Schützen und erkennen

NetApp Ransomware Resilience

NetApp
April 13, 2026

Inhalt

Schützen und erkennen

Schutzstatus in NetApp Ransomware Resilience überprüfen

NetApp Ransomware Resilience's Schutz-Dashboard bietet einen Überblick über den Schutzstatus und die Schutzbereitschaft Ihrer Workloads. Verwenden Sie das Schutz-Dashboard, um Einblicke darin zu erhalten, was geschützt ist, was Schutz benötigt und welchen Umfang der Schutz hat.

Sobald Sie den Umfang Ihres aktuellen Schutzes verstanden haben, "Sie können Ransomware-Schutzstrategien für Ihre Workloads erstellen und anwenden".

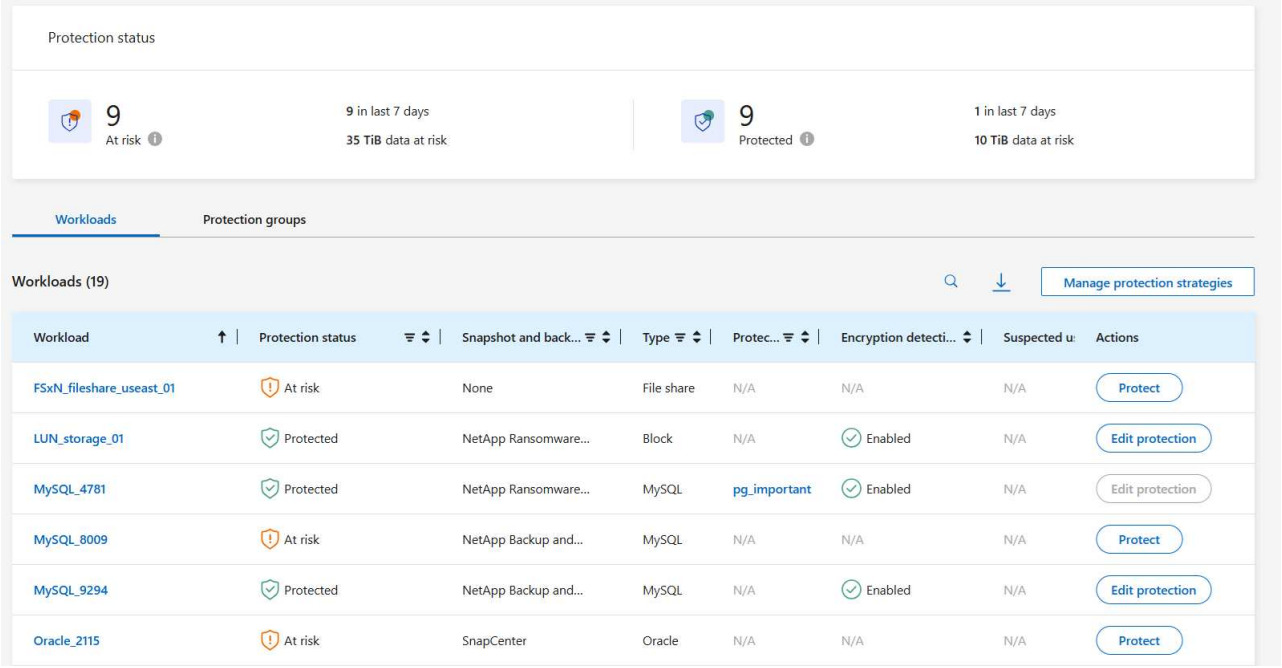
Schutz auf einer Arbeitslast anzeigen

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 „Data Protection“ auf dem Dashboard **View all** aus.
   - Wählen Sie im Menü **Schutz** aus.



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

Siehe "Fügen Sie eine Ransomware-Schutzstrategie hinzu" , um mehr über die Verwendung von Ransomware Resilience bei einer bestehenden Datensicherungsstrategie mit Backup and Recovery zu erfahren.

Das Schutz-Dashboard verstehen

Das Schutz-Dashboard in Ransomware Resilience zeigt detaillierte Informationen zu Workloads (zum Beispiel Workload-Name und -Typ, Console-Agent, System und Storage-VM) sowie Einblicke in den Schutzstatus. Verwenden Sie das Schutz-Dashboard, um die Ransomware-Vorsorge für Workloads zu überprüfen und zu verwalten. Die folgenden Spalten sind besonders hilfreich, um Ihre Schutzsituation zu verstehen:

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:

+ Ransomware Resilience bietet Einblicke in den Umfang der von Ihnen auf Ihren Workloads konfigurierten Ransomware-Erkennungsrichtlinien. Überprüfen Sie den Erkennungsbereich anhand der folgenden Felder.

- **Status der Verschlüsselungserkennung**
- **Status der Erkennung mutmaßlichen Benutzerverhaltens**
- **Verdächtige Dateierweiterungen blockieren**

Snapshot-, Replikations- und Sicherungsrichtlinien: Diese Spalte zeigt das Produkt oder den Dienst an, der die Richtlinie verwaltet. Wenn keine Richtlinie vorhanden ist, wird N/A angezeigt.

Bedeutung

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.

Privacy exposure: Wählen Sie diese Option aus, um "Scannen nach personenbezogenen Daten mit NetApp Data Classification".

Replikationsziel: Wenn Sie die Snapshot-Replikation konfiguriert haben, werden die Namen der Ziel-Speicher-VMs und -Systeme aufgelistet. Wenn keine Replikation vorhanden ist, wird in diesem Feld "N/A"

angezeigt.

Sicherungsziel: Wenn Sie eine Ransomware-Schutzstrategie mit Backups konfiguriert haben, wird hier der Name des Sicherungszielsystems angezeigt.

Nächste Schritte

- "Schützen Sie Workloads mit Strategien zum Schutz vor Ransomware"
- "Schutzgruppen verwalten"
- "Scannen nach personenbezogenen Daten"

Fügen Sie ein Backup-Ziel in NetApp Ransomware Resilience hinzu

Wenn NetApp Ransomware Resilience Workloads erkennt, werden, falls Backups konfiguriert sind, die Backup-Ziele erkannt. Wenn Sie planen, Backups als Teil Ihrer "Ransomware-Schutzstrategie" zu verwenden, aber noch keine Backup-Ziele für den Workload konfiguriert haben, müssen Sie ein Backup-Ziel in NetApp Ransomware Resilience hinzufügen, um die Cyber-Resilienz zu verbessern.

Sie können eines der folgenden Sicherungsziele auswählen:

- NetApp StorageGRID
- Amazon Web Services (AWS)
- Google Cloud Platform
- Microsoft Azure

> Backup-Ziele sind für Workloads in Amazon FSx for NetApp ONTAP und Azure NetApp Files nicht verfügbar. Führen Sie Backup-Vorgänge mit nativen Backup-Lösungen durch: FSx for ONTAP Backup-Service oder Azure NetApp Files Backups.

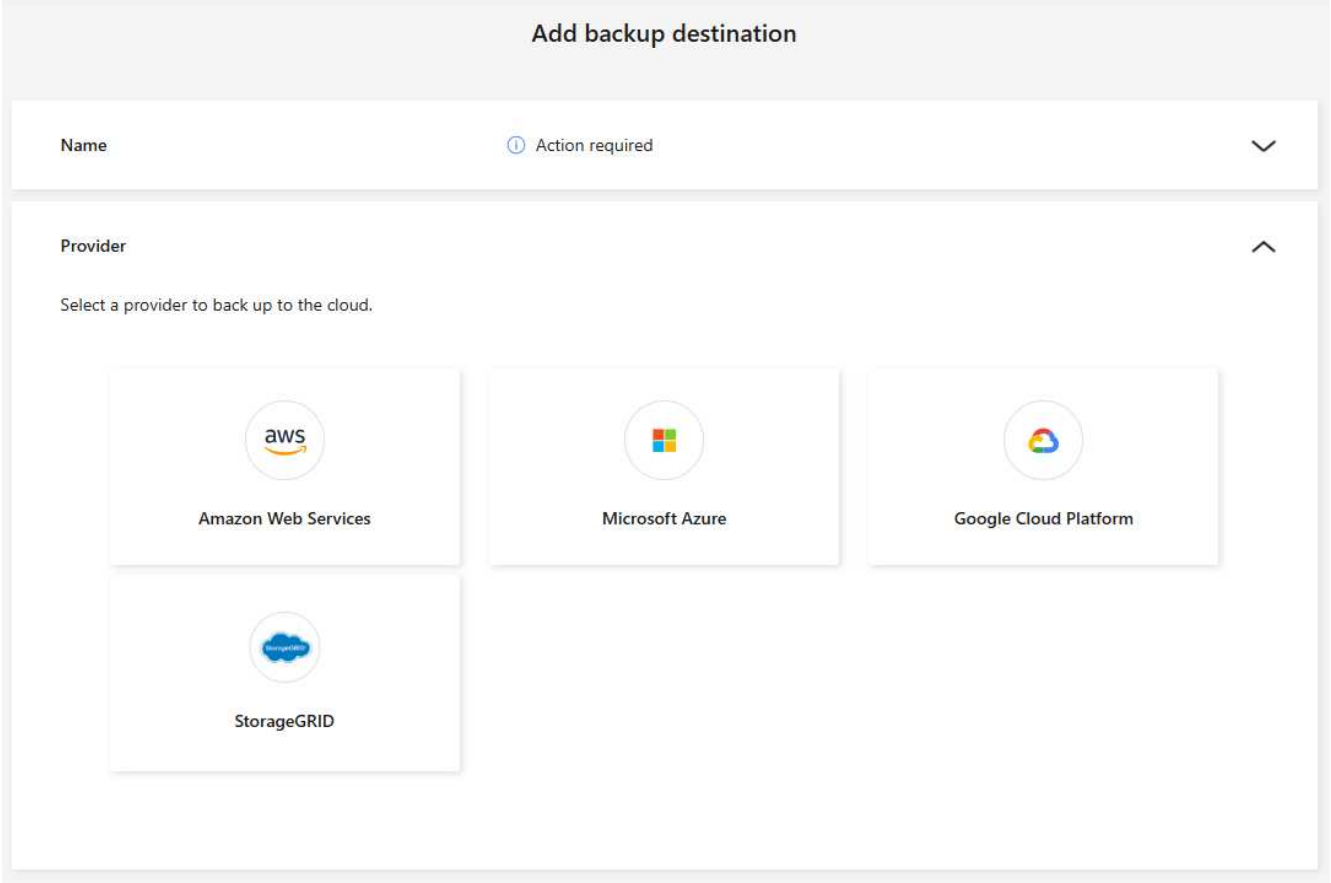
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

StorageGRID als Backup-Ziel hinzufügen

Um NetApp StorageGRID als Sicherungsziel einzurichten, geben Sie die folgenden Informationen ein.

Schritte

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Wählen Sie in der Kachel **Backup-Ziele Anzeigen** aus.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Namen für das Sicherungsziel ein.

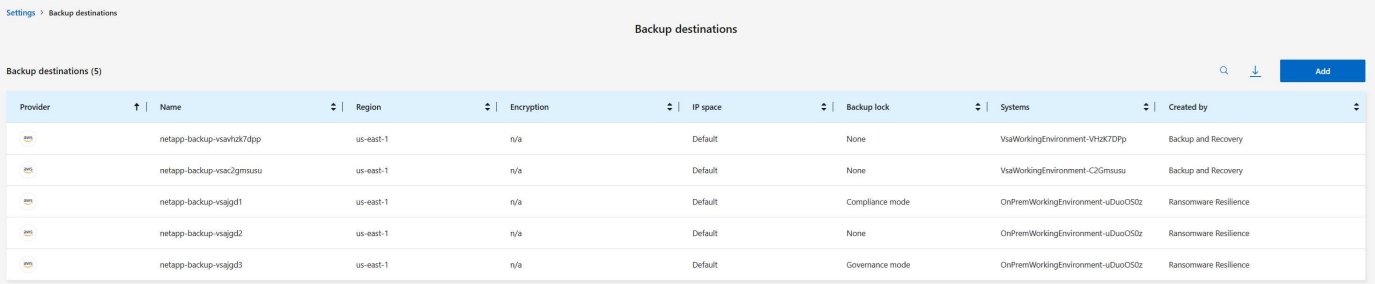


5. Wählen Sie * StorageGRID*.
6. Wählen Sie den Abwärtspfeil neben jeder Einstellung aus, um die erforderlichen Felder zu überprüfen:
   - **Anbietereinstellungen**:
     - Wählen Sie **Neuen Bucket erstellen** oder **Eigenen Bucket verwenden**.
     - Geben Sie den **vollqualifizierten Domainnamen (FQDN) des Gateway-Knotens** und den **Port** an.
     - Geben Sie die StorageGRID-Anmeldedaten an: **Access key** und **Secret key**.
   - **Netzwerk**: Wählen Sie den IP-Bereich.
     - Der IPspace ist der Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.
   - **Backup Lock**

     Wählen Sie, ob Sie die Backup-Sperre konfigurieren möchten. Mit Backup-Sperre sind Kopien vor Änderungen oder Löschung geschützt und werden auf Ransomware-Bedrohungen überprüft. Sie können diese Einstellung nach der Konfiguration des Backup-Ziels nicht mehr ändern. **Wenn Sie keine Backup-Sperre möchten, wählen Sie** None**.** Wählen Sie **Governance mode**, um Benutzern mit bestimmten Berechtigungen das Überschreiben oder Löschen geschützter Backup-Dateien während der Aufbewahrungsfrist zu ermöglichen. **Wählen Sie** Compliance mode**, um zu verhindern, dass Benutzer geschützte Backup-Dateien während der Aufbewahrungsfrist überschreiben oder löschen.
7. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.



