NetApp Ransomware Resilience-Dokumentation

NetApp Ransomware Resilience

NetApp
October 10, 2025

Inhalt

NetApp Ransomware Resilience-Dokumentation

Versionshinweise

Was ist neu bei NetApp Ransomware Resilience?

Informieren Sie sich über die Neuerungen bei NetApp Ransomware Resilience.

06. Oktober 2025

BlueXP ransomware protection heißt jetzt NetApp Ransomware Resilience

Der BlueXP ransomware protection wurde in NetApp Ransomware Resilience umbenannt.

BlueXP heißt jetzt NetApp Console

Die NetApp Console ermöglicht eine zentrale Verwaltung von Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene und liefert Einblicke in Echtzeit, schnellere Workflows und eine vereinfachte Verwaltung.

Einzelheiten zu den Änderungen finden Sie im "Versionshinweise zur NetApp Konsole" .

Erkennung von Datenschutzverletzungen

Ransomware Resilience umfasst einen neuen Erkennungsmechanismus, der in wenigen Schritten aktiviert werden kann, um anomale Benutzerlesevorgänge als Frühindikator für einen Datenverstoß zu erkennen. Ransomware Resilience sammelt und analysiert Lesevorgänge von Benutzern, indem es eine historische Basislinie erstellt, die ein Profil des erwarteten, normalen Verhaltens auf Grundlage der vergangenen Daten darstellt. Wenn die Aktivität eines neuen Benutzers erheblich von dieser festgelegten Norm abweicht (z. B. ein unerwarteter Anstieg der Lesevorgänge in Kombination mit verdächtigen Lesemustern), wird eine Warnung generiert. Ransomware Resilience umfasst ein KI-Modell zum Erkennen verdächtiger Lesemuster.

Anders als bei der Verschlüsselungserkennung durch ARP auf Speicherebene erfolgt die Erkennung der Anomalie des Benutzerverhaltens im Ransomware Resilience SaaS-Dienst durch das Sammeln von FPolicy-Ereignissen.

Weitere Informationen finden Sie unter"Aktivieren Sie die Erkennung verdächtiger Benutzeraktivitäten" Und"Anzeigen von anomalem Benutzerverhalten" .

Weitere Erkennungen verdächtiger Benutzeraktivitäten

Zusätzlich zur Erkennung von Datenschutzverletzungen erkennt Ransomware Resilience auch die folgenden Warnmeldungstypen basierend auf beobachteten verdächtigen Benutzeraktivitäten:

- **Datenzerstörung – potenzieller Angriff** – Eine Warnung mit der Schwere eines potenziellen Angriffs wird erstellt, wenn die Anzahl der Dateilöschungen die historische Norm überschreitet.
- **Verdächtiges Benutzerverhalten – potenzieller Angriff** – Eine Warnung mit dem Schweregrad eines potenziellen Angriffs wird erstellt, wenn Lese-, Umbenennungs- und Löschvorgänge in einer Sequenz beobachtet werden, die einem Ransomware-Angriff ähnelt.
- **Verdächtiges Benutzerverhalten – Warnung** – Eine Warnung mit dem Schweregrad „Warnung“ wird erstellt, wenn die Gesamtzahl der Dateiaktivitäten (Lesen, Löschen, Umbenennen usw.) die historische Norm überschreitet

Neue Benutzerrolle zur Erkennung von Datenschutzverletzungen

Um Warnmeldungen zu verdächtigen Benutzeraktivitäten zu verwalten, hat Ransomware Resilience zwei neue Rollen eingeführt, um einen granularen Zugriff auf vertrauliche Daten wie die Dateiaktivität des Benutzers zu ermöglichen. Weitere Informationen finden Sie unter "Rollenbasierter Zugriff auf NetApp Ransomware Resilience" .

12. August 2025

Diese Version enthält allgemeine Erweiterungen und Verbesserungen.

15. Juli 2025

SAN-Workload-Unterstützung

Diese Version umfasst Unterstützung für SAN-Workloads im BlueXP ransomware protection. Sie können jetzt zusätzlich zu NFS- und CIFS-Workloads auch SAN-Workloads schützen.

Weitere Informationen finden Sie unter "Voraussetzungen für den BlueXP ransomware protection" .

Verbesserter Workload-Schutz

Diese Version verbessert den Konfigurationsprozess für Workloads mit Snapshot- und Backup-Richtlinien von anderen NetApp Tools wie SnapCenter oder BlueXP backup and recovery. In früheren Versionen erkannte der BlueXP ransomware protection die Richtlinien anderer Tools und ermöglichte Ihnen nur, die Erkennungsrichtlinie zu ändern. Mit dieser Version können Sie jetzt Snapshot- und Backup-Richtlinien durch BlueXP ransomware protection -Schutzrichtlinien ersetzen oder die Richtlinien anderer Tools weiterhin verwenden.

Weitere Einzelheiten finden Sie unter"Workloads schützen" .

E-Mail-Benachrichtigungen

Wenn der BlueXP ransomware protection einen möglichen Angriff erkennt, wird eine Benachrichtigung in den BlueXP Benachrichtigungen angezeigt und eine E-Mail an die von Ihnen konfigurierte E-Mail-Adresse gesendet.

Die E-Mail enthält Informationen zum Schweregrad, zur betroffenen Arbeitslast und einen Link zur Warnung auf der Registerkarte **Warnungen** des BlueXP ransomware protection .

Wenn Sie im BlueXP ransomware protection ein Sicherheits- und Ereignismanagementsystem (SIEM) konfiguriert haben, sendet der Dienst Warndetails an Ihr SIEM-System.

Weitere Einzelheiten finden Sie unter"Behandeln Sie erkannte Ransomware-Warnungen" .

9. Juni 2025

Aktualisierungen der Zielseite

Diese Version enthält Aktualisierungen der Zielseite für den BlueXP ransomware protection , die den Start der kostenlosen Testversion und die Entdeckung erleichtern.

Aktualisierungen der Bereitschaftsübung

Bisher konnten Sie eine Ransomware-Bereitschaftsübung durchführen, indem Sie einen Angriff auf eine neue Beispiel-Workload simulierten. Mit dieser Funktion können Sie den simulierten Angriff untersuchen und die Arbeitslast wiederherstellen. Verwenden Sie diese Funktion, um Warnbenachrichtigungen, Reaktionen und Wiederherstellungen zu testen. Führen Sie diese Übungen so oft wie nötig durch und planen Sie sie.

Mit dieser Version können Sie über eine neue Schaltfläche im BlueXP ransomware protection eine Ransomware-Bereitschaftsübung für eine Test-Workload ausführen. So können Sie Ransomware-Angriffe einfacher simulieren, ihre Auswirkungen untersuchen und Workloads effizient wiederherstellen – und das alles in einer kontrollierten Umgebung.

Sie können jetzt Bereitschaftsübungen zusätzlich zu NFS-Workloads auch für CIFS-Workloads (SMB) durchführen.

Weitere Einzelheiten finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Aktivieren Sie BlueXP classification Klassifizierungsaktualisierungen

Bevor Sie die BlueXP classification innerhalb des BlueXP ransomware protection verwenden, müssen Sie die BlueXP classification aktivieren, um Ihre Daten zu scannen. Durch die Klassifizierung von Daten können Sie personenbezogene Daten (PII) finden, die das Sicherheitsrisiko erhöhen können.

Sie können die BlueXP classification auf einer Dateifreigabe-Workload innerhalb des BlueXP ransomware protection bereitstellen. Wählen Sie in der Spalte **Datenschutzgefährdung** die Option **Gefährdung identifizieren**. Wenn Sie den Klassifizierungsdienst aktiviert haben, identifiziert diese Aktion die Gefährdung. Andernfalls wird mit dieser Version in einem Dialogfeld die Option zum Bereitstellen der BlueXP classification angezeigt. Wählen Sie **Bereitstellen**, um zur Zielseite des BlueXP classification zu gelangen, wo Sie diesen Dienst bereitstellen können. W

Weitere Einzelheiten finden Sie unter "Stellen Sie die BlueXP classification in der Cloud bereit" und um den Dienst innerhalb des BlueXP ransomware protection zu nutzen, beziehen Sie sich auf "Scannen Sie mit der BlueXP classification nach personenbezogenen Daten" .

13. Mai 2025

Meldung nicht unterstützter Arbeitsumgebungen im BlueXP ransomware protection

Während des Erkennungsworkflows meldet der BlueXP ransomware protection weitere Details, wenn Sie mit der Maus über „Unterstützte“ oder „Nicht unterstützte Workloads“ fahren. Dies wird Ihnen helfen zu verstehen, warum einige Ihrer Workloads vom BlueXP ransomware protection nicht erkannt werden.

Es gibt viele Gründe, warum der Dienst eine Arbeitsumgebung nicht unterstützt. Beispielsweise könnte die ONTAP Version in Ihrer Arbeitsumgebung niedriger sein als die erforderliche Version. Wenn Sie mit der Maus über eine nicht unterstützte Arbeitsumgebung fahren, wird in einem Tooltip der Grund angezeigt.

Sie können die nicht unterstützten Arbeitsumgebungen während der ersten Erkennung anzeigen und dort auch die Ergebnisse herunterladen. Sie können die Ergebnisse der Erkennung auch über die Option **Workload-Erkennung** auf der Seite „Einstellungen“ anzeigen.

Weitere Einzelheiten finden Sie unter "Entdecken Sie Workloads im BlueXP ransomware protection" .

29. April 2025

Unterstützung für Amazon FSx for NetApp ONTAP

Diese Version unterstützt Amazon FSx for NetApp ONTAP. Diese Funktion hilft Ihnen, Ihre FSx für ONTAP -Workloads mit BlueXP ransomware protection zu schützen.

FSx für ONTAP ist ein vollständig verwalteter Dienst, der die Leistung des NetApp ONTAP -Speichers in der Cloud bereitstellt. Es bietet dieselben Funktionen, dieselbe Leistung und dieselben Verwaltungsfunktionen, die Sie vor Ort verwenden, mit der Agilität und Skalierbarkeit eines nativen AWS-Dienstes.

Am BlueXP ransomware protection -Workflow wurden die folgenden Änderungen vorgenommen:

- Discovery umfasst Workloads in FSx für ONTAP 9.15-Arbeitsumgebungen.
- Auf der Registerkarte „Schutz“ werden Workloads in FSx für ONTAP -Umgebungen angezeigt. In dieser Umgebung sollten Sie Sicherungsvorgänge mit dem FSx for ONTAP -Sicherungsdienst durchführen. Sie können diese Workloads mithilfe von BlueXP ransomware protection -Snapshots wiederherstellen.

  Sicherungsrichtlinien für eine auf FSx für ONTAP ausgeführte Workload können in BlueXP nicht festgelegt werden. Alle vorhandenen Sicherungsrichtlinien, die in Amazon FSx for NetApp ONTAP festgelegt sind, bleiben unverändert.

- Warnmeldungen zeigen die neue FSx for ONTAP Arbeitsumgebung.

Weitere Einzelheiten finden Sie unter "Erfahren Sie mehr über den BlueXP ransomware protection" .

Informationen zu den unterstützten Optionen finden Sie im "Einschränkungen des BlueXP ransomware protection" .

BlueXP -Zugriffsrolle erforderlich

Sie benötigen jetzt eine der folgenden Zugriffsrollen, um den BlueXP ransomware protection anzuzeigen, zu erkennen oder zu verwalten: Organisationsadministrator, Ordner- oder Projektadministrator, Ransomware-Schutzadministrator oder Ransomware-Schutz-Viewer.

"Erfahren Sie mehr über BlueXP -Zugriffsrollen für alle Dienste" .

