere Warnungen aufweist, müssen Sie für jede Warnung die CSV-Liste der betroffenen Dateien herunterladen.

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.
2. Sortieren Sie auf der Seite „Warnungen“ die Ergebnisse nach Arbeitslast, um die Warnungen für die Anwendungsarbeitslast anzuzeigen, die Sie wiederherstellen möchten.
3. Wählen Sie aus der Liste der Warnungen für diese Arbeitslast eine Warnung aus.
4. Wählen Sie für diese Warnung einen einzelnen Vorfall aus.



5. Um die vollständige Liste der Dateien anzuzeigen, wählen Sie oben im Bereich „Betroffene Dateien“ die Option „Hier klicken“ aus.
6. Wählen Sie für diesen Vorfall das Download-Symbol aus und laden Sie die Liste der betroffenen Dateien im CSV-Format herunter.

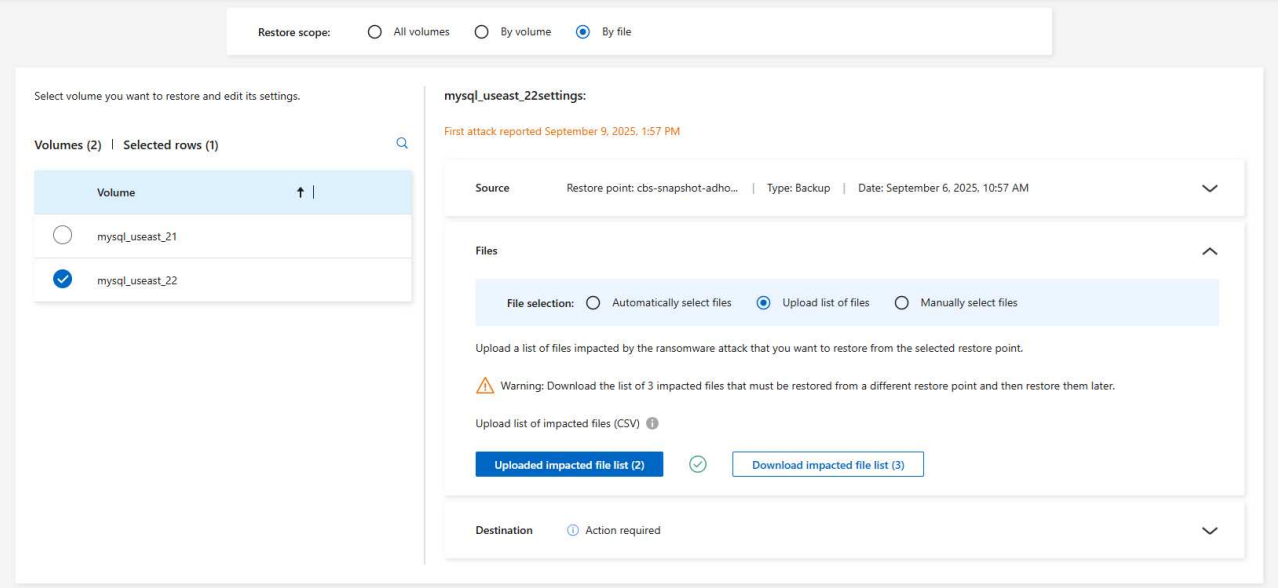
Schritte zum Wiederherstellen dieser Dateien

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
2. Wählen Sie eine Anwendungsarbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.
3. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
4. Wählen Sie auf der Seite „Wiederherstellen“ im Wiederherstellungsbereich die Option „Nach Datei“ aus.
5. Wählen Sie in der Volumeliste das Volume aus, das die Dateien enthält, die Sie wiederherstellen möchten.
6. **Wiederherstellungspunkt**: Wählen Sie den Abwärtspfeil neben **Wiederherstellungspunkt**, um Details anzuzeigen. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