Amazon Web Services als Sicherungsziel hinzufügen

Um AWS als Sicherungsziel einzurichten, geben Sie die folgenden Informationen ein.

Weitere Informationen zur Verwaltung Ihres AWS-Speichers in der Konsole finden Sie unter "Verwalten Sie Ihre Amazon S3-Buckets".

Schritte

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Wählen Sie in der Kachel **Backup-Ziele Anzeigen** aus.
3. Wählen Sie **Hinzufügen**.
4. Wählen Sie **Amazon Web Services** aus.
5. Wählen Sie den Abwärtspfeil neben jeder Einstellung aus und geben Sie Werte ein oder wählen Sie sie aus:
   - **Anbietereinstellungen**:
     - Erstellen Sie einen neuen Bucket, wählen Sie einen vorhandenen Bucket aus, falls bereits einer in der Konsole vorhanden ist, oder bringen Sie Ihren eigenen Bucket mit, in dem die Backups gespeichert werden.
     - AWS-Konto, Region, Zugriffsschlüssel und geheimer Schlüssel für AWS-Anmeldeinformationen

       "Wenn Sie Ihren eigenen Bucket mitbringen möchten, lesen Sie S3-Buckets hinzufügen." .
   - **Verschlüsselung**: Wenn Sie einen neuen S3-Bucket erstellen, geben Sie die Verschlüsselungsschlüsselinformationen ein, die Sie vom Anbieter erhalten haben. Wenn Sie einen vorhandenen Bucket auswählen, sind die Verschlüsselungsinformationen bereits verfügbar.

     Daten im Bucket werden standardmäßig mit von AWS verwalteten Schlüsseln verschlüsselt. Sie können weiterhin von AWS verwaltete Schlüssel verwenden oder die Verschlüsselung Ihrer Daten mit Ihren eigenen Schlüsseln verwalten.
   - **Netzwerk**: Wählen Sie den IP-Bereich und geben Sie an, ob Sie einen privaten Endpunkt verwenden möchten.
     - Der IPspace ist der Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.
     - Wählen Sie optional aus, ob Sie einen zuvor konfigurierten privaten AWS-Endpunkt (PrivateLink) verwenden möchten.

       Wenn Sie AWS PrivateLink verwenden möchten, lesen Sie "AWS PrivateLink für Amazon S3" .

- **Backup-Sperre**: Wählen Sie, ob Ransomware Resilience Backups vor Änderungen oder Löschungen schützen soll. Diese Option verwendet die NetApp DataLock-Technologie. Jedes Backup wird während der Aufbewahrungsfrist oder für mindestens 30 Tage zuzüglich einer Pufferzeit von bis zu 14 Tagen gesperrt.

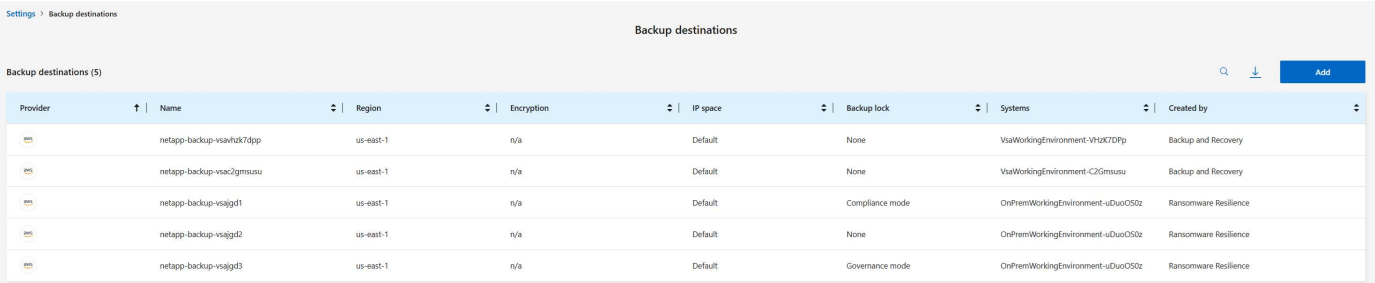
  Wenn Sie die Backup-Sperreinstellung jetzt konfigurieren, können Sie die Einstellung nach der Konfiguration des Backup-Ziels nicht mehr ändern.

  - **Governance-Modus**: Bestimmte Benutzer (mit der Berechtigung s3:BypassGovernanceRetention) können geschützte Dateien während der Aufbewahrungsfrist überschreiben oder löschen.
  - **Compliance-Modus**: Benutzer können geschützte Sicherungsdateien während der Aufbewahrungsfrist nicht überschreiben oder löschen.

6. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.



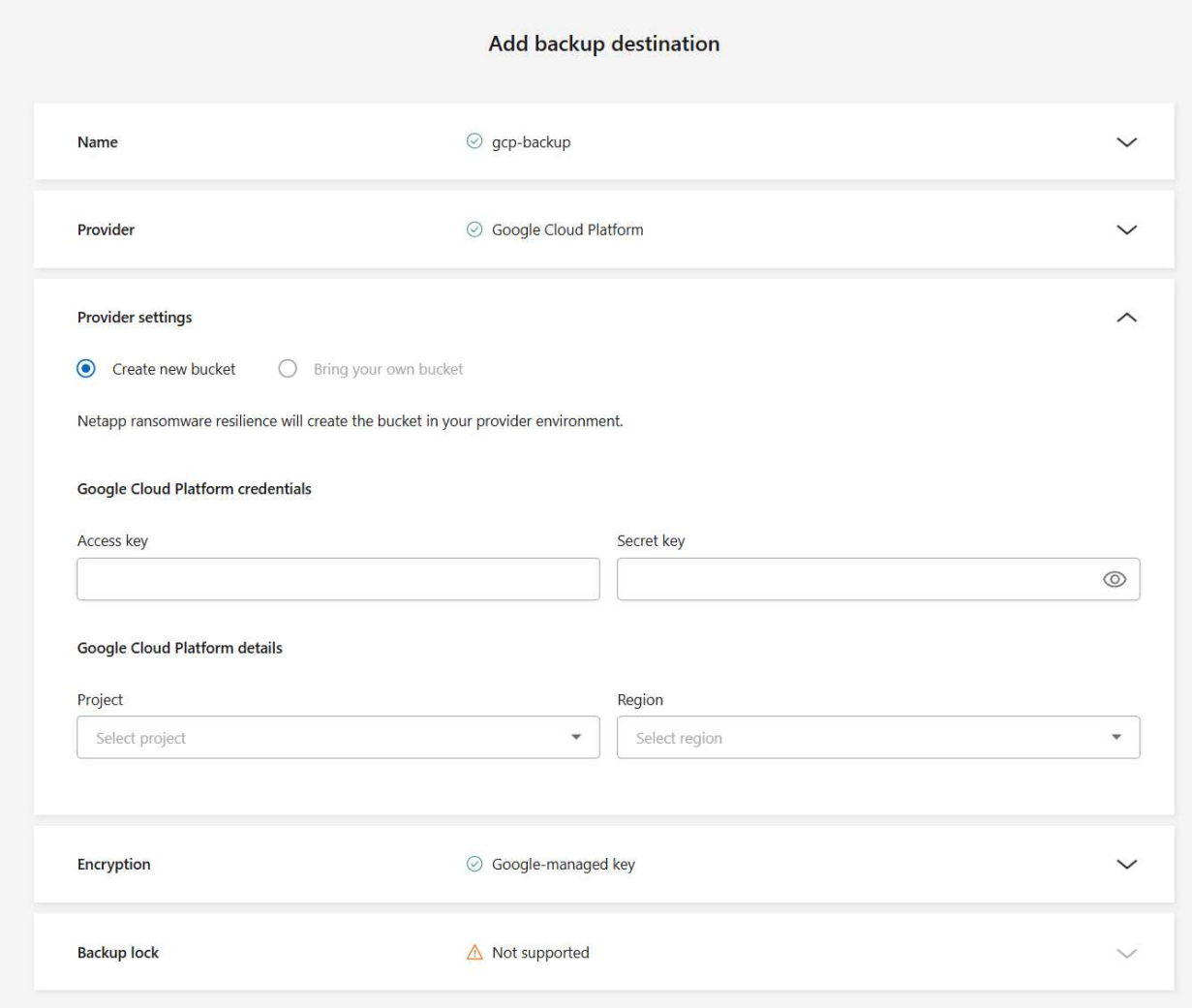
Google Cloud Platform als Backup-Ziel hinzufügen

Um Google Cloud Platform (GCP) als Sicherungsziel einzurichten, geben Sie die folgenden Informationen ein.

Weitere Informationen zur Verwaltung Ihres GCP-Speichers in der Konsole finden Sie unter "Installationsoptionen für den Konsolenagenten in Google Cloud".

Schritte

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Wählen Sie in der Kachel **Backup-Ziele Anzeigen** aus.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Namen für das Sicherungsziel ein.
5. Wählen Sie **Google Cloud Platform** aus.
6. Wählen Sie den Abwärtspfeil neben jeder Einstellung aus und geben Sie Werte ein oder wählen Sie sie aus:
   - **Anbietereinstellungen**:
     - Wählen Sie **Neuen Bucket erstellen** oder **Eigenen Bucket verwenden**.
     - Geben Sie die Google Cloud Platform-Anmeldeinformationen an: **Access key** und **Secret key**.
     - Wählen Sie Ihr **Projekt** und die **Region**, in der es sich befindet.



- **Verschlüsselung**: Wenn Sie einen neuen Bucket erstellen, geben Sie die Verschlüsselungsschlüsselinformationen ein, die Sie vom Anbieter erhalten haben. Wenn Sie einen vorhandenen Bucket auswählen, sind die Verschlüsselungsinformationen bereits verfügbar.

  Die Daten im Bucket werden standardmäßig mit von Google verwalteten Schlüsseln verschlüsselt. Sie können die Standardeinstellung beibehalten, indem Sie **Google-managed keys** auswählen oder **Customer-managed keys** verwenden.

7. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.

Microsoft Azure als Sicherungsziel hinzufügen

Um Azure als Sicherungsziel einzurichten, geben Sie die folgenden Informationen ein.

Weitere Informationen zur Verwaltung Ihrer Azure-Anmeldeinformationen und Marketplace-Abonnements in der Konsole finden Sie unter "Verwalten Sie Ihre Azure-Anmeldeinformationen und Marketplace-Abonnements" .

Schritte

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.

2. Wählen Sie in der Kachel **Backup-Ziele Anzeigen** aus.
3. Wählen Sie **Hinzufügen**.
4. Wählen Sie **Azure** aus.
5. Wählen Sie den Abwärtspfeil neben jeder Einstellung aus und geben Sie Werte ein oder wählen Sie sie aus:
   - **Anbietereinstellungen**:
     - Erstellen Sie ein neues Speicherkonto, wählen Sie ein vorhandenes aus, falls in der Konsole bereits eines vorhanden ist, oder verwenden Sie Ihr eigenes Speicherkonto, in dem die Sicherungen gespeichert werden.
     - Geben Sie die Application (client) ID, das Client secret und die Directory (tenant) ID an. Wählen Sie **Authenticate**.
     - Wählen Sie das Azure-Abonnement, die Region und die Ressourcengruppe für Ihr Azure-Abonnement aus.

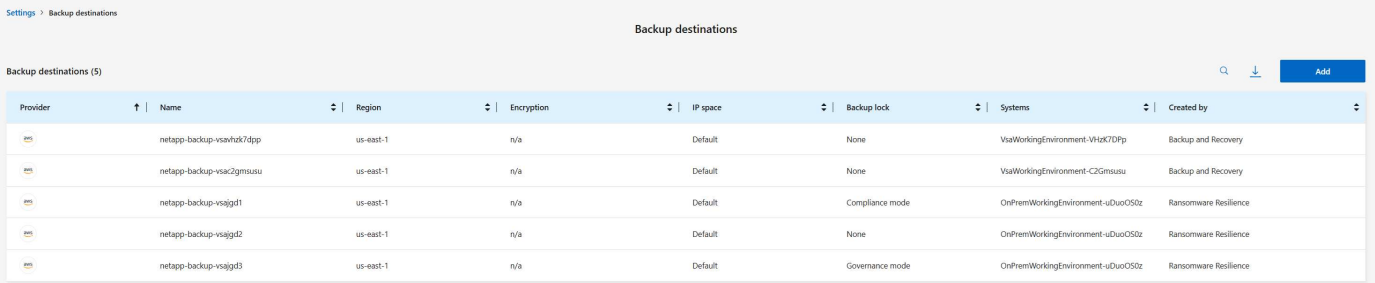
       "Wenn Sie Ihr eigenes Speicherkonto verwenden möchten, lesen Sie den Abschnitt Azure Blob-Speicherkonten hinzufügen." .
   - **Verschlüsselung**: Standardmäßig werden Daten mit einem von Microsoft verwalteten Schlüssel verschlüsselt. Wählen Sie **Microsoft-managed key**, um diese Option beizubehalten; alternativ können Sie **Customer managed key** wählen, um Ihre eigenen Schlüssel für die Verschlüsselung zu verwenden.
   - **Netzwerk**: Wählen Sie den IP-Bereich und geben Sie an, ob Sie einen privaten Endpunkt verwenden möchten.
     - Der IPspace ist der Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.
     - Wählen Sie optional aus, ob Sie einen zuvor konfigurierten privaten Azure-Endpunkt verwenden möchten.