14. April 2025

Bereitschaftsübungsberichte

Mit dieser Version können Sie Übungsberichte zur Vorbereitung auf Ransomware-Angriffe überprüfen. Mithilfe einer Bereitschaftsübung können Sie einen Ransomware-Angriff auf eine neu erstellte Beispiel-Workload simulieren. Untersuchen Sie dann den simulierten Angriff und stellen Sie die Beispiel-Arbeitslast wieder her. Mithilfe dieser Funktion können Sie durch das Testen von Warnbenachrichtigungen, Reaktions- und Wiederherstellungsprozessen sicherstellen, dass Sie im Falle eines tatsächlichen Ransomware-Angriffs vorbereitet sind.

Weitere Einzelheiten finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Neue rollenbasierte Zugriffskontrollrollen und -berechtigungen

Bisher konnten Sie Benutzern basierend auf ihren Verantwortlichkeiten Rollen und Berechtigungen zuweisen, was Ihnen bei der Verwaltung des Benutzerzugriffs auf den BlueXP ransomware protection half. Mit dieser Version gibt es zwei neue Rollen speziell für den BlueXP ransomware protection mit aktualisierten Berechtigungen. Die neuen Rollen sind:

- Ransomware-Schutzadministrator
- Ransomware-Schutz-Viewer

Weitere Informationen zu Berechtigungen finden Sie unter "Rollenbasierter Zugriff auf Funktionen des BlueXP ransomware protection" .

Zahlungsverbesserungen

Diese Version enthält mehrere Verbesserungen des Zahlungsvorgangs.

Weitere Einzelheiten finden Sie unter "Einrichten von Lizenzierungs- und Zahlungsoptionen" .

10. März 2025

Simulieren Sie einen Angriff und reagieren Sie darauf

Simulieren Sie mit dieser Version einen Ransomware-Angriff, um Ihre Reaktion auf eine Ransomware-Warnung zu testen. Mithilfe dieser Funktion können Sie durch das Testen von Warnbenachrichtigungen, Reaktions- und Wiederherstellungsprozessen sicherstellen, dass Sie im Falle eines tatsächlichen Ransomware-Angriffs vorbereitet sind.

Weitere Einzelheiten finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Verbesserungen des Erkennungsprozesses

Diese Version enthält Verbesserungen der selektiven Erkennungs- und Neuerkennungsprozesse:

- Mit dieser Version können Sie neu erstellte Workloads entdecken, die den zuvor ausgewählten Arbeitsumgebungen hinzugefügt wurden.
- Sie können in dieser Version auch *neue* Arbeitsumgebungen auswählen. Mit dieser Funktion können Sie neue Workloads schützen, die Ihrer Umgebung hinzugefügt werden.
- Sie können diese Erkennungsprozesse während des Erkennungsprozesses zu Beginn oder innerhalb der Option „Einstellungen“ durchführen.

Weitere Einzelheiten finden Sie unter "Entdecken Sie neu erstellte Workloads für zuvor ausgewählte Arbeitsumgebungen" Und "Konfigurieren von Funktionen mit der Option „Einstellungen““ .

Warnungen werden ausgelöst, wenn eine hohe Verschlüsselung erkannt wird

Mit dieser Version können Sie Warnmeldungen anzeigen, wenn bei Ihren Workloads eine hohe Verschlüsselung erkannt wird, auch ohne dass es zu starken Änderungen der Dateierweiterungen kommt. Diese Funktion, die ONTAP Autonomous Ransomware Protection (ARP) AI verwendet, hilft Ihnen, Workloads zu identifizieren, die einem Risiko von Ransomware-Angriffen ausgesetzt sind. Verwenden Sie diese Funktion und laden Sie die gesamte Liste der betroffenen Dateien mit oder ohne Erweiterungsänderungen herunter.

Weitere Einzelheiten finden Sie unter "Reagieren Sie auf eine erkannte Ransomware-Warnung" .

16. Dezember 2024

Erkennen Sie anomales Benutzerverhalten mit Data Infrastructure Insights Storage Workload Security

Mit dieser Version können Sie Data Infrastructure Insights Storage Workload Security verwenden, um anomales Benutzerverhalten in Ihren Speicher-Workloads zu erkennen. Diese Funktion hilft Ihnen, potenzielle Sicherheitsbedrohungen zu erkennen und potenziell böswillige Benutzer zu blockieren, um Ihre Daten zu schützen.

Weitere Einzelheiten finden Sie unter "Reagieren Sie auf eine erkannte Ransomware-Warnung" .

Bevor Sie Data Infrastructure Insights Storage Workload Security zum Erkennen anomalen Benutzerverhaltens verwenden, müssen Sie die Option mithilfe der Option **Einstellungen** des BlueXP ransomware protection konfigurieren.

Siehe "Konfigurieren Sie die BlueXP ransomware protection -Schutzeinstellungen" .

Auswählen von Workloads zum Erkennen und Schützen

Mit dieser Version können Sie jetzt Folgendes tun:

- Wählen Sie in jedem Connector die Arbeitsumgebungen aus, in denen Sie Workloads ermitteln möchten. Sie können von dieser Funktion profitieren, wenn Sie bestimmte Workloads in Ihrer Umgebung schützen möchten und andere nicht.
- Während der Workload-Erkennung können Sie die automatische Erkennung von Workloads pro Connector aktivieren. Mit dieser Funktion können Sie die Workloads auswählen, die Sie schützen möchten.
- Entdecken Sie neu erstellte Workloads für zuvor ausgewählte Arbeitsumgebungen.

Siehe "Workloads ermitteln" .

7. November 2024

Aktivieren Sie die Datenklassifizierung und suchen Sie nach personenbezogenen Daten (PII).

Mit dieser Version können Sie die BlueXP classification, eine Kernkomponente der BlueXP Familie, aktivieren, um Daten in Ihren Dateifreigabe-Workloads zu scannen und zu klassifizieren. Durch die Klassifizierung von Daten können Sie feststellen, ob Ihre Daten persönliche oder private Informationen enthalten, die das Sicherheitsrisiko erhöhen können. Dieser Prozess wirkt sich auch auf die Wichtigkeit der Arbeitslast aus und hilft Ihnen sicherzustellen, dass Sie die Arbeitslasten mit dem richtigen Schutzniveau schützen.

Das Scannen nach PII-Daten im BlueXP ransomware protection ist im Allgemeinen für Kunden verfügbar, die die BlueXP classification eingesetzt haben. Die BlueXP classification ist als Teil der BlueXP Plattform ohne zusätzliche Kosten verfügbar und kann vor Ort oder in der Kunden-Cloud bereitgestellt werden.

Siehe "Konfigurieren Sie die BlueXP ransomware protection -Schutzeinstellungen" .

Um den Scanvorgang zu starten, klicken Sie auf der Seite „Schutz“ in der Spalte „Datenschutzgefährdung“ auf **Gefährdung identifizieren**.

"Scannen Sie mit der BlueXP classification nach personenbezogenen sensiblen Daten" .

SIEM-Integration mit Microsoft Sentinel

Sie können jetzt mithilfe von Microsoft Sentinel Daten zur Bedrohungsanalyse und -erkennung an Ihr Sicherheits- und Ereignismanagementsystem (SIEM) senden. Bisher konnten Sie den AWS Security Hub oder Splunk Cloud als Ihr SIEM auswählen.

"Erfahren Sie mehr über die Konfiguration der BlueXP ransomware protection -Schutzeinstellungen" .

Jetzt 30 Tage kostenlos testen

Mit dieser Version können neue Bereitstellungen des BlueXP ransomware protection jetzt 30 Tage lang kostenlos getestet werden. Zuvor war der BlueXP ransomware protection 90 Tage lang als kostenlose Testversion verfügbar. Wenn Sie bereits an der 90-tägigen kostenlosen Testversion teilnehmen, gilt dieses Angebot für die nächsten 90 Tage.

Wiederherstellen der Anwendungsarbeitslast auf Dateiebene für Podman

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie jetzt eine Liste der Dateien anzeigen, die möglicherweise von einem Angriff betroffen waren, und diejenigen identifizieren, die Sie wiederherstellen möchten. Wenn die BlueXP Konnektoren in einer Organisation (früher ein Konto) Podman verwendeten, war diese Funktion zuvor deaktiviert. Es ist jetzt für Podman aktiviert. Sie können die wiederherzustellenden Dateien vom BlueXP ransomware protection auswählen lassen, eine CSV-Datei hochladen, in der alle von einer Warnung betroffenen Dateien aufgelistet sind, oder manuell angeben, welche Dateien Sie wiederherstellen möchten.

"Erfahren Sie mehr über die Wiederherstellung nach einem Ransomware-Angriff" .

30. September 2024

Benutzerdefinierte Gruppierung von Dateifreigabe-Workloads

Mit dieser Version können Sie jetzt Dateifreigaben in Gruppen zusammenfassen, um Ihren Datenbestand einfacher zu schützen. Der Dienst kann alle Volumes einer Gruppe gleichzeitig schützen. Bisher mussten Sie jedes Volume separat schützen.

"Erfahren Sie mehr über die Gruppierung von Dateifreigabe-Workloads in Ransomware-Schutzstrategien" .

2. September 2024

Sicherheitsrisikobewertung von Digital Advisor

Der BlueXP ransomware protection sammelt jetzt Informationen über hohe und kritische Sicherheitsrisiken im Zusammenhang mit einem Cluster von NetApp Digital Advisor. Wenn ein Risiko erkannt wird, gibt der BlueXP ransomware protection im Bereich **Empfohlene Aktionen** des Dashboards eine Empfehlung aus: „Beheben Sie eine bekannte Sicherheitslücke im Cluster <Name>.“ Wenn Sie in der Empfehlung auf dem Dashboard auf **Überprüfen und beheben** klicken, wird vorgeschlagen, Digital Advisor und einen CVE-Artikel (Common Vulnerability & Exposure) zu überprüfen, um das Sicherheitsrisiko zu beheben. Wenn mehrere Sicherheitsrisiken bestehen, überprüfen Sie die Informationen im Digital Advisor.

Siehe "Digital Advisor -Dokumentation" .

Sichern Sie auf der Google Cloud Platform

Mit dieser Version können Sie als Sicherungsziel einen Bucket der Google Cloud Platform festlegen. Bisher

konnten Sie Sicherungsziele nur zu NetApp StorageGRID, Amazon Web Services und Microsoft Azure hinzufügen.

"Erfahren Sie mehr über die Konfiguration der BlueXP ransomware protection -Schutzeinstellungen" .

Unterstützung für Google Cloud Platform

Der Dienst unterstützt jetzt Cloud Volumes ONTAP für Google Cloud Platform zum Speicherschutz. Zuvor unterstützte der Dienst nur Cloud Volumes ONTAP für Amazon Web Services und Microsoft Azure sowie lokales NAS.

"Erfahren Sie mehr über den BlueXP ransomware protection und die unterstützten Datenquellen, Sicherungsziele und Arbeitsumgebungen" .

Rollenbasierte Zugriffskontrolle

Sie können jetzt den Zugriff auf bestimmte Aktivitäten mit der rollenbasierten Zugriffskontrolle (RBAC) beschränken. Der BlueXP ransomware protection verwendet zwei Rollen von BlueXP: BlueXP Kontoadministrator und Nicht-Kontoadministrator (Viewer).

Einzelheiten zu den Aktionen, die jede Rolle ausführen kann, finden Sie unter "Rollenbasierte Zugriffskontrollberechtigungen" .

5. August 2024

Bedrohungserkennung mit Splunk Cloud

Sie können Daten zur Bedrohungsanalyse und -erkennung automatisch an Ihr Sicherheits- und Ereignismanagementsystem (SIEM) senden. Bei früheren Versionen konnten Sie nur den AWS Security Hub als Ihr SIEM auswählen. Mit dieser Version können Sie den AWS Security Hub oder Splunk Cloud als Ihr SIEM auswählen.