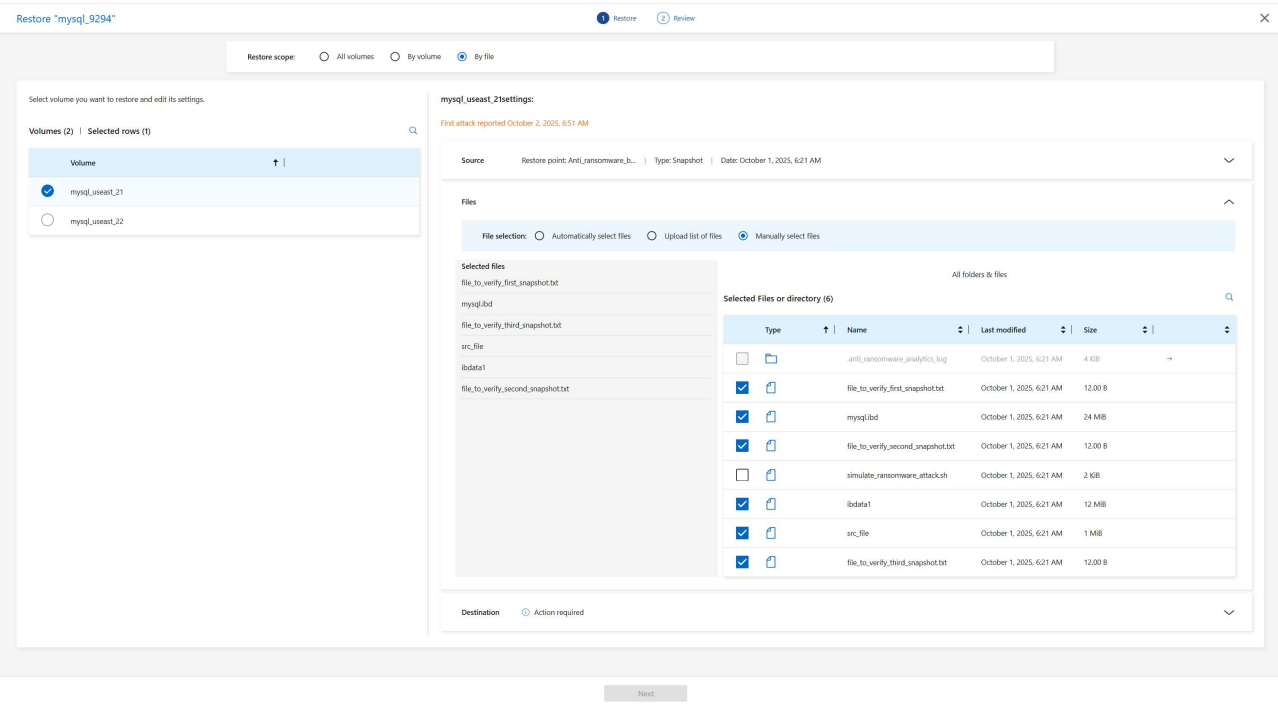
> In der Spalte „Grund“ im Bereich „Wiederherstellungspunkte“ wird der Grund für den Snapshot oder die Sicherung entweder als „Geplant“ oder „Automatisierte Reaktion auf Ransomware-Vorfall“ angezeigt.

7. **Dateien**:
   - **Dateien automatisch auswählen**: Lassen Sie Ransomware Resilience die wiederherzustellenden Dateien auswählen.
   - **Dateiliste hochladen**: Laden Sie eine CSV-Datei hoch, die die Liste der betroffenen Dateien enthält, die Sie von der Warnseite erhalten haben oder über die Sie verfügen. Sie können bis zu 10.000

Dateien gleichzeitig wiederherstellen.



- **Dateien manuell auswählen**: Wählen Sie bis zu 10.000 Dateien oder einen einzelnen Ordner zur Wiederherstellung aus.



Wenn Dateien mit dem ausgewählten Wiederherstellungspunkt nicht wiederhergestellt werden können, wird eine Meldung mit der Anzahl der nicht wiederhergestellten Dateien angezeigt. Sie können die Liste dieser Dateien herunterladen, indem Sie „Liste der betroffenen Dateien herunterladen“ auswählen.

8. **Ziel**: Wählen Sie den Abwärtspfeil neben „Ziel“, um Details anzuzeigen.
   a. Wählen Sie, wo die Daten wiederhergestellt werden sollen: am ursprünglichen Quellspeicherort oder an einem alternativen Speicherort, den Sie angeben können.

Während die ursprünglichen Dateien oder Verzeichnisse durch die wiederhergestellten Daten überschrieben werden, bleiben die ursprünglichen Datei- und Ordnernamen gleich, sofern Sie keine neuen Namen angeben.

b. Wählen Sie das System aus.

c. Wählen Sie die Speicher-VM aus.

d. Geben Sie optional den Pfad ein.