       Wenn Sie Azure PrivateLink verwenden möchten, lesen Sie "Azure PrivateLink" .
   - **Backup Lock**

     Wählen Sie, ob Sie die Backup-Sperre konfigurieren möchten. Mit Backup-Sperre sind Kopien vor Änderungen oder Löschung geschützt und werden auf Ransomware-Bedrohungen überprüft. Sie können diese Einstellung nach der Konfiguration des Backup-Ziels nicht mehr ändern. **Wenn Sie keine Backup-Sperre möchten, wählen Sie** None**.** Wählen Sie **Governance mode**, um Benutzern mit bestimmten Berechtigungen das Überschreiben oder Löschen geschützter Backup-Dateien während der Aufbewahrungsfrist zu ermöglichen. **Wählen Sie** Compliance mode**, um zu verhindern, dass Benutzer geschützte Backup-Dateien während der Aufbewahrungsfrist überschreiben oder löschen.
6. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.



Schützen Sie Workloads mit NetApp Ransomware Resilience -Schutzstrategien

Strategien zum Schutz vor Ransomware sind ein zentrales Merkmal der NetApp Ransomware Resilience: Sie unterstützen Erkennung, Schutz und Replikation. Schutzstrategien sind ein wesentlicher Bestandteil Ihrer Cybersicherheitsstrategie.

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 einen besseren Schutz Ihrer Datenbestände können Sie "Gruppen-Workloads" erstellen, um Volumes gemeinsam unter einer Strategie zu schützen.

Schutzrichtlinien mit anderen von NetApp verwalteten Diensten

Neben Ransomware Resilience können Sie NetApp Backup and Recovery verwenden, um den Schutz für

Dateifreigaben und VM-Dateifreigaben zu verwalten.

Schutzinformationen von Backup & Recovery Services werden in Ransomware Resilience angezeigt. Sie können diesen Services mit Ransomware Resilience Erkennungsrichtlinien hinzufügen. Das Hinzufügen einer Datensicherungsstrategie mit Ransomware Resilience ersetzt die bestehenden Datensicherungsstrategien.

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 oder Ransomware Resilience verwaltet wird, wurden möglicherweise Snapshots im Rahmen von ONTAP oder anderen Produkten erstellt. Wenn ONTAP FPolicy-Schutz aktiviert ist, können Sie den FPolicy-Schutz mit ONTAP ändern.

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

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

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 bestehenden Snapshot- oder Backup-Richtlinien von Backup and Recovery protection durch Datensicherungsstrategien, 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" .

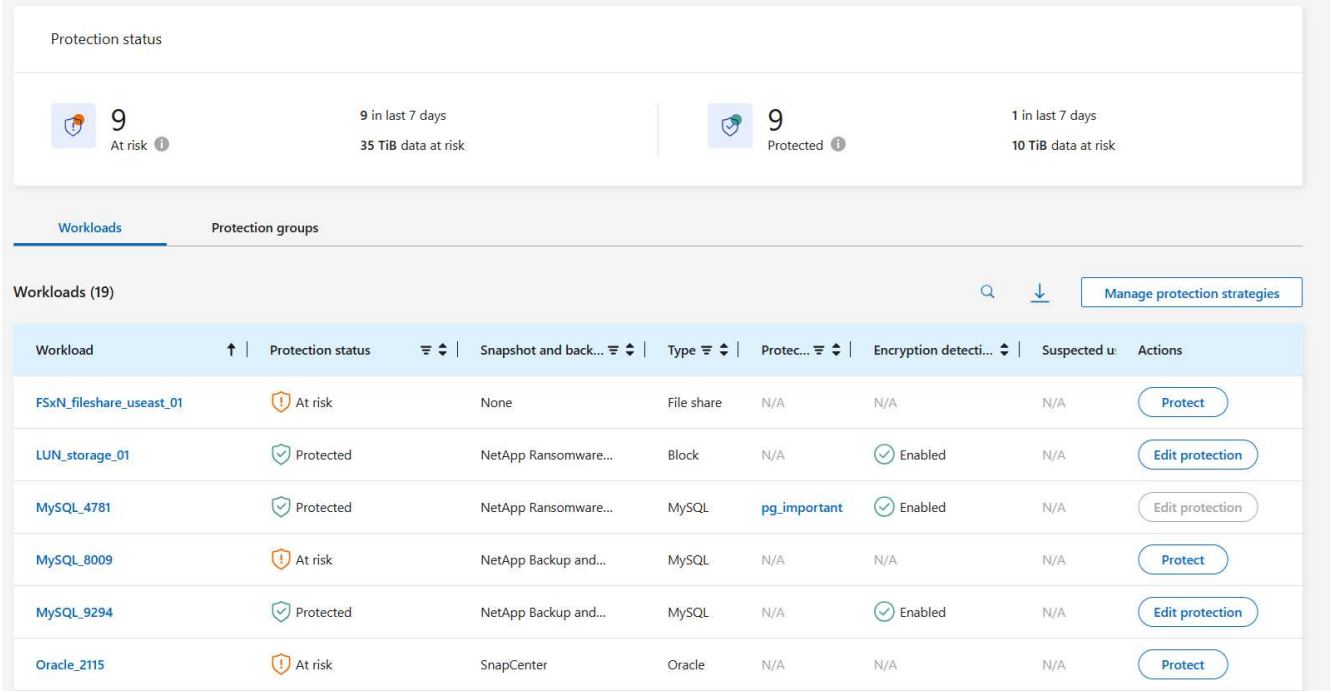
Erstellen Sie eine Ransomware-Schutzstrategie (wenn Sie keine Snapshot- oder Backup-Richtlinien haben)

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:

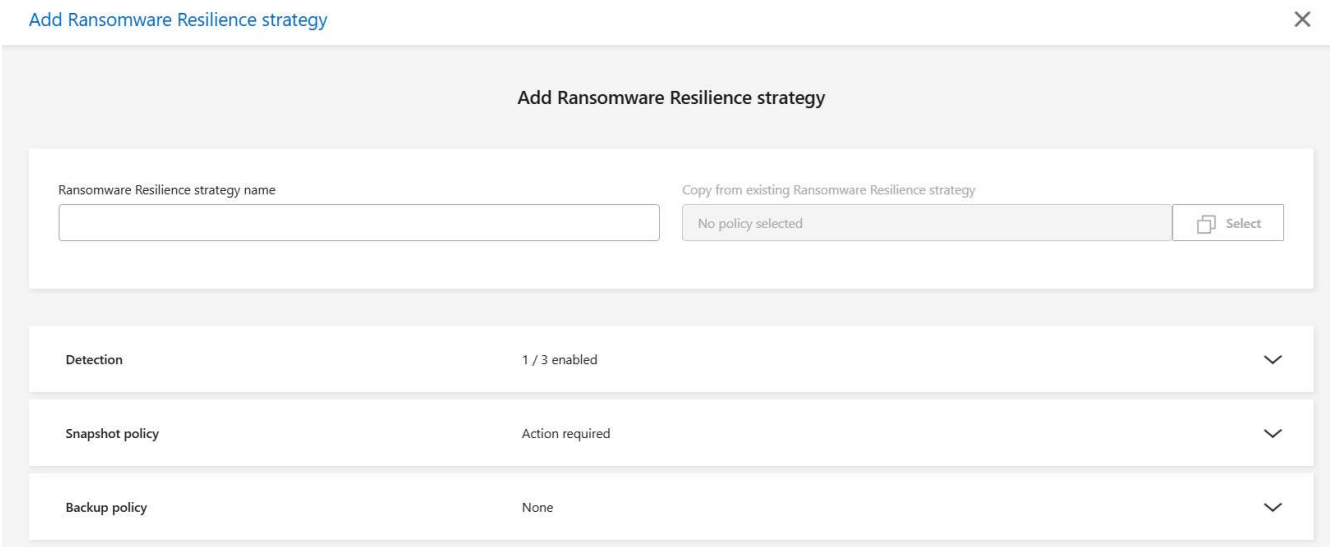
- Snapshot-Richtlinie
- Sicherungsrichtlinie
- Richtlinie zur Ransomware-Erkennung
- Sekundäre Replikation zu ONTAP

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 Sicherungssperrung auf sekundärem 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 eine Erkennungsrichtlinie zu Workloads mit vorhandenen Snapshot- und Backup-Richtlinien hinzu, die von Backup and Recovery verwaltet werden

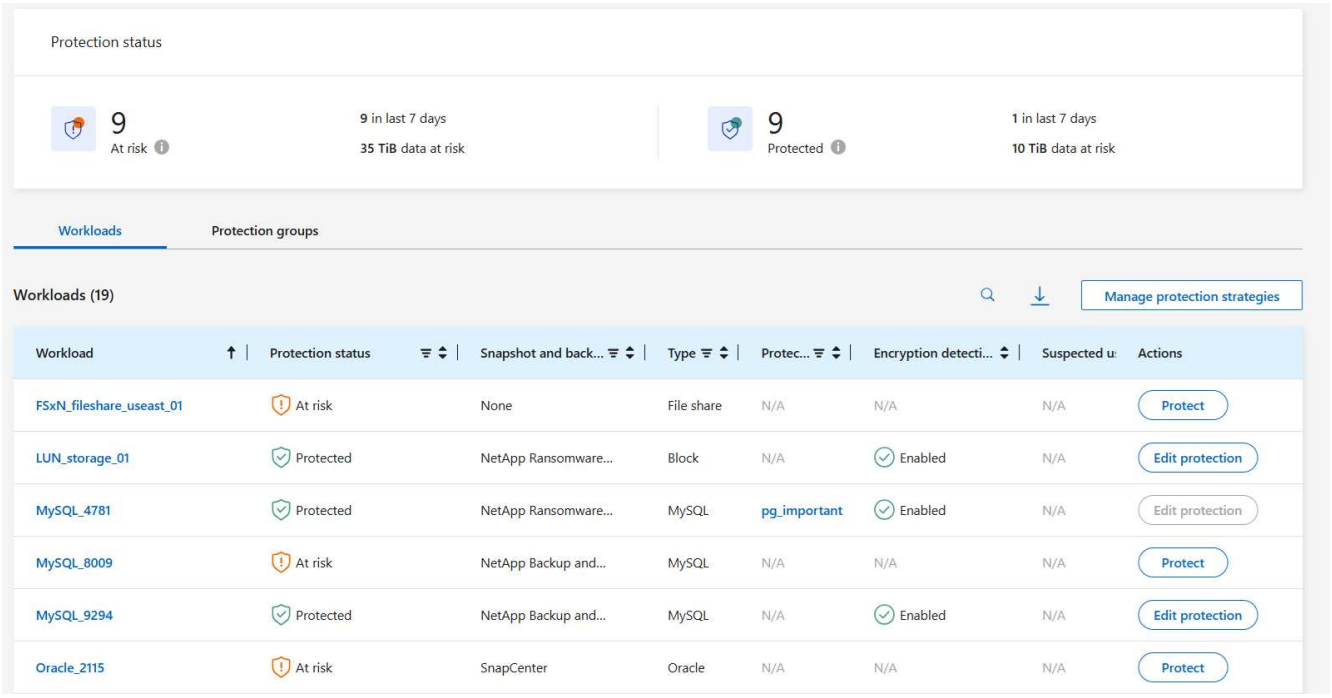
Ransomware Resilience ermöglicht es Ihnen, entweder eine Erkennungsrichtlinie oder eine Datensicherungsstrategie auf Workloads mit bestehendem Snapshot- und Backup-Schutz, der in anderen NetApp Produkten oder Diensten verwaltet wird, anzuwenden. Backup and Recovery verwendet Richtlinien, die Snapshots, die Replikation auf Sekundärspeicher oder Backups auf Objektspeicher steuern.

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

Wenn Sie bereits Snapshot- oder Backup-Richtlinien mit Backup and Recovery verwenden, können Sie eine Richtlinie zum Erkennen von Ransomware-Angriffen hinzufügen. Um Schutz und Erkennung mit Ransomware Resilience zu verwalten, siehe Schutz 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 bereits aktive Backup and Recovery policies vorhanden sind.
4. Um Ihre bestehende Backup and Recovery beizubehalten und nur eine *detection* policy anzuwenden, lassen Sie das Kontrollkästchen **Vorhandene Richtlinien ersetzen** deaktiviert.
5. Wählen Sie die gewünschten Erkennungseinstellungen aus:
   - **Verschlüsselungserkennung**
   - **Erkennung verdächtigen Benutzerverhaltens**
   - **Verdächtige Dateierweiterungen blockieren**
6. Wählen Sie **Weiter**.
7. 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.