"Erfahren Sie mehr über die Konfiguration der BlueXP ransomware protection -Schutzeinstellungen" .

1. Juli 2024

Bringen Sie Ihre eigene Lizenz mit (BYOL)

Mit dieser Version können Sie eine BYOL-Lizenz verwenden, bei der es sich um eine NetApp -Lizenzdatei (NLF) handelt, die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten.

"Weitere Informationen zum Einrichten der Lizenzierung" .

Wiederherstellen der Anwendungsarbeitslast auf Dateiebene

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie jetzt eine Liste der Dateien anzeigen, die möglicherweise von einem Angriff betroffen waren, und diejenigen identifizieren, die Sie wiederherstellen möchten. Sie können die wiederherzustellenden Dateien vom BlueXP ransomware protection auswählen lassen, eine CSV-Datei hochladen, in der alle von einer Warnung betroffenen Dateien aufgelistet sind, oder manuell angeben, welche Dateien Sie wiederherstellen möchten.

Wenn mit dieser Version nicht alle BlueXP Konnektoren in einem Konto Podman verwenden, ist die Funktion zur Wiederherstellung einzelner Dateien aktiviert. Andernfalls ist es für dieses Konto deaktiviert.

"Erfahren Sie mehr über die Wiederherstellung nach einem Ransomware-Angriff" .

Laden Sie eine Liste der betroffenen Dateien herunter

Bevor Sie eine Anwendungsarbeitslast auf Dateiebene wiederherstellen, können Sie jetzt auf die Seite „Warnungen“ zugreifen, um eine Liste der betroffenen Dateien in einer CSV-Datei herunterzuladen und dann die CSV-Datei über die Seite „Wiederherstellung“ hochzuladen.

"Erfahren Sie mehr über das Herunterladen betroffener Dateien vor der Wiederherstellung einer Anwendung" .

Schutzplan löschen

Mit dieser Version können Sie jetzt eine Ransomware-Schutzstrategie löschen.

"Erfahren Sie mehr über den Schutz von Workloads und die Verwaltung von Ransomware-Schutzstrategien" .

10. Juni 2024

Sperren von Snapshot-Kopien auf dem Primärspeicher

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.

"Erfahren Sie mehr über den Schutz von Workloads und die Aktivierung der Backup-Sperre in einer Ransomware-Schutzstrategie" .

Unterstützung für Cloud Volumes ONTAP für Microsoft Azure

Diese Version unterstützt Cloud Volumes ONTAP für Microsoft Azure als System zusätzlich zu Cloud Volumes ONTAP für AWS und lokalem ONTAP NAS.

"Schnellstart für Cloud Volumes ONTAP in Azure"

"Erfahren Sie mehr über den BlueXP ransomware protection" .

Microsoft Azure als Backup-Ziel hinzugefügt

Sie können jetzt Microsoft Azure zusammen mit AWS und NetApp StorageGRID als Sicherungsziel hinzufügen.

"Erfahren Sie mehr über die Konfiguration von Schutzeinstellungen" .

14. Mai 2024

Lizenzierungsupdates

Sie können sich für eine 90-tägige kostenlose Testversion anmelden. In Kürze können Sie ein Pay-as-you-go-Abonnement beim Amazon Web Services Marketplace erwerben oder Ihre eigene NetApp -Lizenz mitbringen.

"Weitere Informationen zum Einrichten der Lizenzierung" .

CIFS-Protokoll

Der Dienst unterstützt jetzt lokales ONTAP und Cloud Volumes ONTAP in AWS-Systemen unter Verwendung der Protokolle NFS und CIFS. Die vorherige Version unterstützte nur das NFS-Protokoll.

Details zur Arbeitslast

Diese Version bietet jetzt mehr Details in den Workload-Informationen vom Schutz und anderen Seiten für eine verbesserte Bewertung des Workload-Schutzes. Anhand der Workload-Details können Sie die aktuell zugewiesene Richtlinie und die konfigurierten Sicherungsziele überprüfen.

"Erfahren Sie mehr über das Anzeigen von Workloaddetails auf den Schutzseiten" .

Anwendungskonsistenter und VM-konsistenter Schutz und Wiederherstellung

Sie können jetzt anwendungskonsistenten Schutz mit der NetApp SnapCenter -Software und VM-konsistenten Schutz mit dem SnapCenter Plug-in for VMware vSphere durchführen und so einen ruhigen und konsistenten Zustand erreichen, um einen möglichen späteren Datenverlust zu vermeiden, falls eine Wiederherstellung erforderlich ist. Wenn eine Wiederherstellung erforderlich ist, können Sie die Anwendung oder VM in einen der zuvor verfügbaren Zustände zurückversetzen.

"Erfahren Sie mehr über den Schutz von Workloads" .

Strategien zum Schutz vor Ransomware

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

- Snapshot-Richtlinie
- Sicherungsrichtlinie
- Erkennungsrichtlinie

"Erfahren Sie mehr über den Schutz von Workloads" .

Bedrohungserkennung

Die Bedrohungserkennung ist jetzt über ein SIEM-System (Security and Event Management) eines Drittanbieters verfügbar. Das Dashboard zeigt jetzt eine neue Empfehlung zum Aktivieren der Bedrohungserkennung an, die auf der Seite „Einstellungen“ konfiguriert werden kann.

"Erfahren Sie mehr über das Konfigurieren von Einstellungsoptionen" .

Falsche positive Warnungen verwerfen

Auf der Registerkarte „Warnungen“ können Sie jetzt Fehlalarme verwerfen oder sich für eine sofortige Wiederherstellung Ihrer Daten entscheiden.

"Erfahren Sie mehr über die Reaktion auf eine Ransomware-Warnung" .

Erkennungsstatus

Auf der Seite „Schutz“ werden neue Erkennungsstatus angezeigt, die den Status der auf die Arbeitslast angewendeten Ransomware-Erkennung zeigen.

"Erfahren Sie mehr über den Schutz von Workloads und die Anzeige des Schutzstatus" .

CSV-Dateien herunterladen

Sie können CSV-Dateien* von den Seiten „Schutz“, „Warnungen“ und „Wiederherstellung“ herunterladen.

"Erfahren Sie mehr über das Herunterladen von CSV-Dateien vom Dashboard und anderen Seiten" .

Dokumentationslink

Der Link „Dokumentation anzeigen“ ist jetzt in der Benutzeroberfläche enthalten. Sie können auf diese Dokumentation über die Dashboard-Vertikale **Aktionen** zugreifen.  Option. Wählen Sie **Was ist neu**, um Details in den Versionshinweisen anzuzeigen, oder **Dokumentation**, um die Homepage der Dokumentation zum BlueXP ransomware protection anzuzeigen.

BlueXP backup and recovery

Der BlueXP backup and recovery muss auf dem System nicht mehr aktiviert sein. Sehen "Voraussetzungen" . Der BlueXP ransomware protection hilft bei der Konfiguration eines Sicherungsziels über die Option „Einstellungen“. Sehen "Konfigurieren der Einstellungen" .

Einstellungsoption

Sie können jetzt Sicherungsziele in den Einstellungen des BlueXP ransomware protection einrichten.

"Erfahren Sie mehr über das Konfigurieren von Einstellungsoptionen" .

5. März 2024

Schutzrichtlinienverwaltung

Zusätzlich zur Verwendung vordefinierter Richtlinien können Sie jetzt Richtlinien erstellen. "Weitere Informationen zum Verwalten von Richtlinien" .

Unveränderlichkeit auf sekundärem Speicher (DataLock)

Sie können das Backup jetzt mithilfe der NetApp DataLock-Technologie im Objektspeicher im Sekundärspeicher unveränderlich machen. "Weitere Informationen zum Erstellen von Schutzrichtlinien" .

Automatisches Backup auf NetApp StorageGRID

Zusätzlich zur Verwendung von AWS können Sie jetzt StorageGRID als Ihr Sicherungsziel auswählen. "Erfahren Sie mehr über die Konfiguration von Sicherungszielen" .

Zusätzliche Funktionen zur Untersuchung potenzieller Angriffe

Sie können jetzt weitere forensische Details anzeigen, um den erkannten potenziellen Angriff zu untersuchen. "Erfahren Sie mehr über die Reaktion auf eine Ransomware-Warnung" .

Wiederherstellungsprozess

Der Wiederherstellungsprozess wurde verbessert. Jetzt können Sie Volume für Volume oder alle Volumes für eine Arbeitslast wiederherstellen. "Erfahren Sie mehr über die Wiederherstellung nach einem Ransomware-

Angriff (nachdem Vorfälle neutralisiert wurden)" .

"Erfahren Sie mehr über den BlueXP ransomware protection" .

6. Oktober 2023

Der BlueXP ransomware protection ist eine SaaS-Lösung zum Schutz von Daten, zur Erkennung potenzieller Angriffe und zur Wiederherstellung von Daten nach einem Ransomware-Angriff.

In der Vorschauversion schützt der Dienst anwendungsbasierte Workloads von Oracle, MySQL, VM-Datenspeichern und Dateifreigaben auf lokalem NAS-Speicher sowie Cloud Volumes ONTAP auf AWS (unter Verwendung des NFS-Protokolls) in BlueXP -Organisationen einzeln und sichert Daten im Cloud-Speicher von Amazon Web Services.

Der BlueXP ransomware protection bietet die volle Nutzung mehrerer NetApp -Technologien, sodass Ihr Datensicherheitsadministrator oder Sicherheitsbetriebsingenieur die folgenden Ziele erreichen kann:

- Sehen Sie sich auf einen Blick den Ransomware-Schutz für alle Ihre Workloads an.
- Erhalten Sie Einblicke in Empfehlungen zum Schutz vor Ransomware
- Verbessern Sie Ihre Schutzlage basierend auf den Empfehlungen von BlueXP ransomware protection .
- Weisen Sie Ransomware-Schutzrichtlinien zu, um Ihre wichtigsten Workloads und Hochrisikodaten vor Ransomware-Angriffen zu schützen.
- Überwachen Sie den Zustand Ihrer Workloads und schützen Sie sie vor Ransomware-Angriffen, indem Sie nach Datenanomalien suchen.
- Bewerten Sie schnell die Auswirkungen von Ransomware-Vorfällen auf Ihre Arbeitslast.
- Erholen Sie sich intelligent von Ransomware-Vorfällen, indem Sie Daten wiederherstellen und sicherstellen, dass keine erneute Infektion von gespeicherten Daten aus erfolgt.

"Erfahren Sie mehr über den BlueXP ransomware protection" .

Bekannte Einschränkungen der NetApp Ransomware Resilience

Bekannte Einschränkungen kennzeichnen Plattformen, Geräte oder Funktionen, die von dieser Produktversion nicht unterstützt werden oder nicht ordnungsgemäß mit ihr zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Problem mit der Reset-Option für die Bereitschaftsübung

Wenn Sie für die Übung zur Vorbereitung auf Ransomware-Angriffe ein ONTAP 9.11.1-Volume auswählen, sendet Ransomware Resilience eine Warnung. Wenn Sie die Daten mit der Option „Auf Volume klonen“ wiederherstellen und den Drill zurücksetzen, schlägt der Rücksetzvorgang fehl.

Einschränkungen von Amazon FSx for NetApp ONTAP

Das Amazon FSx for NetApp ONTAP -System wird in Ransomware Resilience unterstützt. Für dieses System gelten die folgenden Einschränkungen:

- Sicherungsrichtlinien werden für Fsx for ONTAP nicht unterstützt. In dieser Umgebung sollten Sie Sicherungsvorgänge mit Amazon FSx für Sicherungen durchführen. Sie können diese Workloads mithilfe

von Ransomware Resilience wiederherstellen.

- Wiederherstellungsvorgänge werden nur von Snapshots aus durchgeführt.