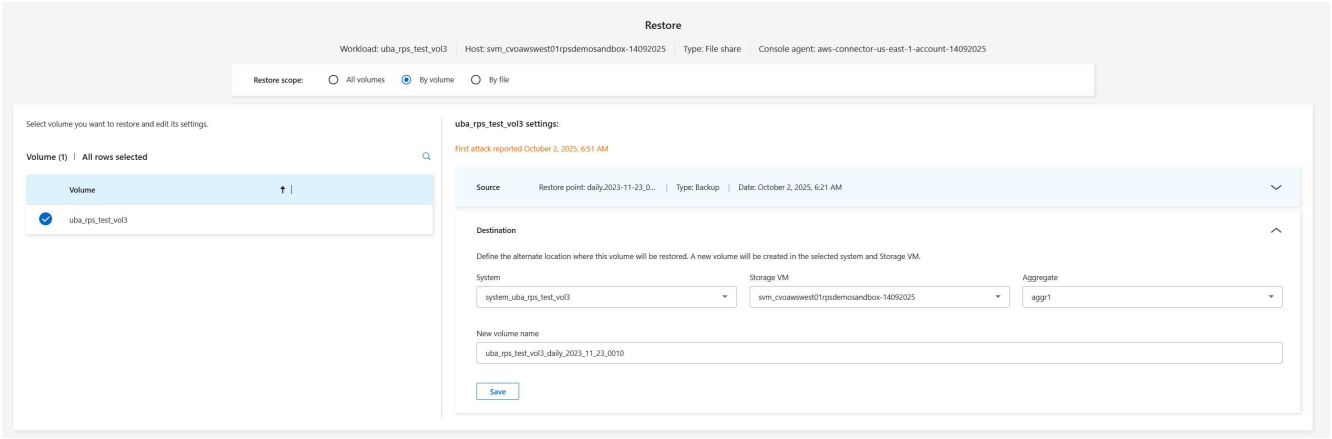
Wenn Sie keinen Pfad für die Wiederherstellung angeben, werden die Dateien auf einem neuen Volume im obersten Verzeichnis wiederhergestellt.

e. Wählen Sie aus, ob die Namen der wiederhergestellten Dateien oder Verzeichnisse dieselben oder andere Namen wie am aktuellen Speicherort haben sollen.

9. Wählen Sie **Weiter**.
10. Überprüfen Sie Ihre Auswahl.
11. Wählen Sie **Wiederherstellen**.
12. Wählen Sie im oberen Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Wiederherstellungsseite zu überprüfen, auf der der Status des Vorgangs durch die Zustände wechselt.

Wiederherstellen einer Dateifreigabe oder eines Datenspeichers

1. Nachdem Sie eine Dateifreigabe oder einen Datenspeicher zum Wiederherstellen ausgewählt haben, wählen Sie auf der Seite „Wiederherstellen“ im Wiederherstellungsbereich die Option **Nach Volume** aus.



2. Wählen Sie in der Volumeliste das Volume aus, das Sie wiederherstellen möchten.
3. **Quelle**: Wählen Sie den Abwärtspfeil neben „Quelle“, um Details anzuzeigen.

a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

Ransomware Resilience identifiziert den besten Wiederherstellungspunkt als die letzte Sicherung unmittelbar vor dem Vorfall und zeigt die Meldung „Empfohlen“ an.

4. **Ziel**: Wählen Sie den Abwärtspfeil neben „Ziel“, um Details anzuzeigen.

a. Wählen Sie, wo die Daten wiederhergestellt werden sollen: am ursprünglichen Quellspeicherort oder an einem alternativen Speicherort, den Sie angeben können.

Während die ursprünglichen Dateien oder Verzeichnisse durch die wiederhergestellten Daten überschrieben werden, bleiben die ursprünglichen Datei- und Ordnernamen gleich, sofern Sie keine neuen Namen angeben.

b. Wählen Sie das System aus.

c. Wählen Sie die Speicher-VM aus.

d. Geben Sie optional den Pfad ein.