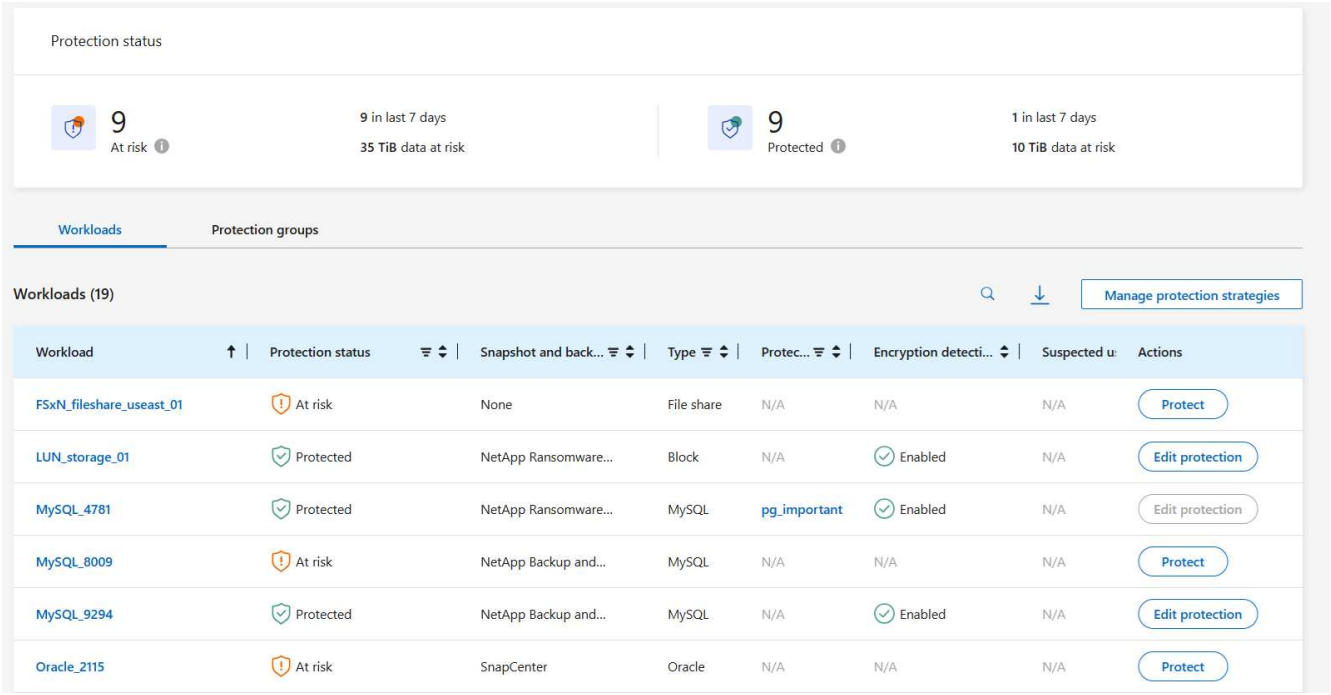
8. Wählen Sie **Weiter**.
9. Überprüfen Sie Ihre Auswahl. Wählen Sie **Erstellen**, um die Erkennung zu aktivieren.
10. Überprüfen Sie auf der Seite „Schutz“ den **Erkennungsstatus**, um zu bestätigen, dass die Erkennung aktiv ist.

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 bereits aktive Backup and Recovery policies vorhanden sind. Um die vorhandenen policies zu ersetzen, aktivieren Sie das Kontrollkästchen **Replace existing policies**. Wenn Sie das Kontrollkästchen aktivieren, ersetzt Ransomware Resilience die Liste der detection policies durch detection policies.
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 bereits eine Backup and Recovery-Strategie existiert, die Sie beibehalten möchten, deaktivieren Sie **Replace existing policies**. Um die vorhandenen Strategien zu ersetzen, aktivieren Sie **Replace existing policies**.
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.

Verwalten Sie Strategien zum Schutz vor Ransomware

Sie können eine Ransomware-Strategie löschen.

Durch eine Ransomware-Schutzstrategie geschützte Workloads anzeigen

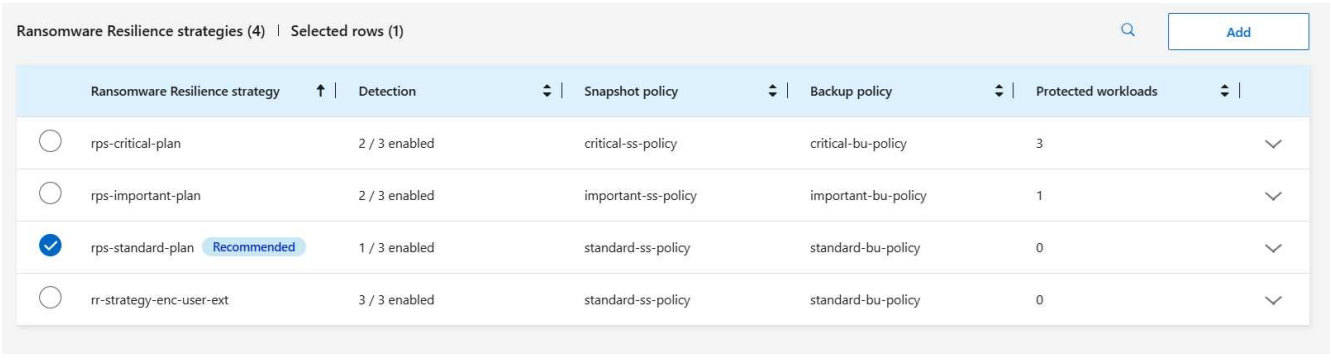
Bevor Sie eine Ransomware-Schutzstrategie löschen, möchten Sie möglicherweise prüfen, welche Workloads durch diese Strategie geschützt sind.

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.

Benutzeraktivitätserkennung konfigurieren

Erfahren Sie mehr über die Erkennung von Benutzeraktivitäten in NetApp Ransomware Resilience

Mit der Erkennung von Benutzeraktivitäten ermöglicht NetApp Ransomware Resilience Ihnen, Ransomware-Ereignisse auf Benutzerebene zu adressieren und Ereignisse wie Datenlecks und großflächige Löschungen zu stoppen.

NetApp Ransomware Resilience bietet eine KI-gestützte Erkennung von Datenschutzverletzungen durch Überwachung verdächtiger Benutzeraktivitäten. Deutliche Anstiege der Leseaktivität und Zugriffsmuster bei Lesezugriffen werden genutzt, um böswillige Absichten zu erkennen. Nach der Erkennung generiert Ransomware Resilience automatisch Warnmeldungen in der NetApp Console, per E-Mail und in jedem konfigurierten Sicherheitssystem (zum Beispiel SIEM).

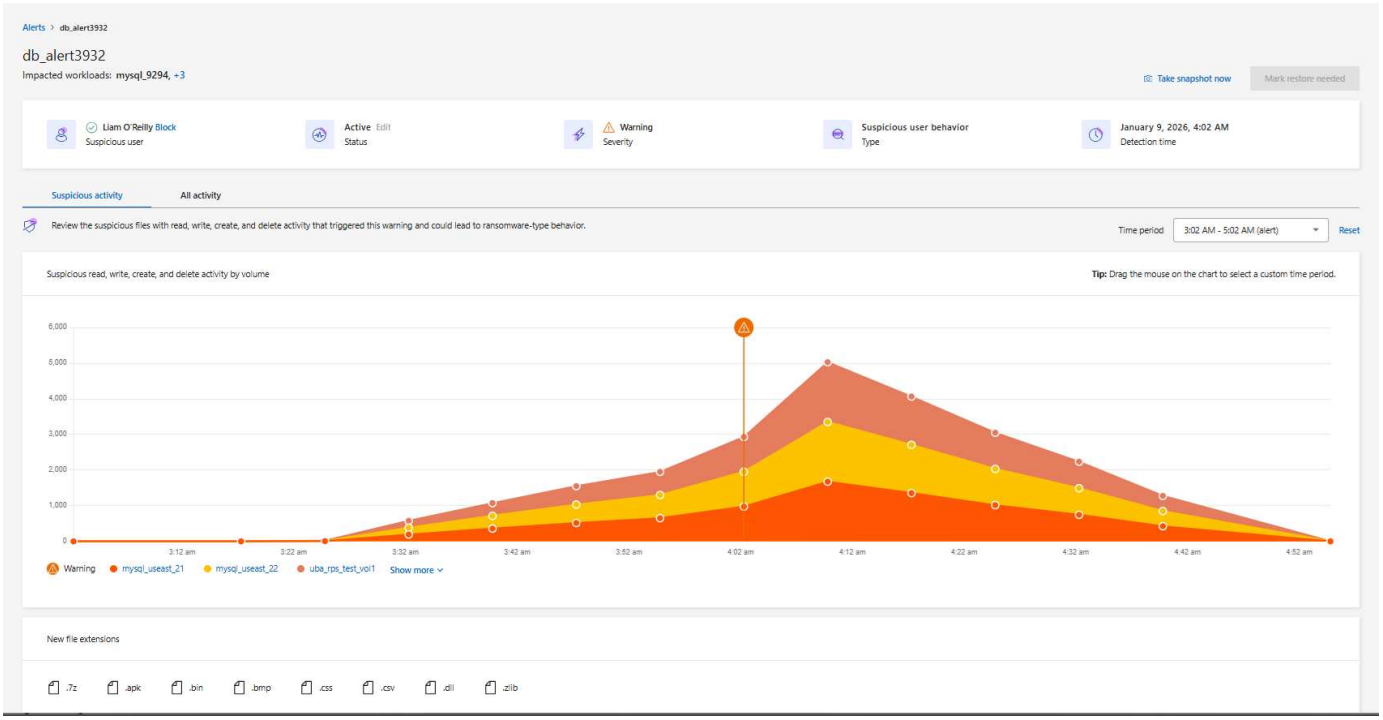
Durch die Erkennung und Benachrichtigung über verdächtiges Nutzerverhalten warnt Sie Ransomware Resilience vor Datenlecks und Datenzerstörungsversuchen sowie Mustern, die verdächtig erscheinen. In jeder Benachrichtigung identifiziert Ransomware Resilience einen Benutzer, den Sie sperren können.

Ransomware Resilience erkennt verdächtige Benutzeraktivitäten durch die Analyse von Benutzeraktivitätsereignissen, die von FPolicy in ONTAP generiert werden. Um Daten zur Benutzeraktivität zu erfassen, müssen Sie einen oder mehrere Benutzeraktivitätsagenten bereitstellen. Der Agent ist ein Linux-Server oder eine VM mit Konnektivität zu Geräten auf Ihrem Mandanten.

Die Erkennung von Benutzeraktivitäten wird derzeit für SAN-Workloads nicht unterstützt. Sie können die Erkennung von Benutzeraktivitäten mit NAS-Workloads in Amazon FSxN für ONTAP, Cloud Volumes ONTAP und ONTAP verwenden.

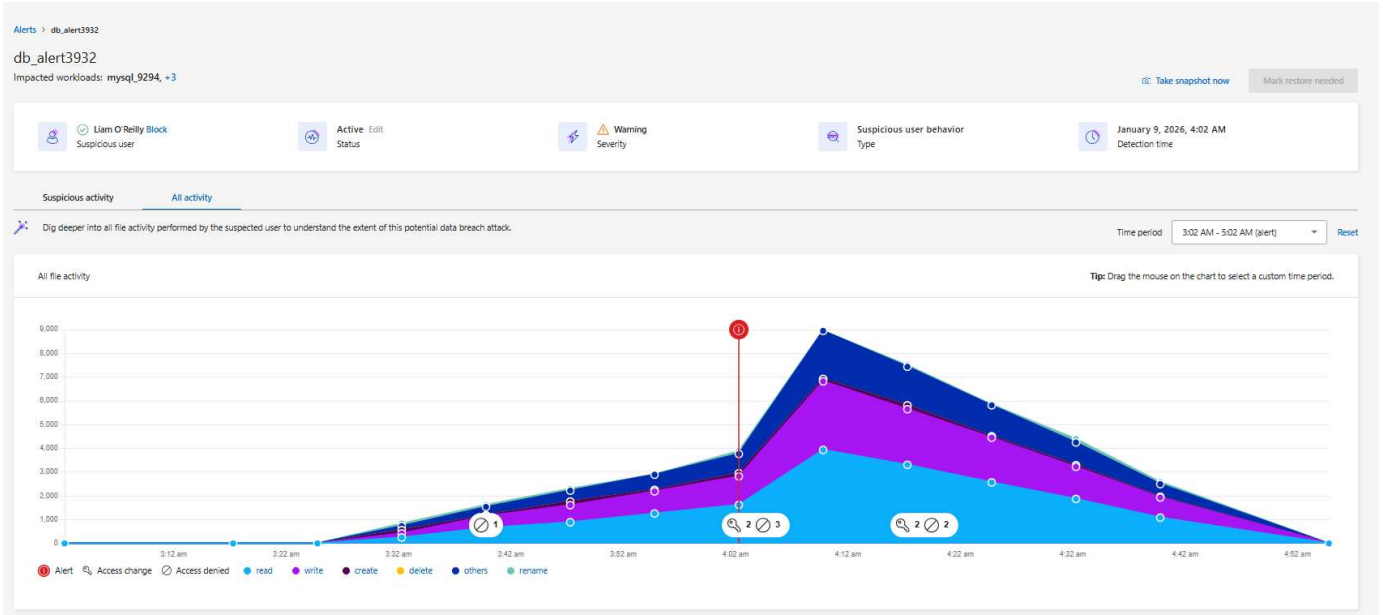
Forensik verdächtiger Benutzeraktivität

Ransomware Resilience bietet forensische Analysen des Nutzerverhaltens: Listen und Diagramme zeigen, wann verdächtige Aktivitäten auftraten und wann Benachrichtigungen versendet wurden. Diese zeigen die Häufigkeit verdächtiger Aktivitäten auf Dateien, Verzeichnissen, Volumes und Workloads im Zeitverlauf, um die Ereignisse zu veranschaulichen. Sie können auch das Auftreten neuer Dateierweiterungen beobachten.



.

Sie können verdächtige Aktivitäten mit einer Übersicht aller Aktivitäten vergleichen. In der Übersicht aller Aktivitäten können Sie neben Zugriffsänderungs- und Zugriffsverweigerungsereignissen auch Lese-, Schreib-, Umbenennungs-, Verschiebe-, Erstellungs- und Löschereignisse beobachten.



.

Komponenten

Es gibt drei Schlüsselkomponenten bei der Erkennung verdächtiger Benutzeraktivitäten in der Ransomware Resilience.

- Der **Benutzeraktivitätsagent** ist eine ausführbare Umgebung für Datensammler. Sie müssen den Benutzeraktivitätsagenten konfigurieren.