Erste Schritte

Erfahren Sie mehr über NetApp Ransomware Resilience

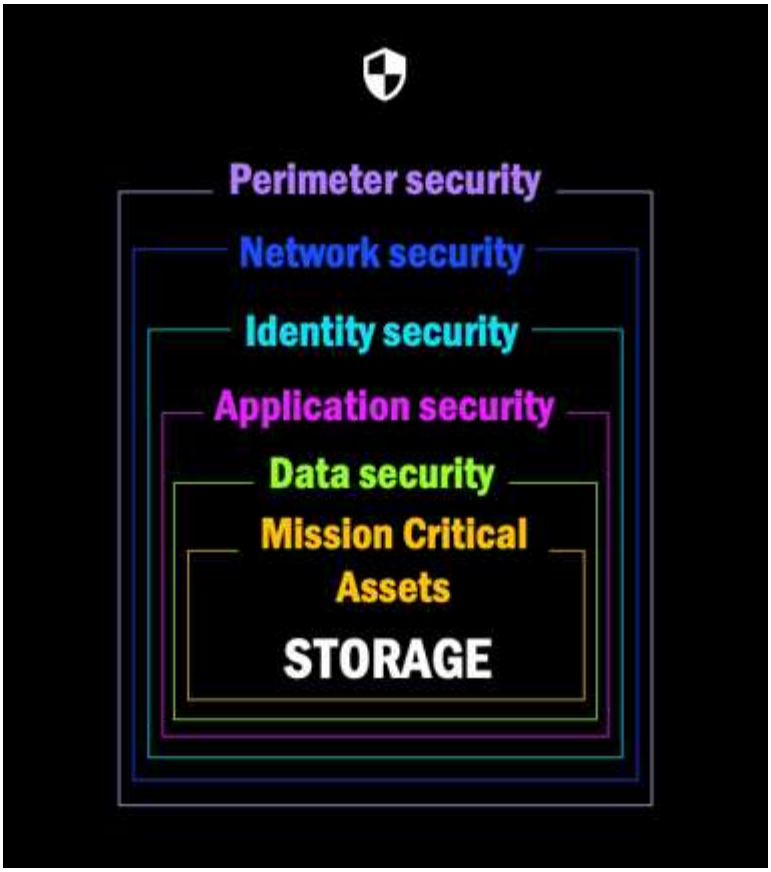
Ransomware-Angriffe können den Zugriff auf Ihre Daten blockieren und Angreifer können Lösegeld im Austausch für die Freigabe der Daten oder die Entschlüsselung verlangen. Laut IDC ist es nicht ungewöhnlich, dass Opfer von Ransomware mehreren Ransomware-Angriffen ausgesetzt sind. Der Angriff kann den Zugriff auf Ihre Daten für einen Tag bis zu mehreren Wochen unterbrechen.

NetApp Ransomware Resilience schützt Ihre Daten vor Ransomware-Angriffen. In Ransomware Resilience ist Schutz für anwendungsbasierte Workloads von Oracle, MySQL, VM-Datenspeichern und Dateifreigaben auf lokalem NAS-Speicher (unter Verwendung der Protokolle NFS und CIFS) und SAN-Speicher (FC, iSCSI und NVMe) sowie Cloud Volumes ONTAP für Amazon Web Services, Cloud Volumes ONTAP für Google Cloud, Cloud Volumes ONTAP für Microsoft Azure und Amazon FSx for NetApp ONTAP über die NetApp Console verfügbar. Sie können Daten auf Amazon Web Services, Google Cloud, Microsoft Azure Cloud Storage und NetApp StorageGRID sichern.

Ransomware-Resilienz auf Datenebene

Ihre Sicherheitslage umfasst in der Regel mehrere Verteidigungsebenen zum Schutz vor einer Reihe von Cyberbedrohungen.

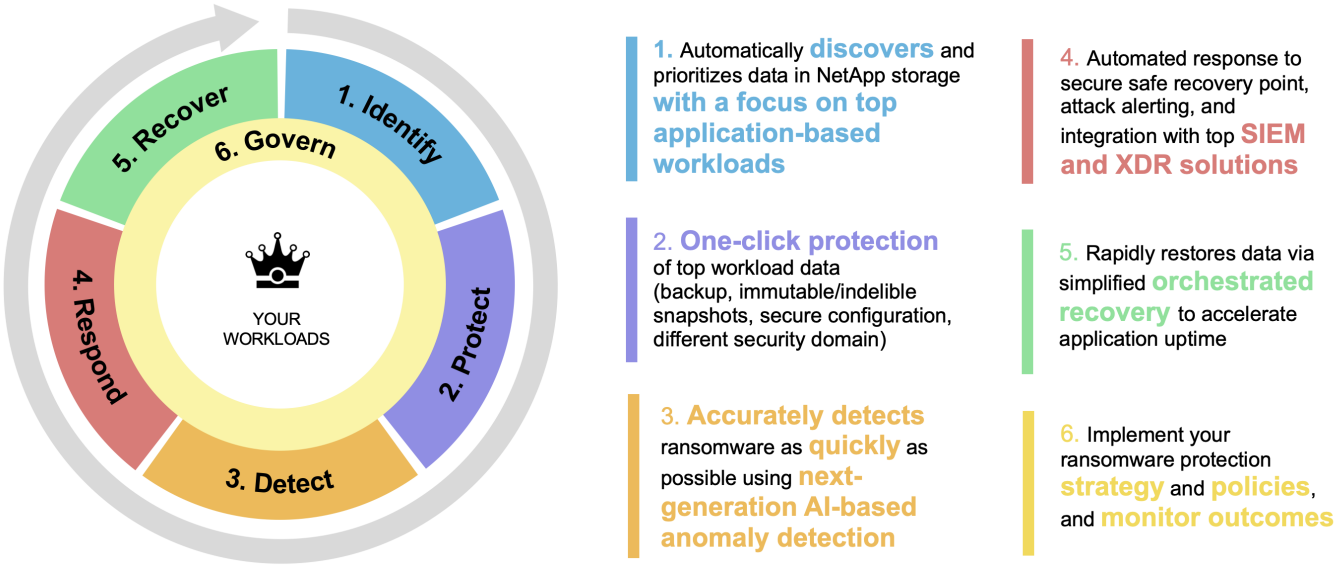
- **Äußerste Schicht**: Dies ist Ihre erste Verteidigungslinie, die Firewalls, Intrusion Detection Systems und virtuelle private Netzwerke zum Schutz der Netzwerkgrenzen verwendet.
- **Netzwerksicherheit**: Diese Ebene baut auf der Grundlage von Netzwerksegmentierung, Verkehrsüberwachung und Verschlüsselung auf.
- **Identitätssicherheit**: Verwendet Authentifizierungsmethoden, Zugriffskontrollen und Identitätsmanagement, um sicherzustellen, dass nur autorisierte Benutzer auf vertrauliche Ressourcen zugreifen können.
- **Anwendungssicherheit**: Schützt Softwareanwendungen durch sichere Codierungspraktiken, Sicherheitstests und Selbstschutz der Laufzeitanwendung.
- **Datensicherheit**: Schützt Ihre Daten mit Datenschutz-, Backup- und Wiederherstellungsstrategien. Ransomware Resilience arbeitet auf dieser Ebene.



Was Sie mit Ransomware Resilience tun können

Ransomware Resilience ermöglicht die vollständige Nutzung mehrerer NetApp -Technologien, sodass Ihr Speicheradministrator, Datensicherheitsadministrator oder Sicherheitsbetriebsingenieur die folgenden Ziele erreichen kann:

- **Identifizieren** Sie alle anwendungsbasierten, File-Share- oder VMware-verwalteten Workloads in lokalen NetApp -NAS- (NFS oder CIFS) und SAN-Systemen (FC, iSCSI und NVMe) über die NetApp Konsole, Projekte und Konsolenagenten hinweg. Ransomware Resilience kategorisiert die Datenpriorität und gibt Ihnen Empfehlungen zur Verbesserung der Ransomware-Resilienz.
- **Schützen** Sie Ihre Workloads, indem Sie Backups, Snapshot-Kopien und Ransomware-Schutzstrategien für Ihre Daten aktivieren.
- **Erkennen** Sie Anomalien, bei denen es sich um Ransomware-Angriffe handeln könnte. Fußnote: [Auch wenn es möglich ist, dass ein Angriff unentdeckt bleibt, haben unsere Untersuchungen ergeben, dass die NetApp -Technologie zu einem hohen Erkennungsgrad bei bestimmten Ransomware-Angriffen auf Basis der Dateiverschlüsselung geführt hat.]
- **Reagieren** Sie auf potenzielle Ransomware-Angriffe, indem Sie automatisch einen manipulationssicheren NetApp ONTAP -Snapshot initiieren, der gesperrt ist, sodass die Kopie nicht versehentlich oder böswillig gelöscht werden kann. Ihre Sicherungsdaten bleiben unveränderlich und durchgängig vor Ransomware-Angriffen an der Quelle und am Ziel geschützt.
- **Stellen Sie Ihre Workloads wieder her** und beschleunigen Sie so die Workload-Betriebszeit durch die Orchestrierung mehrerer NetApp -Technologien. Sie können die Wiederherstellung bestimmter Volumes auswählen. Ransomware Resilience bietet Empfehlungen zu den besten Optionen.
- **Regieren**: Implementieren Sie Ihre Ransomware-Schutzstrategie und überwachen Sie die Ergebnisse.



Vorteile der Verwendung von Ransomware Resilience

Ransomware Resilience bietet die folgenden Vorteile:

- Erkennt Workloads und ihre vorhandenen Snapshot- und Backup-Zeitpläne und ordnet sie nach ihrer relativen Wichtigkeit.
- Bewertet Ihren Ransomware-Schutzstatus und zeigt ihn in einem leicht verständlichen Dashboard an.
- Bietet Empfehlungen zu den nächsten Schritten basierend auf der Erkennung und Analyse der Schutzlage.
- Wendet KI-/ML-gesteuerte Datenschutzempfehlungen mit Ein-Klick-Zugriff an.
- Schützt Daten in den wichtigsten anwendungsbasierten Workloads, wie MySQL, Oracle, VMware-Datenspeichern und Dateifreigaben.
- Erkennt mithilfe von KI-Technologie Ransomware-Angriffe auf Daten im Primärspeicher in Echtzeit.
- Leitet als Reaktion auf erkannte potenzielle Angriffe automatisierte Aktionen ein, indem es Snapshot-Kopien erstellt und Warnungen bei ungewöhnlichen Aktivitäten auslöst.
- Wendet kuratierte Wiederherstellung an, um RPO-Richtlinien zu erfüllen. Ransomware Resilience orchestriert die Wiederherstellung nach Ransomware-Vorfällen mithilfe mehrerer NetApp Wiederherstellungsdienste, darunter NetApp Backup and Recovery (früher Cloud Backup) und SnapCenter.
- Verwendet die rollenbasierte Zugriffskontrolle (RBAC), um den Zugriff auf Funktionen und Vorgänge zu regeln.

Kosten

NetApp berechnet Ihnen für die Nutzung der Testversion von Ransomware Resilience keine Gebühren.

> Mit der Veröffentlichung im Oktober 2024 bieten neue Bereitstellungen von Ransomware Resilience eine 30-tägige kostenlose Testversion. Zuvor bot Ransomware Resilience eine 90-tägige kostenlose Testversion an. Wenn Sie sich bereits für die 90-tägige kostenlose Testversion angemeldet haben, ist diese Testversion 90 Tage lang gültig.

Wenn Sie sowohl über Backup and Recovery als auch über Ransomware Resilience verfügen, werden alle

gemeinsamen Daten, die durch beide Produkte geschützt werden, nur über Ransomware Resilience abgerechnet.