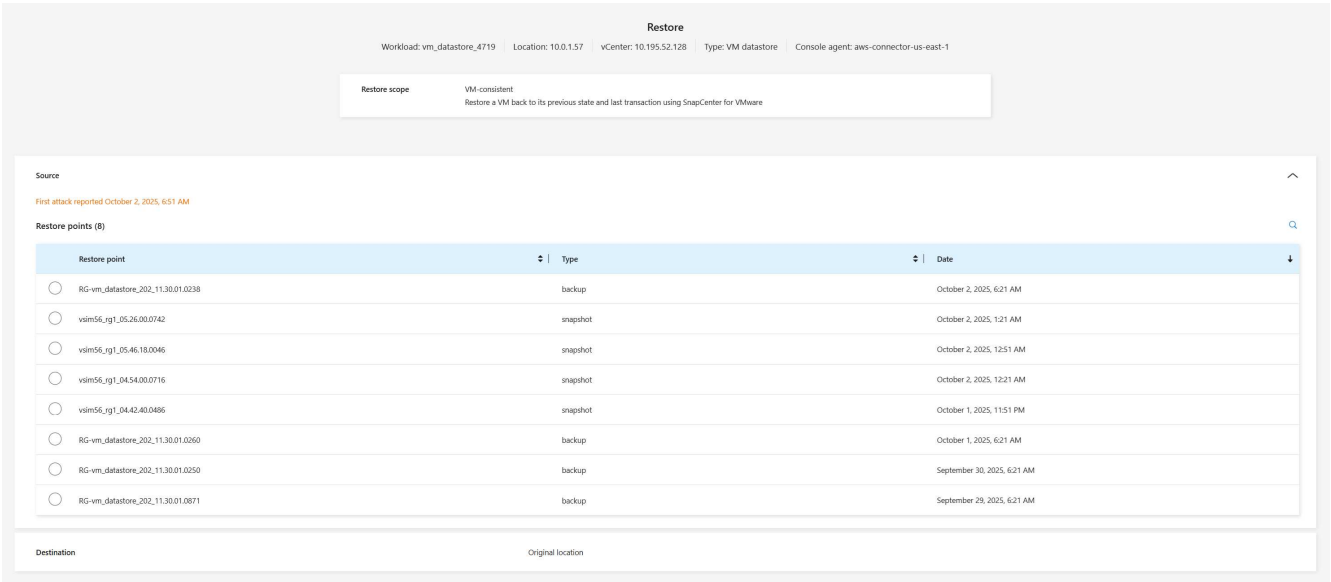
Wenn Sie keinen Pfad für die Wiederherstellung angeben, werden die Dateien auf einem neuen Volume im obersten Verzeichnis wiederhergestellt.

5. Wählen Sie **Speichern**.
6. Überprüfen Sie Ihre Auswahl.
7. Wählen Sie **Wiederherstellen**.
8. Wählen Sie im Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Wiederherstellungsseite zu überprüfen, auf der der Status des Vorgangs durch die Zustände wechselt.

Wiederherstellen einer VM-Dateifreigabe auf VM-Ebene

Nachdem Sie eine VM zur Wiederherstellung ausgewählt haben, fahren Sie auf der Seite „Wiederherstellung“ mit diesen Schritten fort.

1. **Quelle**: Wählen Sie den Abwärtspfeil neben „Quelle“, um Details anzuzeigen.



2. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.
3. **Ziel**: Zum ursprünglichen Standort.
4. Wählen Sie **Weiter**.
5. Überprüfen Sie Ihre Auswahl.
6. Wählen Sie **Wiederherstellen**.
7. Wählen Sie im Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Wiederherstellungsseite zu

überprüfen, auf der der Status des Vorgangs durch die Zustände wechselt.

Berichte in NetApp Ransomware Resilience herunterladen

Sie können Schutzdaten exportieren und die CSV- oder JSON-Dateien herunterladen, die Details zu Angriffsbereitschaftsübungen, Schutz, Warnungen und Wiederherstellung enthalten.

Bevor Sie die Dateien herunterladen, aktualisieren Sie das Dashboard, um die aktuellsten Daten in Ihren Berichten zu erfassen.