- Der **Datensammler** teilt Benutzeraktivitätsereignisse mit Ransomware Resilience. Der Datensammler wird automatisch erstellt, wenn Sie "Aktivieren Sie eine Ransomware-Schutzstrategie mit Erkennung verdächtiger Benutzeraktivität".
- Der **Benutzerverzeichnis-Connector** ermöglicht die Zuordnung von Benutzernamen und Benutzer-IDs und sorgt so für mehr Klarheit bei der Reaktion auf verdächtiges Benutzerverhalten. Sie müssen den Benutzerverzeichnis-Connector konfigurieren.

Ransomware Resilience und Data Infrastructure Insights

Die Erkennung verdächtigen Nutzerverhaltens in Ransomware Resilience ist eine Integration mit Data Infrastructure Insights (DII) Workload Security und verwendet "DII-Endpunkte". Sie benötigen keine DII-Konfiguration, um die Nutzerverhaltenserkennung in Ransomware Resilience zu aktivieren. Um die Nutzerverhaltenserkennung zu aktivieren, "Erstellen Sie die erforderlichen Agenten und Collector und aktivieren Sie die geeignete Ransomware-Schutzstrategie".

Wenn Sie bereits NetApp Data Infrastructure Insights (DII) Workload Security verwenden, wird empfohlen, dieselben Workload Security Agents auch für Ransomware Resilience zu verwenden. Sie müssen keine separaten Workload Security Agents für Ransomware Resilience bereitstellen, jedoch erfordert die Verwendung derselben Workload Security Agents eine Kopplung zwischen der Ransomware Resilience Console Organization und dem DII Storage Workload Security Tenant. Wenden Sie sich an Ihren Account Representative, um diese Kopplung zu aktivieren.

Nächste Schritte

- "Anforderungen für die Erkennung von Benutzeraktivitäten"
- "Konfigurieren Sie Agenten und Detektoren für Benutzerverhaltensaktivitäten"

Anforderungen an die Erkennung von Benutzeraktivitäten für NetApp Ransomware Resilience

NetApp Ransomware Resilience Benutzerverhaltenserkennung ermöglicht es Ihnen, auf Ransomware-Ereignisse auf Benutzerebene zu reagieren. Sie müssen eine Gruppe von Agenten erstellen, um die Benutzerverhaltenserkennung zu aktivieren. Bevor Sie die Erkennung aktivieren, müssen Sie sicherstellen, dass Sie die beschriebenen Betriebssystem-, Server- und Netzwerkvoraussetzungen erfüllen, damit Ransomware Resilience Ereignisse korrekt erkennen und melden kann.

Cloud-Anbieter-Support

Verdächtige Benutzeraktivitätsdaten können in AWS und Azure in den folgenden Regionen gespeichert werden:

Cloud-Anbieter	Region
AWS	• Asien-Pazifik (Sydney) (ap-southeast-2) • Europa (Frankfurt) (eu-central-1) • US Ost (Nord-Virginia) (us-east-1)
Azurblau	Ostküste der USA

Betriebssystemanforderungen

Die Erkennung verdächtigen Benutzerverhaltens wird mit den folgenden Betriebssystemen unterstützt:

Betriebssystem	Unterstützte Versionen
AlmaLinux	9.4 (64 Bit) bis 9.5 (64 Bit) und 10 (64 Bit), einschließlich SELinux
CentOS	CentOS Stream 9 (64 Bit)
Debian	11 (64 Bit), 12 (64 Bit), einschließlich SELinux
OpenSUSE Leap	15.3 (64 Bit) bis 15.6 (64 Bit)
Oracle Linux	8.10 (64 Bit) und 9.1 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux
Red Hat	8.10 (64 Bit), 9.1 (64 Bit) bis 9.6 (64 Bit) und 10 (64 Bit), einschließlich SELinux
Felsig	Rocky 9.4 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux
SUSE Enterprise Linux	15 SP4 (64 Bit) bis 15 SP6 (64 Bit), einschließlich SELinux
Ubuntu	20.04 LTS (64 Bit), 22.04 LTS (64 Bit) und 24.04 LTS (64 Bit)

Auf dem Computer, den Sie für den Benutzeraktivitätsagenten verwenden, sollte keine andere Software auf Anwendungsebene ausgeführt werden. Ein dedizierter Server wird empfohlen.

Der `unzip` Für die Installation wird ein Befehl benötigt. Der `sudo su -` Der Befehl wird für die Installation, die Ausführung von Skripten und die Deinstallation benötigt.

Serveranforderungen

Der Server muss die folgenden Mindestanforderungen erfüllen:

- **CPU**: 4 Kerne
- **RAM**: 16 GB RAM
- **Festplattenspeicher**: 36 GB freier Festplattenspeicher

Serverempfehlungen

- Weisen Sie zusätzlichen Speicherplatz zu, um die Erstellung des Dateisystems zu ermöglichen. Stellen Sie sicher, dass im Dateisystem mindestens 35 GB freier Speicherplatz vorhanden sind. + Wenn `/opt` Es handelt sich um einen eingebundenen Ordner von einem NAS-Speicher; lokale Benutzer müssen Zugriff auf diesen Ordner haben. Die Erstellung eines Benutzeraktivitätsagenten kann fehlschlagen, wenn lokale Benutzer nicht über die erforderlichen Berechtigungen verfügen.
- Es wird empfohlen, den Benutzeraktivitätsagenten auf einem separaten System zu installieren, das von Ihrer Ransomware Resilience-Umgebung getrennt ist. Wenn Sie sie dennoch auf demselben Rechner installieren, sollten Sie 50 bis 55 GB Festplattenspeicher einplanen. Für Linux sollten Sie 25–30 GB Speicherplatz für `/opt/netapp` und 25 GB für `var/log/netapp` reservieren.

- Es wird empfohlen, die Zeit sowohl auf dem ONTAP System als auch auf dem Rechner des Benutzeraktivitätsagenten mithilfe des Network Time Protocol (NTP) oder des Simple Network Time Protocol (SNTP) zu synchronisieren.

Cloud-Netzwerkzugriffsregeln

Prüfen Sie die Cloud-Netzwerkzugriffsregeln für Ihre jeweilige Region (Asien-Pazifik, Europa oder Vereinigte Staaten).

Ersetzen Sie während der Erstinstallation die `<site_name>` durch eine Platzhalter-(`*` -Berechtigung. Nachdem der Agent aktiviert und voll funktionsfähig ist, können Sie die Berechtigung durch den Standortnamen ersetzen. Wenden Sie sich an Ihren NetApp-Ansprechpartner, um den Standortnamen zu erhalten.

Der Benutzeraktivitätsagent nutzt NetApp Data Insights Infrastructure-Technologie, daher die Verwendung von `cloudinsights` Endpunkten. Weitere Informationen finden Sie unter

Bereitstellungen von Benutzeraktivitätsagenten mit Sitz in APAC

Protokoll	Hafen	Quelle	Ziel	Beschreibung
HTTPS (TCP)	443	Benutzeraktivitätsagent	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	Zugang zu Ransomware-Resilienz

Benutzeraktivitätsagenten-Bereitstellungen mit Sitz in Europa

Protokoll	Hafen	Quelle	Ziel	Beschreibung
HTTPS (TCP)	443	Benutzeraktivitätsagent	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	Zugang zu Ransomware-Resilienz

US-basierte Bereitstellungen von Benutzeraktivitätsagenten

Protokoll	Hafen	Quelle	Ziel	Beschreibung
HTTPS (TCP)	443	Benutzeraktivitätsagent	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	Zugang zu Ransomware-Resilienz

Netzwerkinterne Regeln

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	389 (LDAP) 636 (LDAPs / Start-TLS)	Benutzeraktivitätsagent	LDAP-Server-URL	Mit LDAP verbinden
HTTPS (TCP)	443	Benutzeraktivitätsagent	Cluster- oder SVM-Management-IP-Adresse (abhängig von der SVM-Collector-Konfiguration)	API-Kommunikation mit ONTAP

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000 - 55000	SVM-Daten LIF IP-Adressen	Benutzeraktivitätsagent	Kommunikation von ONTAP an den Benutzeraktivitätsagenten für Fpolicy-Ereignisse. Diese Ports müssen zum Benutzeraktivitätsagenten hin geöffnet werden, damit ONTAP Ereignisse an ihn senden kann, einschließlich etwaiger Firewall-Anforderungen auf dem Benutzeraktivitätsagenten selbst (falls vorhanden). + **HINWEIS:** Sie müssen nicht **alle** dieser Ports reservieren, aber die Ports, die Sie hierfür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, mit der Reservierung von 100 Ports zu beginnen und diese bei Bedarf zu erhöhen.

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000-55000	Cluster-Verwaltungs-IP	Benutzeraktivitätsagent	Kommunikation von der ONTAP Clusterverwaltungs-IP zum Benutzeraktivitätsagenten für **EMS-Ereignisse**. Diese Ports müssen zum Benutzeraktivitätsagenten hin geöffnet werden, damit ONTAP EMS-Ereignisse an ihn senden kann, einschließlich etwaiger Firewall-Anforderungen auf dem Benutzeraktivitätsagenten selbst. + **HINWEIS:** Sie müssen nicht **alle** dieser Ports reservieren, aber die Ports, die Sie hierfür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, mit der Reservierung von 100 Ports zu beginnen und diese bei Bedarf zu erhöhen.
SSH	22	Benutzeraktivitätsagent	Clusterverwaltung	Wird für die CIFS/SMB-Benutzerblockierung benötigt.

Nächster Schritt

- "Benutzeraktivitätsagenten und -sammler konfigurieren"

Konfigurieren der Benutzeraktivitätserkennung in NetApp Ransomware Resilience

NetApp Ransomware Resilience Benutzeraktivitätserkennung hilft Ihnen, Ransomware-Ereignisse auf Benutzerebene zu verhindern. Um die Erkennung verdächtigen Benutzerverhaltens in Ransomware Resilience zu aktivieren, müssen Sie mindestens einen Benutzeraktivitätsagenten installieren, der eine Datenerfassungsumgebung erstellt, um das Benutzerverhalten auf abweichende Muster zu überwachen, die Ransomware-

Ereignissen ähneln.

Ein Benutzeraktivitätsagent hostet einen Datensammler und einen Benutzerverzeichnis-Connector, die beide Daten zur Analyse an einen SaaS-Standort senden.

- Der **Datensammler** erfasst Benutzeraktivitätsdaten von ONTAP. Der Datensammler wird automatisch erstellt, wenn Sie eine Schutzstrategie mit Benutzerverhaltenserkennung erstellen.
- Der **Benutzerverzeichnis-Connector** stellt eine Verbindung zu Ihrem Verzeichnis her, um Benutzer-IDs Benutzernamen zuzuordnen. Sie müssen den Benutzerverzeichnis-Connector konfigurieren.

Der Benutzeraktivitätsagent, der Datensammler und der Benutzerverzeichnis-Connector können alle über das Dashboard der Ransomware Resilience-Einstellungen verwaltet werden.

> Wenn Sie bereits NetApp Data Infrastructure Insights (DII) Workload Security verwenden, wird empfohlen, dieselben Workload Security Agents auch für Ransomware Resilience zu verwenden. Sie müssen keine separaten Workload Security Agents für Ransomware Resilience bereitstellen, jedoch erfordert die Verwendung derselben Workload Security Agents eine Kopplung zwischen der Ransomware Resilience Console Organization und dem DII Storage Workload Security Tenant. Wenden Sie sich an Ihren Account Representative, um diese Kopplung zu aktivieren.

+ Falls Sie *nicht* DII verwenden, fahren Sie mit den Konfigurationsanweisungen hier fort.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie die "Anforderungen an Betriebssystem, Server und Netzwerk" erfüllen.

Erforderliche Konsolenrolle Um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren, benötigen Sie die **Organization admin role**. Für nachfolgende Konfigurationen verdächtiger Benutzeraktivitäten benötigen Sie die **Ransomware Resilience user behavior admin role**. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console".

Stellen Sie sicher, dass jede Rolle auf Organisationsebene angewendet wird.

Erstellen Sie einen Benutzeraktivitätsagenten

Benutzeraktivitätsagenten sind ausführbare Umgebungen für "Datensammler"; Datensammler teilen Benutzeraktivitätsereignisse mit Ransomware Resilience. Sie müssen mindestens einen Benutzeraktivitätsagenten erstellen, um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren.

Schritte

1. Wenn Sie zum ersten Mal einen Benutzeraktivitätsagenten erstellen, gehen Sie zum **Dashboard**. Wählen Sie in der Kachel **Benutzeraktivität** die Option **Aktivieren** aus.