Nachdem Sie eine Lizenz oder ein PayGo-Abonnement erworben haben, wird jede Arbeitslast, für die eine Ransomware-Erkennungsrichtlinie (Autonomous Ransomware Protection) aktiviert ist (von Ransomware Resilience erkannt oder festgelegt) und für die mindestens eine Snapshot- oder Sicherungsrichtlinie gilt, von Ransomware Resilience als „Geschützt“ eingestuft und auf die erworbene Kapazität oder das PayGo-Abonnement angerechnet. Wenn eine Arbeitslast ohne Erkennungsrichtlinie erkannt wird, selbst wenn sie über Sicherungs- oder Snapshot-Richtlinien verfügt, wird sie als „gefährdet“ eingestuft und *nicht* auf die erworbene Kapazität angerechnet.

Geschützte Workloads werden nach Ablauf der 90-tägigen Testphase auf die erworbene Kapazität oder das Abonnement angerechnet. Ransomware Resilience wird pro GB für die Daten berechnet, die mit geschützten Workloads vor Effizienzsteigerungen verbunden sind.

Lizenzierung

Mit Ransomware Resilience können Sie verschiedene Lizenzpläne nutzen, darunter eine kostenlose Testversion, ein Pay-as-you-go-Abonnement oder die Nutzung Ihrer eigenen Lizenz.

Für Ransomware Resilience ist eine NetApp ONTAP One-Lizenz erforderlich.

Die Ransomware Resilience-Lizenz umfasst keine zusätzlichen NetApp Produkte. Ransomware Resilience kann Backup und Recovery verwenden, auch wenn Sie keine Lizenz dafür haben.

Um anomales Benutzerverhalten zu erkennen, verwendet Ransomware Resilience NetApp Autonomous Ransomware Protection, ein Machine-Learning-Modell (ML) innerhalb von ONTAP , das bösartige Dateiaktivitäten erkennt. Dieses Modell ist in der Ransomware Resilience-Lizenz enthalten.

Weitere Informationen finden Sie unter "Einrichten der Lizenzierung" .

NetApp Konsole

Auf Ransomware Resilience kann über die NetApp Konsole zugegriffen werden.

Die NetApp Konsole ermöglicht eine zentrale Verwaltung von NetApp -Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene. Die Konsole ist für den Zugriff auf und die Nutzung der NetApp -Datendienste erforderlich. Als Verwaltungsschnittstelle ermöglicht es Ihnen, viele Speicherressourcen über eine Schnittstelle zu verwalten. Konsolenadministratoren können den Zugriff auf Speicher und Dienste für alle Systeme innerhalb des Unternehmens steuern.

Sie benötigen weder eine Lizenz noch ein Abonnement, um die NetApp -Konsole zu verwenden. Es fallen nur dann Kosten an, wenn Sie Konsolenagenten in Ihrer Cloud bereitstellen müssen, um die Konnektivität zu Ihren Speichersystemen oder NetApp -Datendiensten sicherzustellen. Einige NetApp -Datendienste, auf die über die Konsole zugegriffen werden kann, sind jedoch lizenz- oder abonnementbasiert.

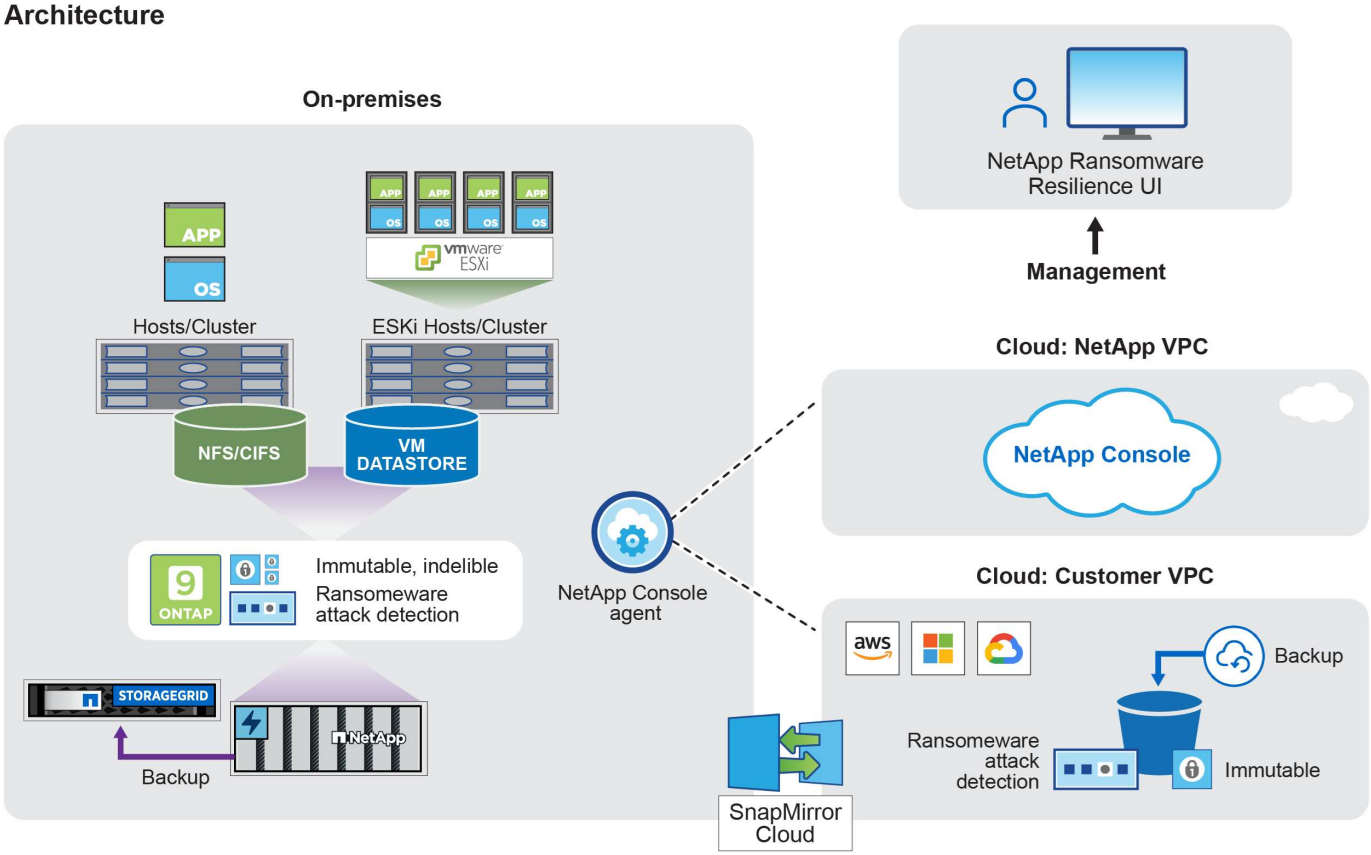
Erfahren Sie mehr über die"NetApp Konsole" .

So funktioniert Ransomware Resilience

Ransomware Resilience verwendet NetApp Backup and Recovery, um Snapshot- und Backup-Richtlinien für Dateifreigabe-Workloads zu ermitteln und festzulegen, und SnapCenter oder SnapCenter für VMware, um Snapshot- und Backup-Richtlinien für Anwendungs- und VM-Workloads zu ermitteln und festzulegen. Darüber hinaus verwendet Ransomware Resilience Backup and Recovery und SnapCenter / SnapCenter für VMware,

um eine datei- und workloadkonsistente Wiederherstellung durchzuführen.

Architecture



Funktion	Beschreibung
IDENTIFIZIEREN	• Findet alle lokalen NAS- (NFS- und CIFS-Protokolle), SAN- (FC, iSCSI und NVMe) und Cloud Volumes ONTAP Daten des Kunden, die mit der Konsole verbunden sind. • Identifiziert Kundendaten von ONTAP und SnapCenter Service-APIs und verknüpft sie mit Workloads. Erfahren Sie mehr über "ONTAP" Und "SnapCenter Software" . • Ermittelt die aktuelle Schutzstufe der NetApp Snapshot-Kopien und Sicherungsrichtlinien jedes Volumes sowie alle On-Box-Erkennungsfunktionen. Ransomware Resilience verknüpft diese Schutzhaltung dann mit den Workloads, indem es Backup und Recovery, ONTAP Dienste und NetApp -Technologien wie Autonomous Ransomware Protection (ARP oder ARP/AI, abhängig von Ihrer ONTAP Version), FPolicy, Backup-Richtlinien und Snapshot-Richtlinien verwendet. Erfahren Sie mehr über "Autonomer Ransomware-Schutz" , "NetApp Backup und Recovery" , Und "ONTAP FPolicy" . • Weist jedem Workload basierend auf automatisch erkannten Schutzstufen eine Geschäftspriorität zu und empfiehlt Schutzrichtlinien für Workloads basierend auf ihrer Geschäftspriorität. Die Arbeitslastpriorität basiert auf den Snapshot-Häufigkeiten, die bereits auf jedes mit der Arbeitslast verknüpfte Volume angewendet werden.
SCHÜTZEN	• Überwacht aktiv Workloads und orchestriert die Verwendung von Backup und Recovery, SnapCenter und ONTAP -APIs, indem Richtlinien auf jeden der identifizierten Workloads angewendet werden.

Funktion	Beschreibung
ERKENNEN	• Erkennt potenzielle Angriffe mit einem integrierten Machine-Learning-Modell (ML), das potenziell anomale Verschlüsselung und Aktivität erkennt. • Bietet eine zweischichtige Erkennung, die mit der Erkennung potenzieller Ransomware-Angriffe im Primärspeicher beginnt und auf abnormale Aktivitäten reagiert, indem zusätzliche automatisierte Snapshot-Kopien erstellt werden, um die nächstgelegenen Datenwiederherstellungspunkte zu erstellen. Ransomware Resilience bietet die Möglichkeit, tiefer zu graben, um potenzielle Angriffe präziser zu identifizieren, ohne die Leistung der primären Workloads zu beeinträchtigen. • Bestimmt die spezifischen verdächtigen Dateien und ordnet diese Angriffe den zugehörigen Workloads zu. Dabei kommen ONTAP, Autonomous Ransomware Protection (ARP oder ARP/AI, abhängig von Ihrer ONTAP Version) und FPolicy-Technologien zum Einsatz.
ANTWORTEN	• Zeigt relevante Daten wie Dateiaktivität, Benutzeraktivität und Entropie an, um Ihnen bei der Durchführung forensischer Überprüfungen des Angriffs zu helfen. • Initiiert schnelle Snapshot-Kopien mithilfe von NetApp -Technologien und -Produkten wie ONTAP, Autonomous Ransomware Protection (ARP oder ARP/AI, abhängig von Ihrer ONTAP Version) und FPolicy.
GENESEN	• Bestimmt den besten Snapshot oder das beste Backup und empfiehlt den besten tatsächlichen Wiederherstellungspunkt (RPA) unter Verwendung von Backup und Recovery, ONTAP, Autonomous Ransomware Protection (ARP oder ARP/AI, abhängig von Ihrer ONTAP Version) und FPolicy-Technologien und -Diensten. • Orchestriert die Wiederherstellung von Workloads, einschließlich VMs, Dateifreigaben, Blockspeicher und Datenbanken mit Anwendungskonsistenz.
REGIEREN	• Weist die Ransomware-Schutzstrategien zu • Hilft Ihnen, die Ergebnisse zu überwachen.