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

Welche Daten können Sie herunterladen? Sie können Dateien von jeder der Hauptmenüoptionen herunterladen:

- **Zusammenfassung**: Enthält Listen unterstützter und nicht unterstützter Workloads, empfohlene Maßnahmen zur Verbesserung Ihrer Cyber-Resilienz sowie Informationen, die im Ransomware-Resilienz-Dashboard erfasst werden.
- **Schutz**: Beinhaltet den Status und die Details aller Workloads, einschließlich der Gesamtzahl der geschützten und gefährdeten Workloads.
- **Warnungen**: Enthält den Status und die Details aller Warnungen, einschließlich der Gesamtzahl der Warnungen und automatisierten Snapshots.
- **Wiederherstellung**: Enthält den Status und die Details aller Workloads, die wiederhergestellt werden müssen, einschließlich der Gesamtzahl der Workloads mit den Markierungen „Wiederherstellung erforderlich“, „In Bearbeitung“, „Wiederherstellung fehlgeschlagen“ und „Erfolgreich wiederhergestellt“.
- **Berichte**: Sie können Daten von jeder Seite exportieren und die Dateien herunterladen.

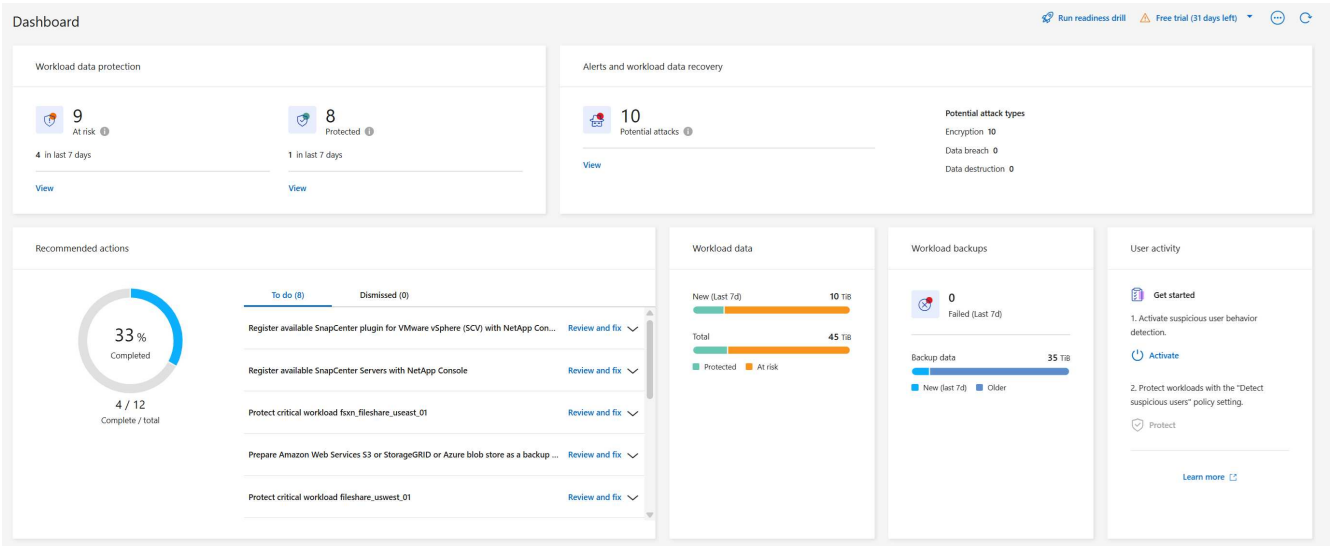
  Sie können Bereitschaftsübungsberichte nur von der Seite **Berichte** herunterladen.

Wenn Sie CSV- oder JSON-Dateien von der Seite „Schutz“, „Warnungen“ oder „Wiederherstellung“ herunterladen, werden nur die Daten auf dieser Seite angezeigt.

Die CSV- oder JSON-Dateien enthalten Daten für alle Workloads auf allen Konsolensystemen.

Schritte

1. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz** aus.



2. Wählen Sie im Dashboard oder auf einer anderen Seite die Option *Aktualisieren* Klicken Sie oben rechts auf die Option, um die Daten zu aktualisieren, die in den Berichten angezeigt werden.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie auf der Seite *Download* Option.
   - Wählen Sie im NetApp Ransomware Resilience Menü **Berichte** aus.
4. Wenn Sie die Option **Berichte** ausgewählt haben, wählen Sie einen der vorkonfigurierten Dateinamen und wählen Sie **Herunterladen**.