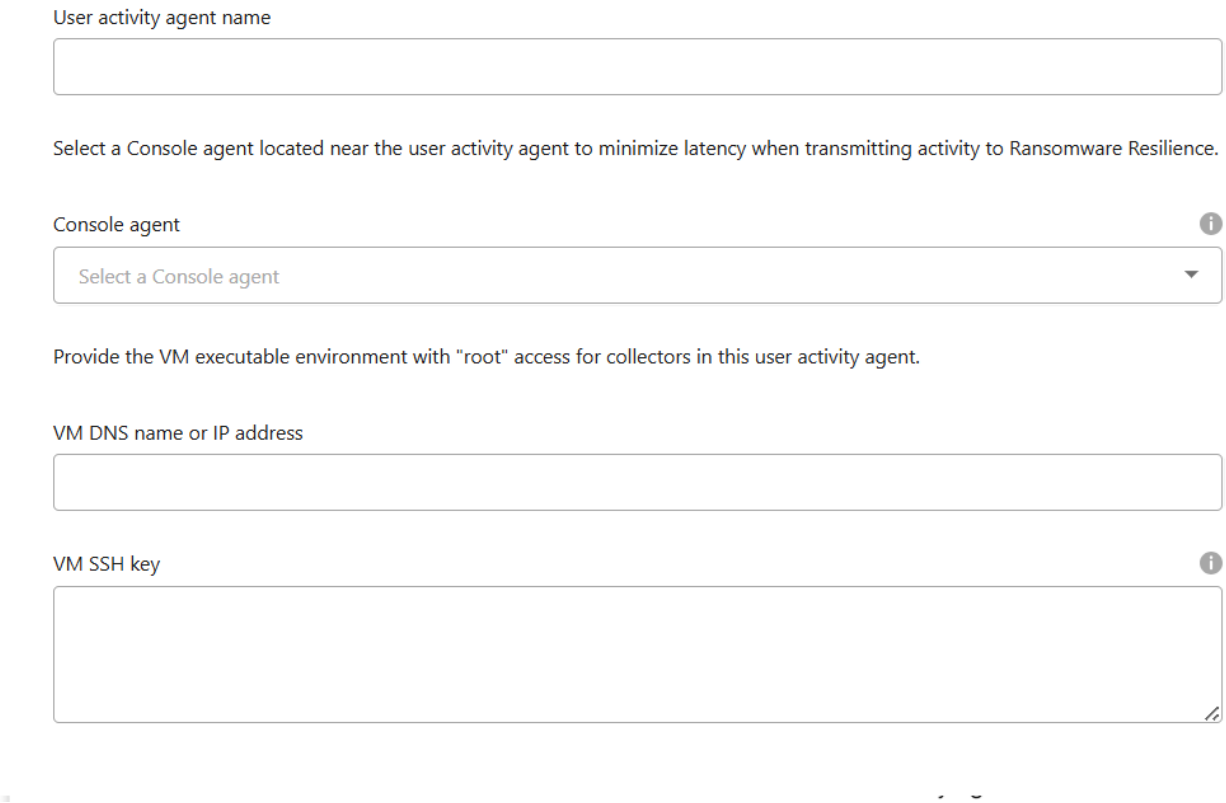
   Wenn Sie einen zusätzlichen Benutzeraktivitätsagenten hinzufügen, gehen Sie zu **Einstellungen**, suchen Sie die Kachel **Benutzeraktivität** und wählen Sie dann **Verwalten**. Wählen Sie auf dem Bildschirm „Benutzeraktivität“ die Registerkarte **Benutzeraktivitätsagenten** und dann **Hinzufügen**.

2. Wählen Sie einen **Cloud-Anbieter** und dann eine **Region** aus. Wählen Sie **Weiter**.
3. Geben Sie die Details des Benutzeraktivitätsagenten an:
   - **Name des Benutzeraktivitätsagenten**
   - **Konsolenagent** - Der Konsolenagent sollte sich im selben Netzwerk wie der Benutzeraktivitätsagent

befinden und über eine SSH-Verbindung zur IP-Adresse des Benutzeraktivitätsagenten verfügen.

- **VM-DNS-Name oder IP-Adresse**
- **VM SSH Key** - Geben Sie den SSH-Schlüssel in diesem Format ein:

```
-----BEGIN OPENSSH PRIVATE KEY-----
private-key-contents
-----END OPENSSH PRIVATE KEY-----
```



4. Wählen Sie **Weiter**.
5. Überprüfen Sie Ihre Einstellungen. Wählen Sie **Aktivieren**, um das Hinzufügen des Benutzeraktivitätsagenten abzuschließen.
6. Bestätigen Sie, dass der Benutzeraktivitätsagent erfolgreich erstellt wurde. In der Kachel „Benutzeraktivität“ wird eine erfolgreiche Bereitstellung als **Wird ausgeführt** angezeigt.

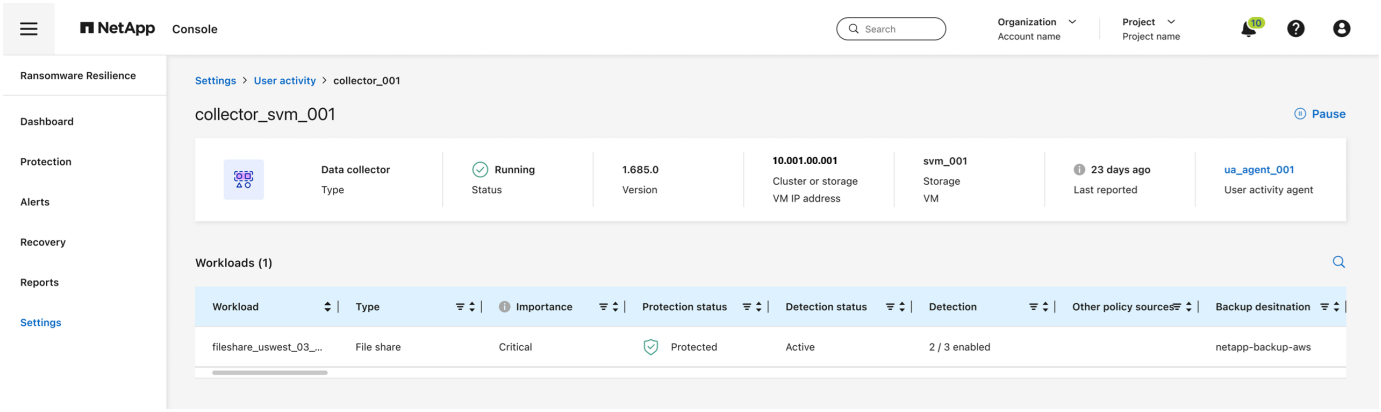
Ergebnis

Nachdem der Benutzeraktivitätsagent erfolgreich erstellt wurde, kehren Sie zum Menü **Einstellungen** zurück und wählen Sie dann **Verwalten** im Bereich Benutzeraktivität. Wählen Sie den Tab **Benutzeraktivitätsagenten** und dann den Benutzeraktivitätsagenten aus, um Details dazu anzuzeigen, einschließlich Datensammler und Benutzerverzeichnis-Konnektoren.

Hinzufügen eines Datensammlers

Datensammler werden automatisch erstellt, wenn Sie eine Ransomware-Schutzstrategie mit Erkennung verdächtiger Benutzeraktivitäten aktivieren. Weitere Informationen finden Sie unter "Hinzufügen einer Erkennungsrichtlinie".

Sie können die Details des Datensammlers anzeigen. Wählen Sie in den Einstellungen in der Kachel „Benutzeraktivität“ die Option **Verwalten** aus. Wählen Sie die Registerkarte **Datensammler** und dann den Datensammler aus, um seine Details anzuzeigen oder ihn anzuhalten.



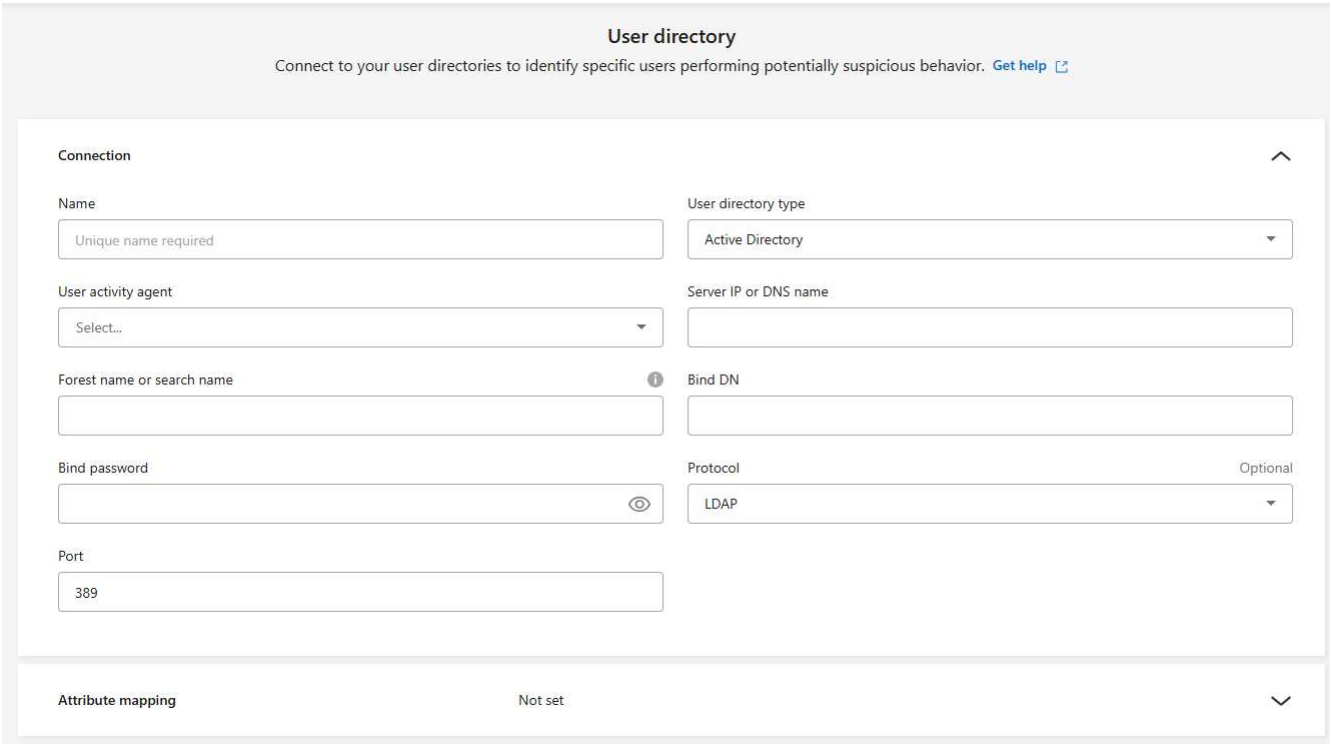
Erstellen Sie einen Benutzerverzeichnis-Connector

Um Benutzer-IDs Benutzernamen zuzuordnen, müssen Sie einen Benutzerverzeichnis-Connector erstellen.

Schritte

1. Gehen Sie in Ransomware Resilience zu **Einstellungen**.
2. Wählen Sie in der Kachel „Benutzeraktivität“ **Verwalten** aus.
3. Wählen Sie die Registerkarte **Benutzerverzeichnis-Konnektoren** und dann **Hinzufügen**.
4. Konfigurieren Sie die Verbindung. Geben Sie die erforderlichen Informationen für jedes Feld ein.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Benutzerverzeichnis-Connector ein.
Benutzerverzeichnistyp	Der Verzeichnistyp
Server-IP-Adresse oder Domänenname	Die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des Servers, der die Verbindung hostet
Waldname oder Suchname	Sie können die Gesamtstrukturebene der Verzeichnisstruktur als direkten Domänennamen angeben (zum Beispiel `unit.company.com`) oder eine Reihe relativer, angesehener Namen (zum Beispiel: `DC=unit,DC=company,DC=com`). Sie können auch einen Eintrag eingeben `OU` um nach einer Organisationseinheit oder einem `CN` auf einen bestimmten Benutzer beschränken (zum Beispiel: `CN=user,OU=engineering,DC=unit,DC=company,DC=com`).
BIND DN	Der BIND DN ist ein Benutzerkonto, das berechtigt ist, das Verzeichnis zu durchsuchen, z. B. user@domain.com. Der Benutzer benötigt die Berechtigung „Domänenlesbar“.
BIND-Passwort	Das Passwort für den in BIND DN angegebenen Benutzer.
Protokoll	Das Feld „Protokoll“ ist optional. Sie können LDAP, LDAPS oder LDAP over StartTLS verwenden.
Hafen	Geben Sie die von Ihnen gewählte Portnummer ein.



Geben Sie die Details zur Attributzuordnung an:

- **Anzeigename**
- **SID** (wenn Sie LDAP verwenden)
- **Benutzername**
- **Unix-ID** (wenn Sie NFS verwenden)
- Wenn Sie **Optionale Attribute einbeziehen** auswählen, können Sie auch eine E-Mail-Adresse, eine Telefonnummer, eine Rolle, ein Bundesland, ein Land, eine Abteilung, ein Foto, den Vorgesetzten-DN oder Gruppen hinzufügen. Wählen Sie **Erweitert**, um eine optionale Suchanfrage hinzuzufügen.

5. Wählen Sie **Hinzufügen**.
6. Kehren Sie zur Registerkarte „Benutzerverzeichnis-Konnektoren“ zurück, um den Status Ihres Benutzerverzeichnis-Konnektors zu überprüfen. Bei erfolgreicher Erstellung wird der Status des Benutzerverzeichnis-Connectors als **Wird ausgeführt** angezeigt.

Löschen eines Benutzerverzeichnis-Connectors

Schritte

1. Gehen Sie in Ransomware Resilience zu **Einstellungen**.
2. Suchen Sie die Kachel „Benutzeraktivität“ und wählen Sie **Verwalten** aus.
3. Wählen Sie die Registerkarte **Benutzerverzeichnis-Connector**.
4. Identifizieren Sie den Benutzerverzeichnis-Connector, den Sie löschen möchten. Wählen Sie im Aktionsmenü am Ende der Zeile die drei Punkte aus … dann **Löschen**.
5. Wählen Sie im Popup-Dialogfeld **Löschen** aus, um zu bestätigen.

Benutzer von Warnmeldungen ausschließen

Wenn es bestimmte vertrauenswürdige Benutzer gibt, deren Verhalten möglicherweise Warnmeldungen zum

Benutzerverhalten auslöst, können Sie sie von Warnmeldungen ausschließen.