Unterstützte Sicherungsziele, Systeme und Workload-Datenquellen

Ransomware Resilience unterstützt die folgenden Sicherungsziele, Systeme und Datenquellen:

Unterstützte Backup-Ziele

- Amazon Web Services (AWS) S3
- Google Cloud Platform
- Microsoft Azure Blob
- NetApp StorageGRID

Unterstützte Systeme

- On-Premises ONTAP NAS (mit NFS- und CIFS-Protokollen) mit ONTAP Version 9.11.1 und höher
- On-Premises ONTAP SAN (mit FC-, iSCSI- und NVMe-Protokollen) mit ONTAP Version 9.17.1 und höher
- Cloud Volumes ONTAP 9.11.1 oder höher für AWS (unter Verwendung der Protokolle NFS und CIFS)

- Cloud Volumes ONTAP 9.11.1 oder höher für Google Cloud Platform (unter Verwendung der Protokolle NFS und CIFS)
- Cloud Volumes ONTAP 9.12.1 oder höher für Microsoft Azure (unter Verwendung der Protokolle NFS und CIFS)
- Cloud Volumes ONTAP 9.17.1 oder höher für AWS, Google Cloud Platform und Microsoft Azure (unter Verwendung der Protokolle FC, iSCSI und NVMe)
- Amazon FSx for NetApp ONTAP, das Autonomous Ransomware Protection (ARP und nicht ARP/AI) verwendet

  ARP/AI erfordert ONTAP 9.16 oder höher.

Folgendes wird nicht unterstützt: FlexGroup Volumes, ONTAP Versionen älter als 9.11.1, Mount Point-Volumes, Mount Path-Volumes, Offline-Volumes und Data Protection (DP)-Volumes.

Unterstützte Workload-Datenquellen

Ransomware Resilience schützt die folgenden anwendungsbasierten Workloads auf primären Datenvolumes:

- NetApp -Dateifreigaben
- Blockspeicher
- VMware-Datenspeicher
- Datenbanken (MySQL und Oracle)
- Mehr folgt in Kürze

Wenn Sie SnapCenter oder SnapCenter für VMware verwenden, werden außerdem alle von diesen Produkten unterstützten Workloads in Ransomware Resilience identifiziert. Ransomware Resilience kann diese auf eine Workload-konsistente Weise schützen und wiederherstellen.

Begriffe, die Ihnen beim Schutz vor Ransomware helfen könnten

Es kann hilfreich sein, sich mit der Terminologie im Zusammenhang mit dem Schutz vor Ransomware vertraut zu machen.

- **Schutz**: Schutz vor Ransomware-Resilienz bedeutet, sicherzustellen, dass mithilfe von Schutzrichtlinien regelmäßig Snapshots und unveränderliche Backups in einer anderen Sicherheitsdomäne erstellt werden.
- **Workload**: Ein Workload in Ransomware Resilience kann MySQL- oder Oracle-Datenbanken, VMware-Datenspeicher oder Dateifreigaben umfassen.

Voraussetzungen für NetApp Ransomware Resilience

Beginnen Sie mit NetApp Ransomware Resilience, indem Sie die Bereitschaft Ihrer Betriebsumgebung, Anmeldung, Ihres Netzwerkzugriffs und Ihres Webbrowsers überprüfen.

Um Ransomware Resilience zu verwenden, müssen Sie die folgenden Voraussetzungen erfüllen.

In der NetApp Konsole

- Ein NetApp Konsolenbenutzerkonto mit Organisationsadministratorberechtigungen zum Erkennen von Ressourcen.
- Eine Konsolenorganisation mit mindestens einem aktiven Konsolenagenten, der eine Verbindung zu lokalen ONTAP Clustern oder zu Cloud Volumes ONTAP in AWS oder Azure herstellt.
- Der Konsolenagent muss über die `cloudmanager-ransomware-protection` Container in einem aktiven Zustand.
- Mindestens ein Konsolensystem mit einem lokalen NetApp ONTAP -Cluster oder Cloud Volumes ONTAP in AWS oder Azure. Ransomware Resilience unterstützt sowohl NAS- (NFS und SMB) als auch SAN-Protokolle (iSCSI, FC und NVMe).
  - ONTAP oder Cloud Volumes ONTAP Cluster mit ONTAP OS Version 9.11.1 oder höher werden unterstützt.

    SAN-Workloads werden nur in ONTAP 9.17.1 und höher unterstützt.
  - Wenn Ihre lokalen ONTAP Cluster oder Cloud Volumes ONTAP in AWS oder in der Azure-Cloud noch nicht in die Konsole integriert sind, benötigen Sie einen Konsolenagenten.

    Siehe "Erfahren Sie, wie Sie einen Konsolenagenten konfigurieren" Und "Standardanforderungen für die Konsole" .

Wenn Sie mehrere Konsolenagenten in einer einzigen Konsolenorganisation haben, scannt Ransomware Resilience die ONTAP Ressourcen aller Konsolenagenten über den derzeit in der Konsolen-Benutzeroberfläche ausgewählten Agenten hinaus.

In ONTAP 9.11.1 und höher

- Auf der lokalen ONTAP Instanz ist eine ONTAP One-Lizenz aktiviert.
- Eine Lizenz für NetApp Autonomous Ransomware Protection, verwendet von Ransomware Resilience, aktiviert auf der lokalen ONTAP Instanz, abhängig von der von Ihnen verwendeten ONTAP -Version. Siehe "Übersicht über den autonomen Ransomware-Schutz" .

  Die allgemeine Version von Ransomware Resilience enthält im Gegensatz zur Vorschauversion eine Lizenz für die NetApp Autonomous Ransomware Protection-Technologie. Siehe "Übersicht über den autonomen Ransomware-Schutz" für Details.

  Weitere Lizenzdetails finden Sie unter"Erfahren Sie mehr über Ransomware-Resilienz" .
- Um Schutzkonfigurationen anzuwenden (wie etwa die Aktivierung des autonomen Ransomware-Schutzes und anderer), benötigt Ransomware Resilience Administratorberechtigungen für den ONTAP Cluster. Das Onboarding des ONTAP Clusters sollte ausschließlich mit den Anmeldeinformationen des ONTAP Cluster-Administratorbenutzers erfolgen.
- Wenn der ONTAP Cluster bereits mit den Anmeldeinformationen eines Nicht-Administratorbenutzers in der Konsole integriert ist, müssen die Berechtigungen des Nicht-Administratorbenutzers durch die Anmeldung beim ONTAP Cluster mit den erforderlichen Berechtigungen aktualisiert werden, wie auf dieser Seite beschrieben.

Für Datensicherungen

- Ein Konto in NetApp StorageGRID, AWS S3, Azure Blob oder Google Cloud Platform für Sicherungsziele und die festgelegten Zugriffsberechtigungen.

  Weitere Informationen finden Sie im "AWS-, Azure- oder S3-Berechtigungsliste" für Details.

- NetApp Backup and Recovery muss auf dem System nicht aktiviert werden.

  Ransomware Resilience hilft bei der Konfiguration eines Sicherungsziels über die Option „Einstellungen“. Sehen "Konfigurieren der Einstellungen" .

Aktualisieren Sie die Berechtigungen von Nicht-Administratorbenutzern in einem ONTAP -System

Wenn Sie die Berechtigungen von Nicht-Administratorbenutzern für ein bestimmtes System aktualisieren müssen, führen Sie diese Schritte aus.

1. Melden Sie sich bei der Konsole an und suchen Sie nach dem System, dessen ONTAP Benutzerberechtigungen aktualisiert werden müssen.
2. Wählen Sie das System aus, um Details anzuzeigen.
3. Wählen Sie **Zusätzliche Informationen anzeigen**, um den Benutzernamen anzuzeigen.
4. Melden Sie sich mit dem Administratorbenutzer bei der CLI des ONTAP -Clusters an.
5. Zeigen Sie die vorhandenen Rollen für diesen Benutzer an. Eingeben:

   ```
   security login show -user-or-group-name <username>
   ```

6. Ändern Sie die Rolle für den Benutzer. Eingeben:

   ```
   security login modify -user-or-group-name <username> -application
   console|http|ontapi|ssh|telnet -authentication-method password -role
   admin
   ```

7. Kehren Sie zur Ransomware Resilience-Benutzeroberfläche zurück, um es zu verwenden.

Schnellstart für NetApp Ransomware Resilience

Hier finden Sie eine Übersicht über die erforderlichen Schritte für den Einstieg in NetApp Ransomware Resilience. Über die Links in den einzelnen Schritten gelangen Sie zu einer Seite mit weiteren Einzelheiten.

Überprüfen der Voraussetzungen

"Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt" .

Ransomware-Resilienz einrichten

- "Bereiten Sie NetApp StorageGRID, Amazon Web Services, Google Cloud Platform oder Microsoft Azure als Sicherungsziel vor" .
- "Konfigurieren eines Konsolenagenten" .
- "Einrichten der Lizenzierung" .
- "Workloads in der Konsole ermitteln" .
- "Konfigurieren von Sicherungszielen" .
- "Aktivieren Sie optional die Bedrohungserkennung" .
- "Führen Sie optional eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Wie geht es weiter?

Nachdem Sie Ransomware Resilience eingerichtet haben, können Sie als Nächstes Folgendes tun.

- "Zeigen Sie den Zustand des Workload-Schutzes auf dem Dashboard an" .
- "Workloads schützen" .
- "Reagieren Sie auf die Erkennung potenzieller Ransomware-Angriffe" .
- "Wiederherstellung nach einem Angriff (nachdem Vorfälle neutralisiert wurden)" .

Einrichten von NetApp Ransomware Resilience

Sie können NetApp Ransomware Resilience problemlos bereitstellen. Bevor Sie beginnen, überprüfen Sie"Voraussetzungen" um sicherzustellen, dass Ihre Umgebung bereit ist.

Vorbereiten des Sicherungsziels

Bereiten Sie eines der folgenden Sicherungsziele vor:

- NetApp StorageGRID
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

Nachdem Sie Optionen im Sicherungsziel selbst konfiguriert haben, konfigurieren Sie es später als Sicherungsziel in Ransomware Resilience. Einzelheiten zum Konfigurieren des Sicherungsziels in Ransomware Resilience finden Sie unter"Konfigurieren von Sicherungszielen" .

Bereiten Sie StorageGRID als Backup-Ziel vor

Wenn Sie StorageGRID als Backup-Ziel verwenden möchten, lesen Sie "StorageGRID -Dokumentation" für Details zu StorageGRID.

Bereiten Sie AWS darauf vor, ein Backup-Ziel zu werden

- Richten Sie ein Konto in AWS ein.
- Konfigurieren "AWS-Berechtigungen" in AWS.

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

Bereiten Sie Azure als Sicherungsziel vor

- Richten Sie ein Konto in Azure ein.
- Konfigurieren "Azure-Berechtigungen" in Azure.

Weitere Informationen zur Verwaltung Ihres Azure-Speichers in der Konsole finden Sie unter "Verwalten Ihrer Azure-Speicherkonten" .

Einrichten der NetApp Konsole

Der nächste Schritt besteht darin, die Konsole und die Ransomware-Resilienz einzurichten.

Rezension "Konsolenanforderungen für den Standardmodus" .

Erstellen eines Konsolenagenten

Wenden Sie sich an Ihren NetApp -Vertriebsmitarbeiter, um diesen Service auszuprobieren oder zu nutzen. Wenn Sie dann den Konsolenagenten verwenden, enthält dieser die entsprechenden Funktionen für Ransomware-Resilienz.

Um einen Konsolen-Agenten mit Ransomware Resilience zu erstellen, wenden Sie sich an den Administrator Ihrer Konsolenorganisation, der über die Berechtigung zum Erstellen von Konsolen-Agenten verfügt, und lesen Sie die Dokumentation, die Folgendes beschreibt: "So erstellen Sie einen Konsolenagenten" .

> Wenn Sie über mehrere Konsolenagenten verfügen, scannt der Ransomware-Resilienz-Datensatz alle Konsolenagenten zusätzlich zu dem, der aktuell in der Konsole angezeigt wird. Dieser Dienst erkennt alle Projekte und alle Konsolenagenten, die mit dieser Organisation verknüpft sind.