Schritte

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Suchen Sie im Dashboard „Einstellungen“ die Karte „Benutzeraktivität“ und wählen Sie dann **Manage** aus.
3. Wählen Sie die Registerkarte **Excluded users** aus.
4. Um einzelne Benutzer in der Benutzeroberfläche zu überprüfen, wählen Sie **Manuell auswählen**. Um eine Liste ausgeschlossener Benutzer hochzuladen, wählen Sie **Hochladen**.

   a. Wenn Sie **Manuell auswählen** gewählt haben, aktivieren Sie das Kontrollkästchen neben den Namen der spezifischen Benutzer, die Sie ausschließen möchten.

   b. Wenn Sie **Hochladen** auswählen, laden Sie die CSV- oder JSON-Datei mit der Liste aller Benutzer herunter. Wählen Sie **Herunterladen**, um auf die Liste zuzugreifen.

      Überprüfen Sie die Datei auf Ihrem lokalen Rechner. Entfernen Sie die Namen aller Benutzer, für die Sie die Erkennung beibehalten möchten. Wenn die Liste nur noch die Namen der Benutzer enthält, die Sie von der Erkennung ausschließen möchten, speichern Sie sie.

   Wählen Sie in Ransomware Resilience **Hochladen** aus. Suchen Sie die Datei und laden Sie sie hoch.

5. Wählen Sie **Hinzufügen** aus, um das Hinzufügen der Benutzer zur Ausschlussliste abzuschließen.
6. Auf der Registerkarte **Ausgeschlossene Benutzer** werden nun die Namen der Benutzer angezeigt, die aus den Warnmeldungen zur Benutzerverhaltenserkennung entfernt wurden.

> Sie können einen Benutzer auch direkt von einer Benachrichtigung ausschließen. Weitere Informationen finden Sie unter "Auf Ransomware-Warnungen reagieren".

Benutzer aus der Liste der ausgeschlossenen Benutzer entfernen

Sie können einen Benutzer anschließend wieder zur Erkennung hinzufügen.

Schritte

1. Suchen Sie im Dashboard „Einstellungen“ die Karte „Benutzeraktivität“ und wählen Sie dann **Manage** aus.
2. Wählen Sie die Registerkarte **Excluded users** aus.
3. Wählen Sie **Hinzufügen**.
4. Um einzelne Benutzer von der UI auszuschließen, wählen Sie **Select manually**.
5. Suchen Sie den Namen des Benutzers, den Sie aus der Liste der ausgeschlossenen Benutzer entfernen möchten. Wählen Sie das Aktionsmenü (…) in der Zeile mit dem Benutzernamen und dann **Entfernen**.
6. Wählen Sie im Dialogfeld **Entfernen** aus, um zu bestätigen, dass Sie die ausgewählten Benutzer entfernen möchten.

Reagieren Sie auf Warnungen zu verdächtigen Benutzeraktivitäten

Nachdem Sie die Erkennung verdächtiger Benutzeraktivitäten konfiguriert haben, können Sie Ereignisse auf der Warnseite überwachen. Weitere Informationen finden Sie unter "Erkennen Sie bösartige Aktivitäten und verdächtiges Nutzerverhalten".

Schutzgruppen in NetApp Ransomware Resilience verwalten

NetApp Ransomware Resilience bietet Schutzgruppen zur einfacheren Verwaltung Ihrer Datenbestände. Schutzgruppen sind logische Gruppierungen von Workloads. Ransomware Resilience kann alle Volumes in einer Schutzgruppe gleichzeitig mit einer einzigen Datensicherungsstrategie schützen, sodass Sie keine Strategie für jeden Workload einzeln anwenden müssen.

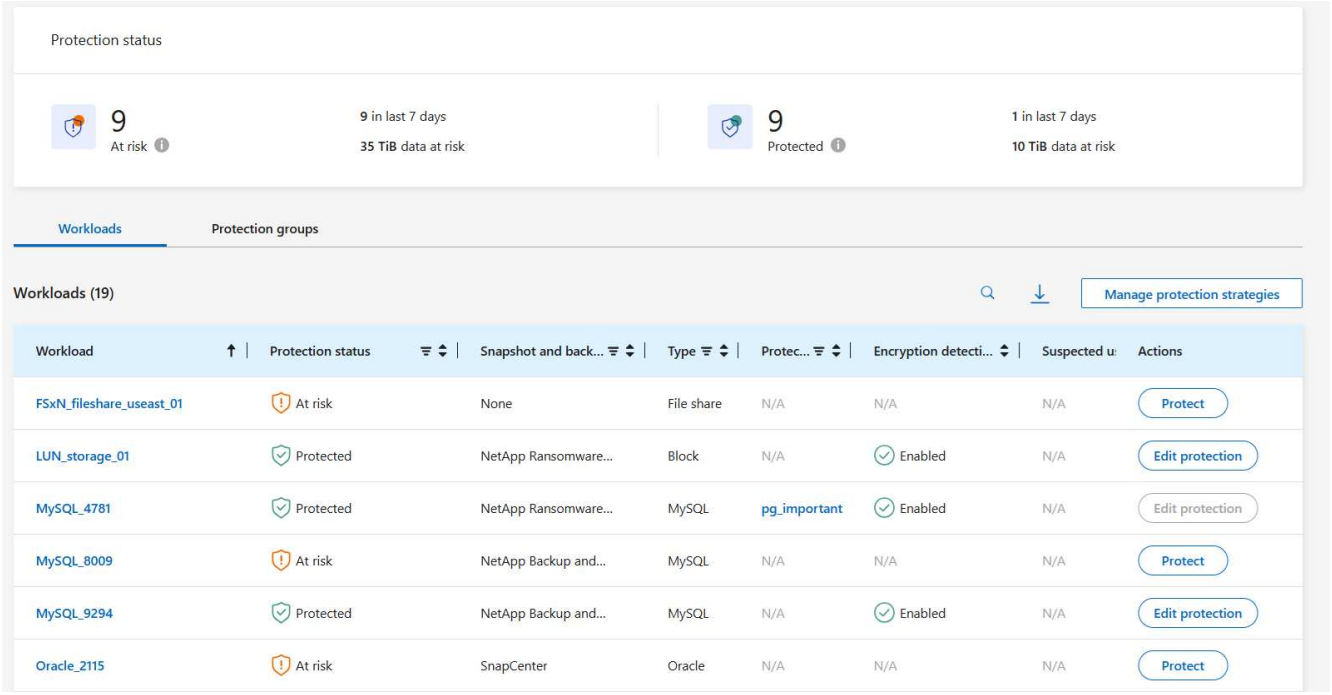
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Erstellen einer Schutzgruppe

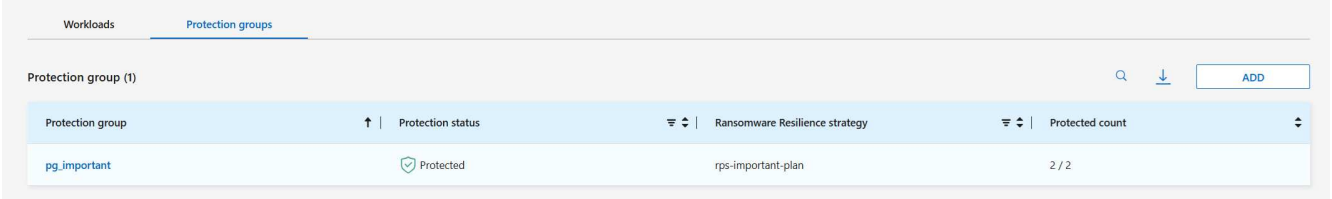
Sie können Gruppen unabhängig von ihrem Schutzstatus erstellen (d. h. Gruppen, die nicht geschützt sind, und Gruppen, die geschützt sind). Wenn Sie einer Schutzgruppe eine Datensicherungsstrategie hinzufügen, ersetzt die neue Datensicherungsstrategie alle vorhandenen Richtlinien, einschließlich der von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

Schritte

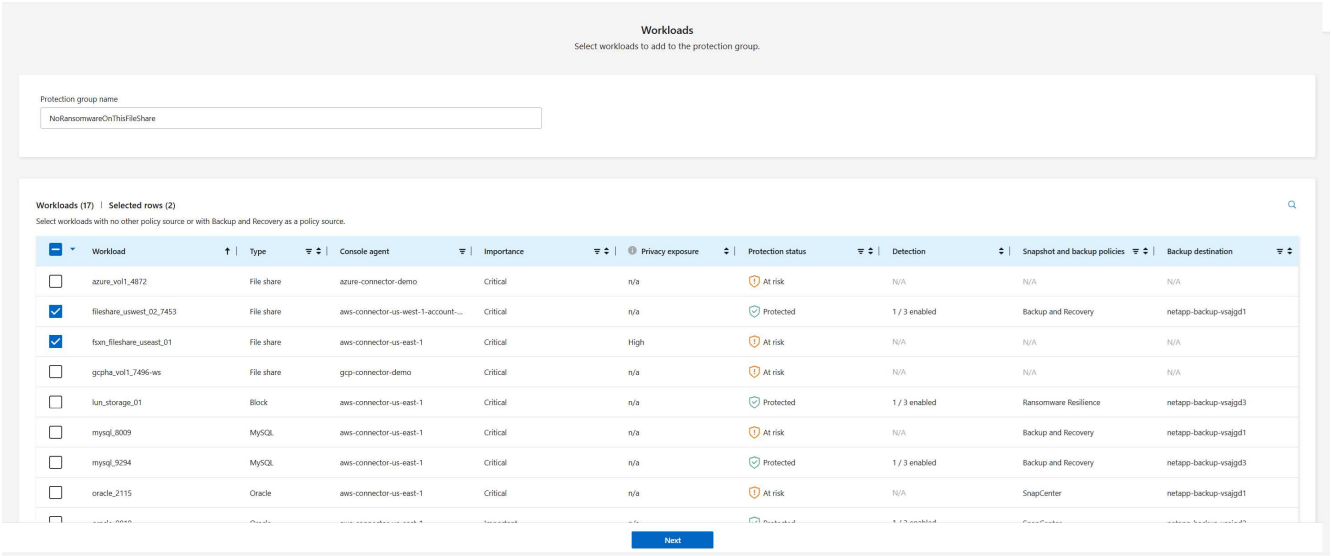
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



2. Wählen Sie im Protection-Dashboard die Registerkarte **Protection groups** aus.



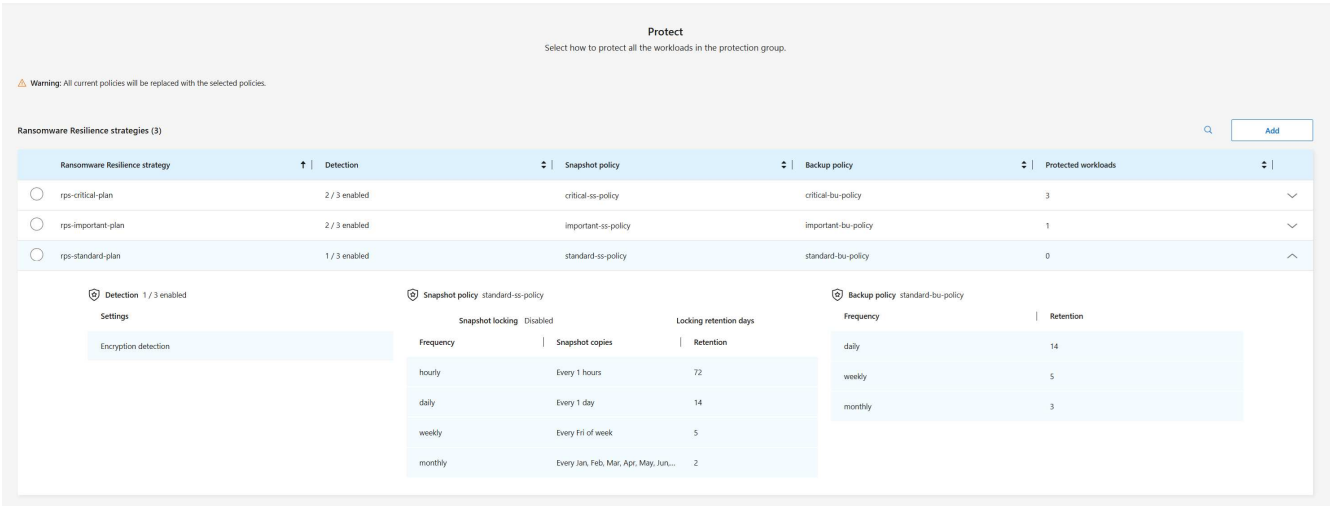
3. Wählen Sie **Hinzufügen**.



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 eine Datensicherungsstrategie für die Gruppe.
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 Schutzgruppe abzuschließen, wählen Sie **Add**.

Beim Überprüfen des Schutz-Dashboards in Ransomware Resilience können Sie Workloads nach Schutzgruppe sortieren.

Gruppenschutz bearbeiten

Sie können die Erkennungsrichtlinie für eine vorhandene Gruppe ändern.