Zugriff auf NetApp Ransomware Resilience

Melden Sie sich über die NetApp -Konsole bei NetApp Ransomware Resilience an.

Um sich bei der Konsole anzumelden, können Sie Ihre Anmeldeinformationen für die NetApp Support-Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für eine NetApp Cloud-Anmeldung anmelden. "Erfahren Sie mehr über die Anmeldung" .

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 BlueXP -Zugriffsrollen für alle Dienste" .

Schritte

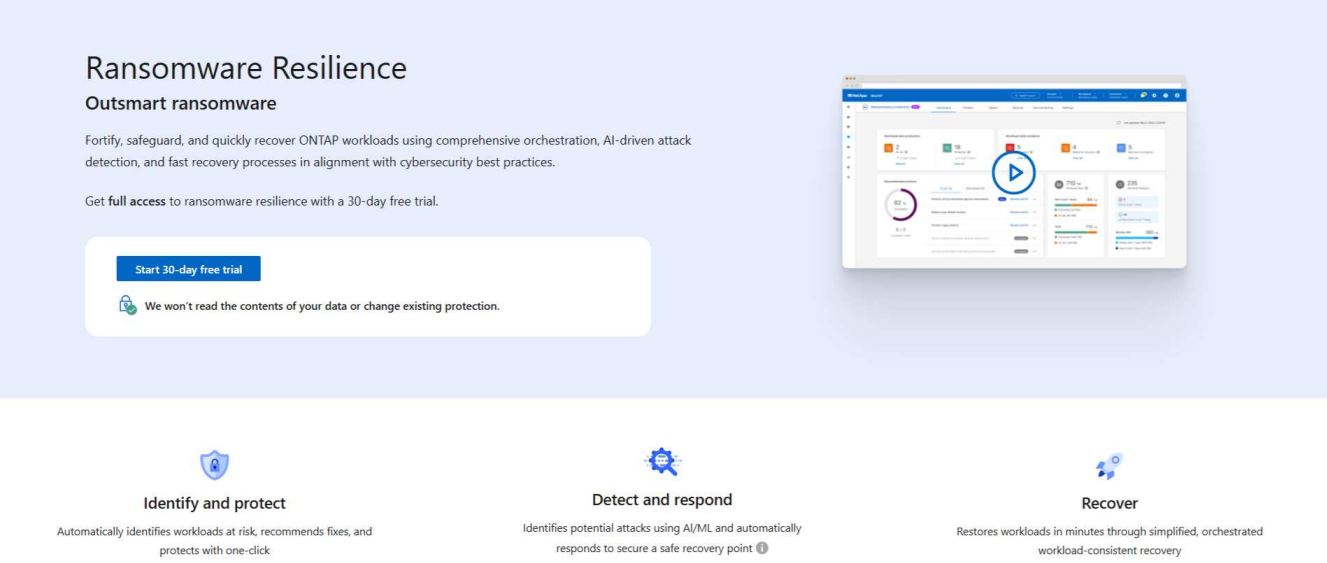
1. Öffnen Sie einen Webbrowser und gehen Sie zu"die Konsole" .

Die Anmeldeseite der Konsole wird angezeigt.

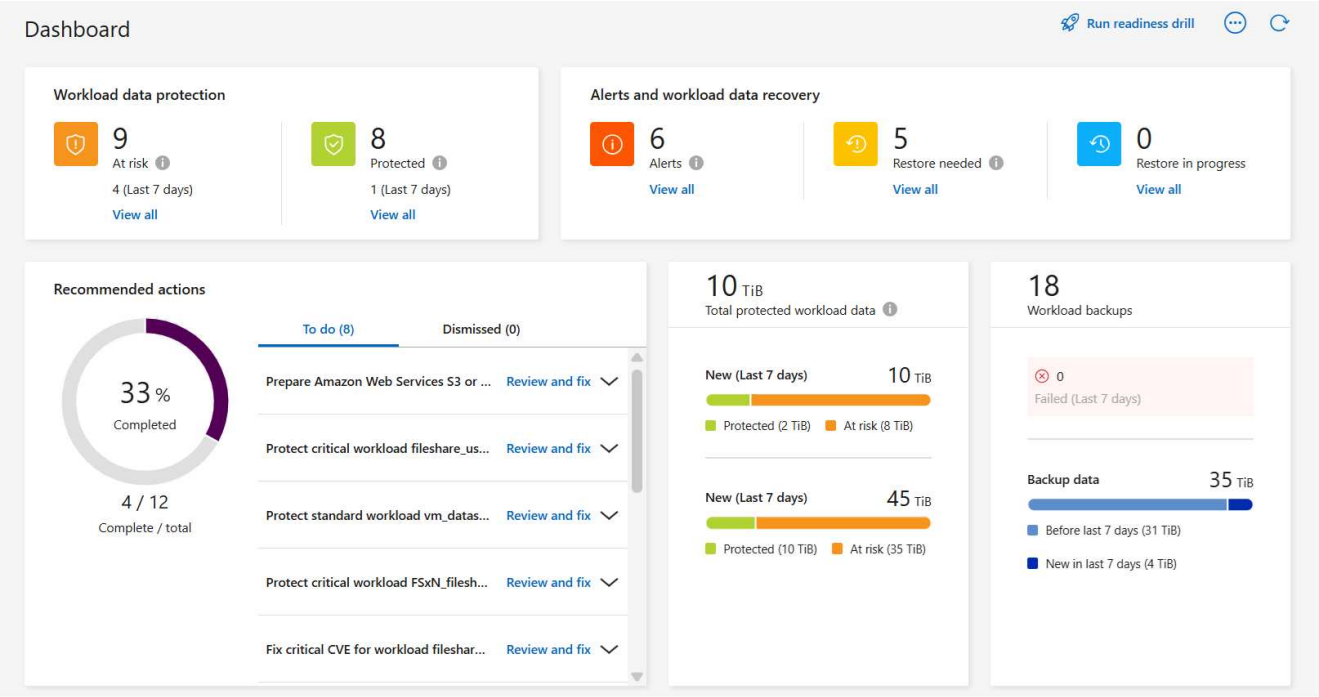
2. Melden Sie sich bei der Konsole an.
3. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz** aus.

   Wenn Sie sich zum ersten Mal bei diesem Dienst anmelden, wird die Zielseite angezeigt.

   Wenn Sie keinen Konsolenagenten haben oder es nicht der richtige für diesen Dienst ist, müssen Sie einen bereitstellen. "Erfahren Sie, wie Sie einen Konsolenagenten einrichten" .



Andernfalls wird das Ransomware Resilience-Dashboard angezeigt.



4. Wählen Sie die Option **Workloads ermitteln** aus, falls Sie dies noch nicht getan haben.

Weitere Informationen finden Sie unter "Workloads ermitteln" .

Einrichten der Lizenzierung für NetApp Ransomware Resilience

Mit NetApp Ransomware Resilience können Sie verschiedene Lizenzpläne nutzen.

Um diese Aufgabe auszuführen, benötigen Sie die Rolle des Organisationsadministrators, Ordner- oder Projektadministrators. "Erfahren Sie mehr über Konsolenzugriffsrollen" .

Lizenztypen Sie können die folgenden Lizenztypen verwenden:

- Melden Sie sich für eine 30-tägige kostenlose Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) bei Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace oder Azure Marketplace.
- Bringen Sie Ihre eigene Lizenz (BYOL) mit. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL in der Konsole zu aktivieren.

Nachdem Sie Ihr BYOL eingerichtet oder ein PAYGO-Abonnement erworben haben, können Sie die Lizenz im Abschnitt „Lizenzen und Abonnements“ der Konsole sehen.

Nach Ablauf der kostenlosen Testversion oder der Lizenz bzw. des Abonnements können Sie in Ransomware Resilience weiterhin Folgendes tun:

- Zeigen Sie Arbeitslasten und Arbeitslastzustand an.
- Löschen Sie eine beliebige Ressource, beispielsweise eine Richtlinie.
- Führen Sie alle geplanten Vorgänge aus, die während der Testphase oder unter der Lizenz erstellt wurden.

Andere Lizenzen

Die Ransomware Resilience-Lizenz umfasst keine zusätzlichen NetApp Produkte. Ransomware Resilience kann NetApp Backup and Recovery verwenden, auch wenn Sie keine Lizenz dafür haben.

Wenn Sie sowohl über Backup and Recovery als auch über Ransomware Resilience verfügen, werden alle gemeinsamen Daten, die durch beide Produkte geschützt werden, nur über Ransomware Resilience abgerechnet.

Probieren Sie es mit einer 30-tägigen kostenlosen Testversion aus

Sie können Ransomware Resilience mit einer 30-tägigen kostenlosen Testversion ausprobieren. Sie müssen ein Konsolenorganisationsadministrator sein, um die kostenlose Testversion zu starten.

Mit der Veröffentlichung im Oktober 2024 können neue Bereitstellungen von Ransomware Resilience jetzt 30 Tage lang kostenlos getestet werden. Zuvor war für Ransomware Resilience eine 90-tägige kostenlose Testversion verfügbar. Wenn Sie bereits an der 90-tägigen kostenlosen Testversion teilnehmen, gilt dieses Angebot für die nächsten 90 Tage.

Während der Testphase gelten keine Kapazitätsbeschränkungen.

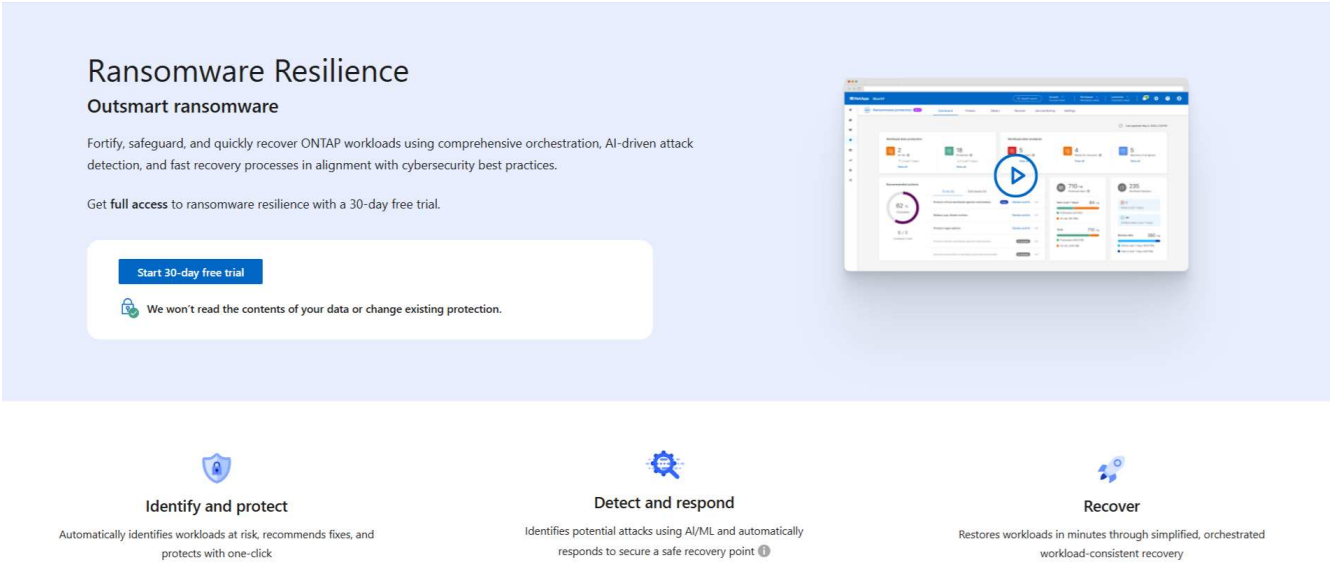
Sie können jederzeit eine Lizenz erwerben oder ein Abonnement abschließen. Bis zum Ende der 30-tägigen Testphase werden Ihnen keine Kosten berechnet. Um nach der 30-tägigen Testversion fortzufahren, müssen Sie eine BYOL-Lizenz oder ein PAYGO-Abonnement erwerben.