Schritte

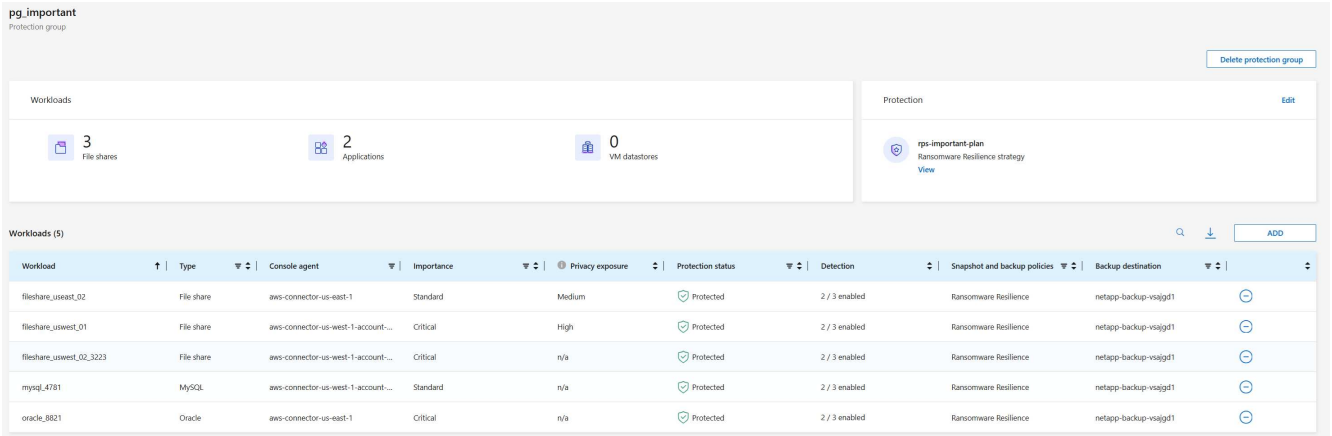
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.
2. Wählen Sie auf der Seite „Schutz“ die Registerkarte **Schutzgruppen** und dann die Gruppe aus, deren Richtlinie Sie ändern möchten.
3. Wählen Sie auf der Übersichtsseite der Schutzgruppe **Schutz bearbeiten** aus.
4. Wählen Sie eine vorhandene Datensicherungsstrategie aus, die Sie anwenden möchten, oder wählen Sie **Hinzufügen**, um eine neue Datensicherungsstrategie zu erstellen. Weitere Informationen zum Hinzufügen einer Datensicherungsstrategie finden Sie unter "Erstellen einer Schutzrichtlinie". Wählen Sie anschließend **Speichern** aus.
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.

Workloads aus einer Datensicherungsgruppe entfernen

Möglicherweise müssen Sie später Workloads aus einer bestehenden Datensicherungsgruppe 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 Schutzgruppe die Workload aus, die Sie aus der Gruppe entfernen möchten, und wählen Sie die Option **Aktionen** ⋯.
5. Wählen Sie im Menü „Aktionen“ die Option „Arbeitslast entfernen“ aus.

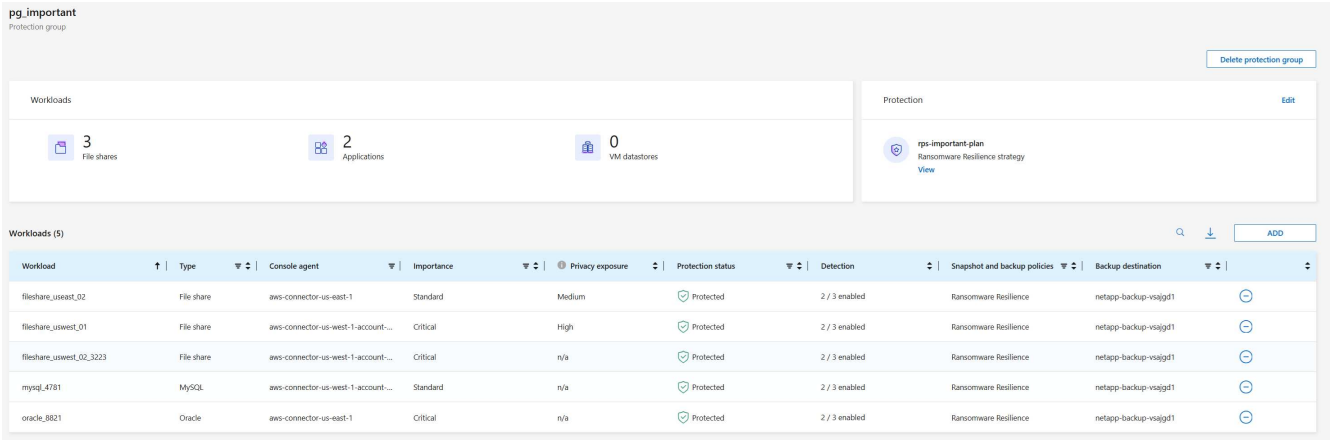
6. Bestätigen Sie, dass Sie die Arbeitslast entfernen möchten, und wählen Sie **Entfernen**.

Eine Schutzgruppe löschen

Wenn Sie eine Schutzgruppe löschen, entfernt Ransomware Resilience die Gruppe und die Datensicherungsstrategie von den Workloads. Es werden nicht die einzelnen Workloads gelöscht.

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**.

Identifizieren Sie Datenschutzlücken mit NetApp Ransomware Resilience

Innerhalb von NetApp Ransomware Resilience können Sie NetApp Data Classification verwenden, um die Daten in einer Dateifreigabe-Workload zu scannen und zu klassifizieren. Die Klassifizierung von Daten hilft Ihnen festzustellen, ob der Datensatz personenbezogene Daten (PII) enthält, was die Sicherheitsrisiken erhöhen kann.

"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.

Data Classification ist eine Kernkomponente der NetApp Console. Für die Nutzung von Data Classification ist keine Lizenz erforderlich. Je nach Ihrer Konfiguration können bei der Einrichtung von Data Classification Kosten anfallen, die jedoch nicht von Ransomware Resilience in Rechnung gestellt werden. Weitere Informationen finden Sie unter "Erfahren Sie mehr über die Datenklassifizierung".

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:

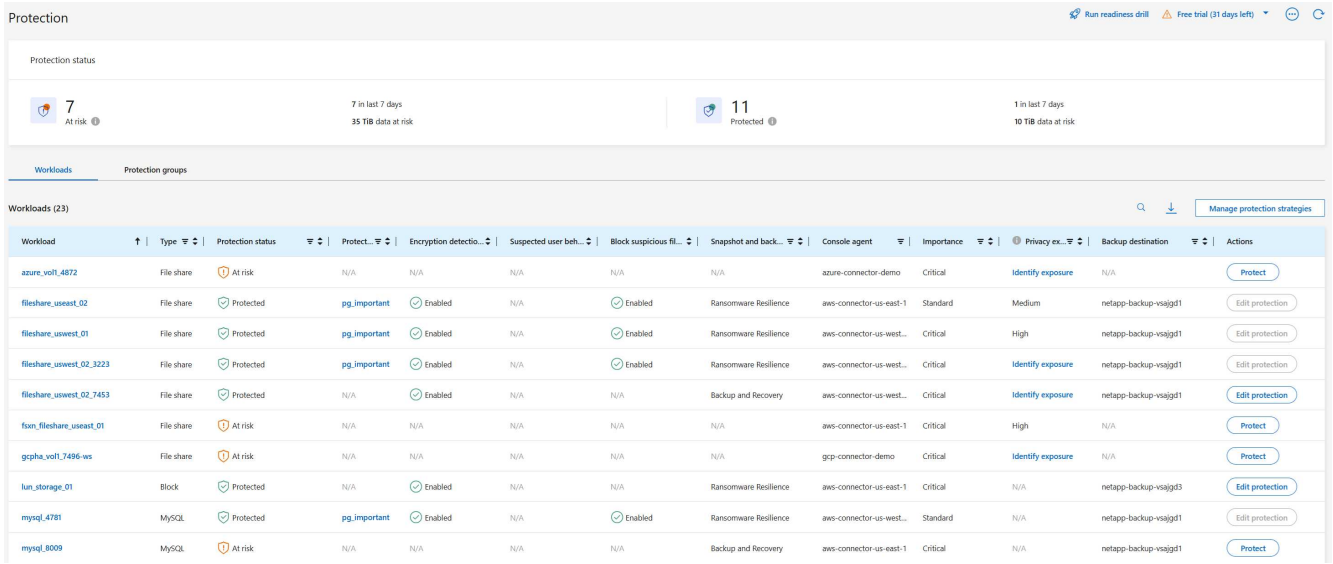
- "Erfahren Sie mehr über die Datenklassifizierung"
- "Kategorien personenbezogener Daten"
- "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten"

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

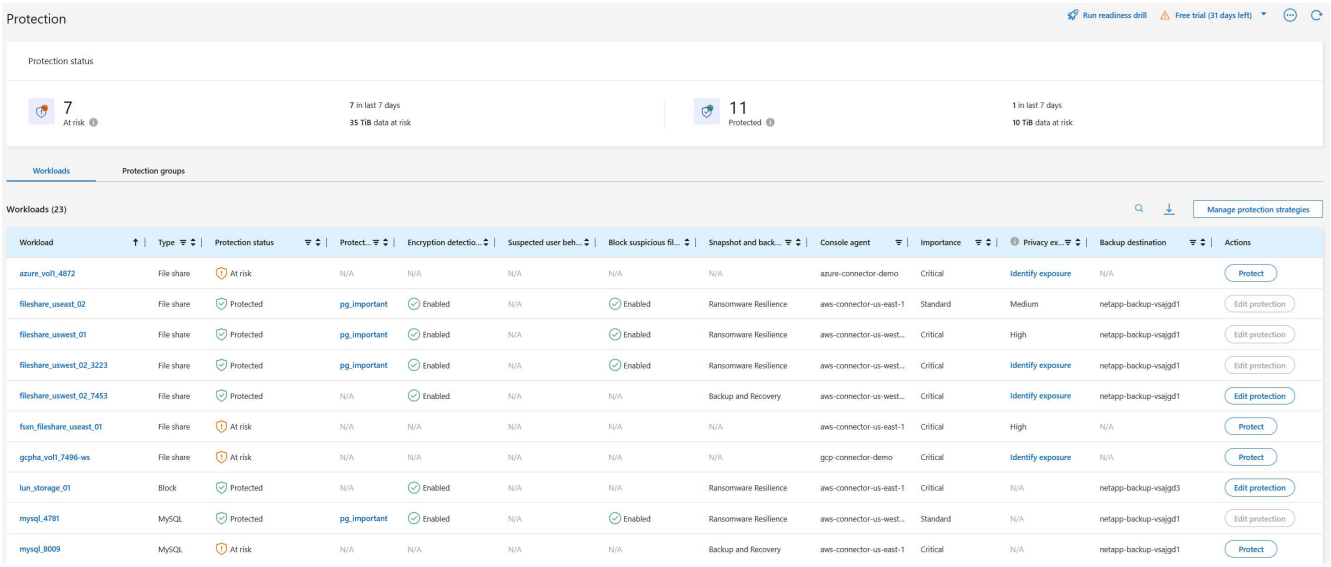
Bewerten Sie das Risiko, nachdem die Datenklassifizierung nach PII gesucht hat.

PII-Daten werden einer von drei Kategorien zugeordnet:

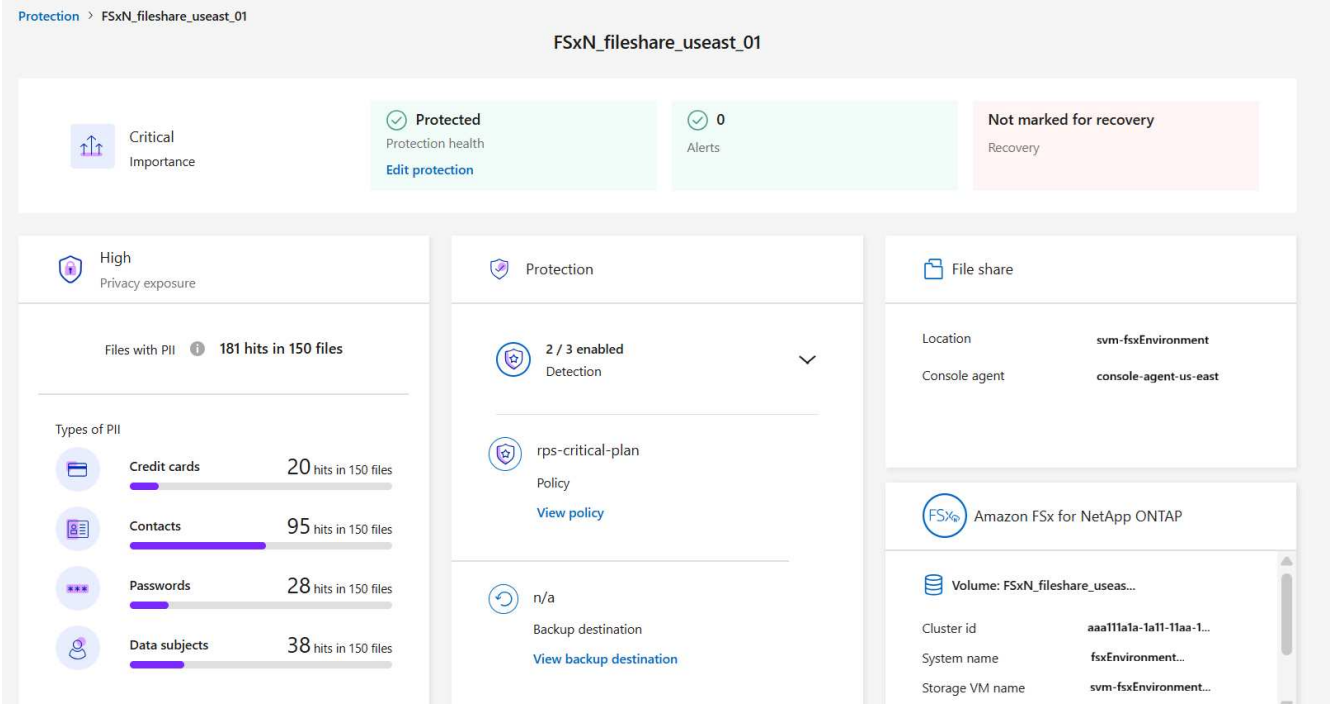
- **Hoch**: Mehr als 70 % der Dateien enthalten PII
- **Mittel**: Mehr als 30 % und weniger als 70 % der Dateien enthalten PII
- **Niedrig**: Mehr als 0 % und weniger als 30 % der Dateien enthalten PII

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"