Während der Testphase steht Ihnen die volle Funktionalität zur Verfügung.

Schritte

1. Zugriff auf die "Konsole" .
2. Melden Sie sich bei der Konsole an.
3. Wählen Sie in der NetApp Konsole **Schutz** > **Ransomware-Resilienz**.

   Wenn Sie sich zum ersten Mal bei diesem Dienst anmelden, wird die Zielseite angezeigt.



4. Wenn Sie noch keinen Connector für andere Dienste hinzugefügt haben, fügen Sie einen hinzu.

   Informationen zum Hinzufügen eines Konsolenagenten finden Sie unter "Erfahren Sie mehr über Konsolenagenten" .

5. Nachdem Sie einen Konsolen-Agenten eingerichtet haben, ändert sich auf der Zielseite von Ransomware Resilience die Schaltfläche zum Hinzufügen eines Konsolen-Agenten in eine Schaltfläche zum Erkennen von Workloads. Wählen Sie **Beginnen Sie mit der Ermittlung von Workloads** aus.
6. Um die Informationen zur kostenlosen Testversion anzuzeigen, wählen Sie die Dropdown-Option oben rechts aus.

Nach Ablauf der Testphase ein Abonnement oder eine Lizenz erwerben

Nach Ablauf der kostenlosen Testphase können Sie entweder über einen der Marktplätze ein Abonnement abschließen oder eine Lizenz von NetApp erwerben.

Wenn Sie bereits ein PAYGO-Abonnement haben, wird die Lizenz nach Ablauf der kostenlosen Testphase automatisch auf das Abonnement umgestellt.

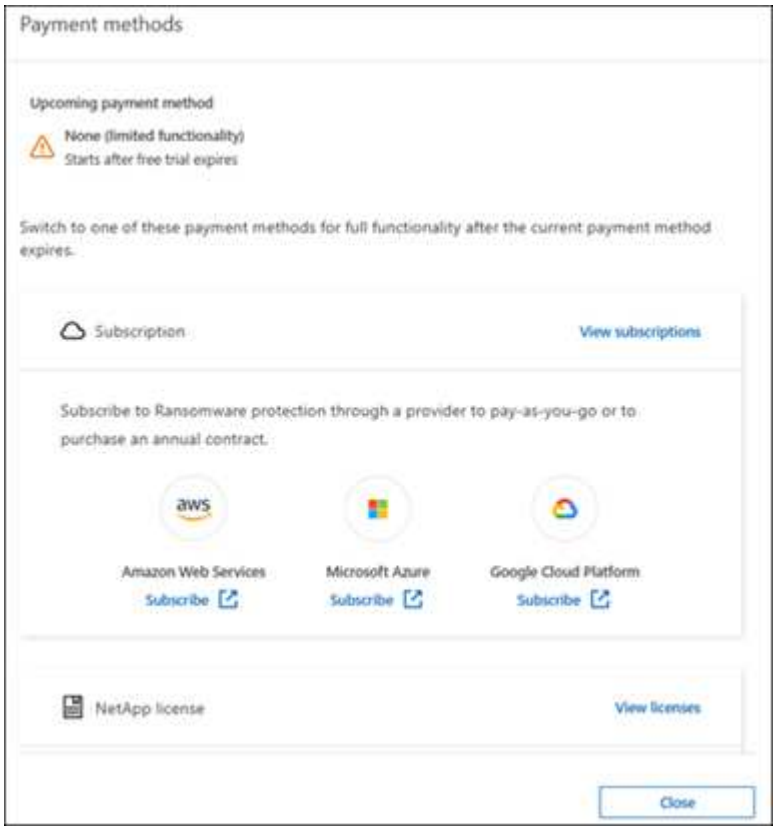
Abonnieren Sie über AWS Marketplace Abonnieren Sie über Microsoft Azure Marketplace Abonnieren Sie über den Google Cloud Platform Marketplace Bringen Sie Ihre eigene Lizenz mit (BYOL)

Abonnieren Sie über AWS Marketplace

Dieses Verfahren bietet einen allgemeinen Überblick darüber, wie Sie sich direkt im AWS Marketplace anmelden können.

Schritte

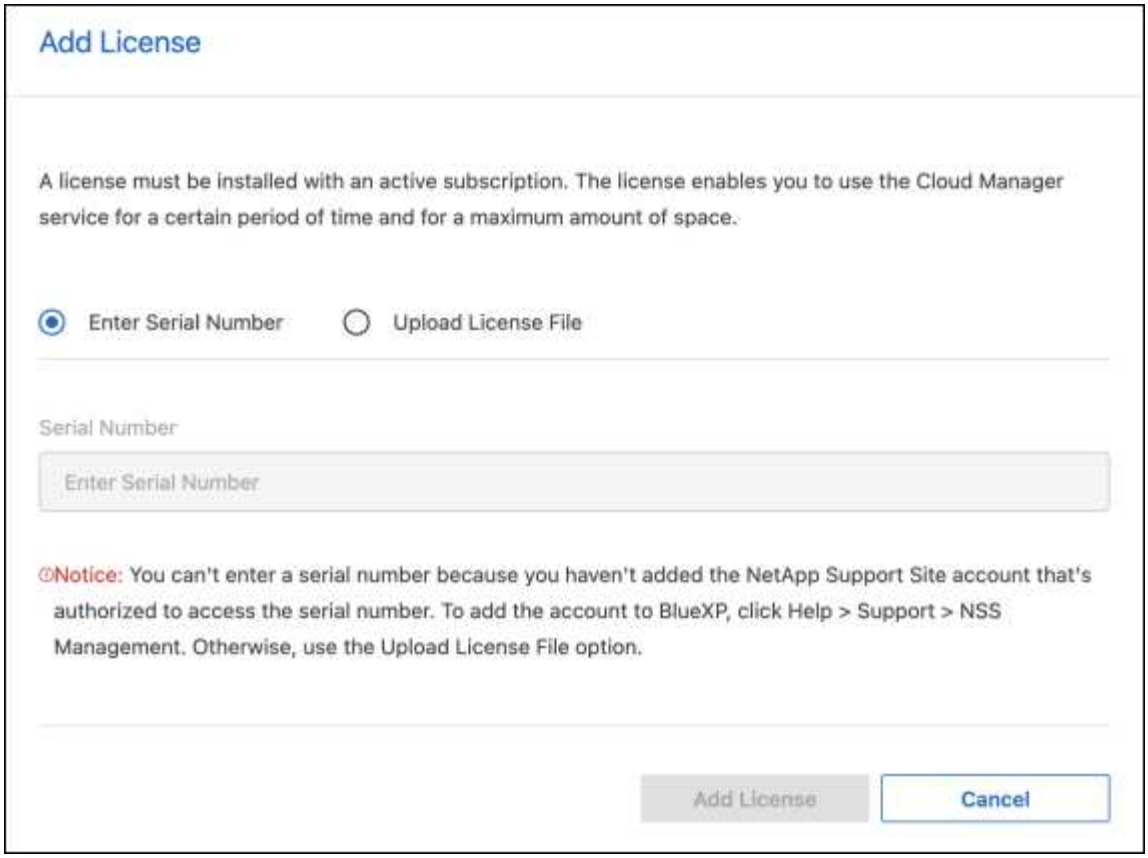
1. Führen Sie in Ransomware Resilience einen der folgenden Schritte aus:
   - Wenn Sie eine Meldung erhalten, dass die kostenlose Testversion abläuft, wählen Sie **Zahlungsmethoden anzeigen**.
   - Wenn Sie die Testversion noch nicht gestartet haben, wählen Sie oben rechts den Hinweis **Kostenlose Testversion** und dann **Zahlungsmethoden anzeigen**.



2. Wählen Sie auf der Seite „Zahlungsmethoden“ **Abonnieren** für **Amazon Web Services** aus.
3. Wählen Sie im AWS Marketplace **Kaufoptionen anzeigen** aus.
4. Verwenden Sie AWS Marketplace, um * NetApp Intelligent Services* und **Ransomware Resilience** zu abonnieren.
5. Wenn Sie zu Ransomware Resilience zurückkehren, wird eine Meldung angezeigt, dass Sie abonniert sind.

   Sie erhalten eine E-Mail mit der Seriennummer von Ransomware Resilience und dem Hinweis, dass Ransomware Resilience im AWS Marketplace abonniert ist.

6. Kehren Sie zur Seite mit den Zahlungsmethoden von Ransomware Resilience zurück.
7. Fügen Sie die Lizenz zur Konsole hinzu, indem Sie **Lizenz hinzufügen** auswählen.



8. Wählen Sie auf der Seite „Lizenz hinzufügen“ die Option „Seriennummer eingeben“, geben Sie die Seriennummer ein, die in der Ihnen zugesandten E-Mail enthalten war, und wählen Sie „Lizenz hinzufügen“ aus.
9. Um Lizenzdetails anzuzeigen, wählen Sie in der linken Navigation der Konsole **Verwaltung** > **Lizenzen und Abonnements**.
   - Um Abonnementinformationen anzuzeigen, wählen Sie **Abonnements**.
   - Um BYOL-Lizenzen anzuzeigen, wählen Sie **Data Services-Lizenzen**.
10. Zurück zur Ransomware-Resilienz. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz** aus.

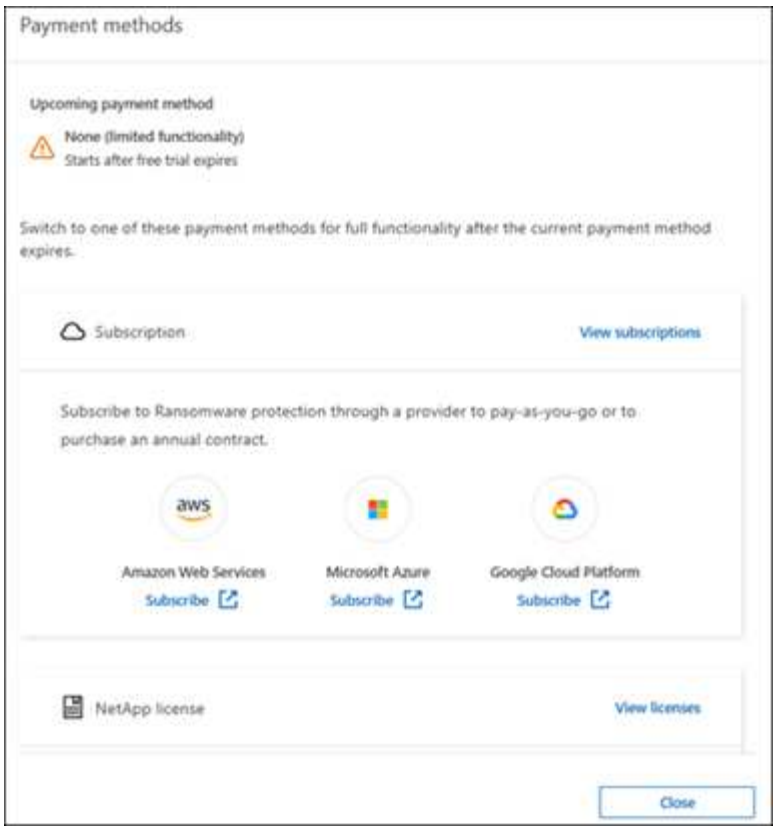
    Es wird eine Meldung angezeigt, dass eine Lizenz hinzugefügt wurde.

Abonnieren Sie über Microsoft Azure Marketplace

Dieses Verfahren bietet einen allgemeinen Überblick darüber, wie Sie sich direkt im Azure Marketplace anmelden können.

Schritte

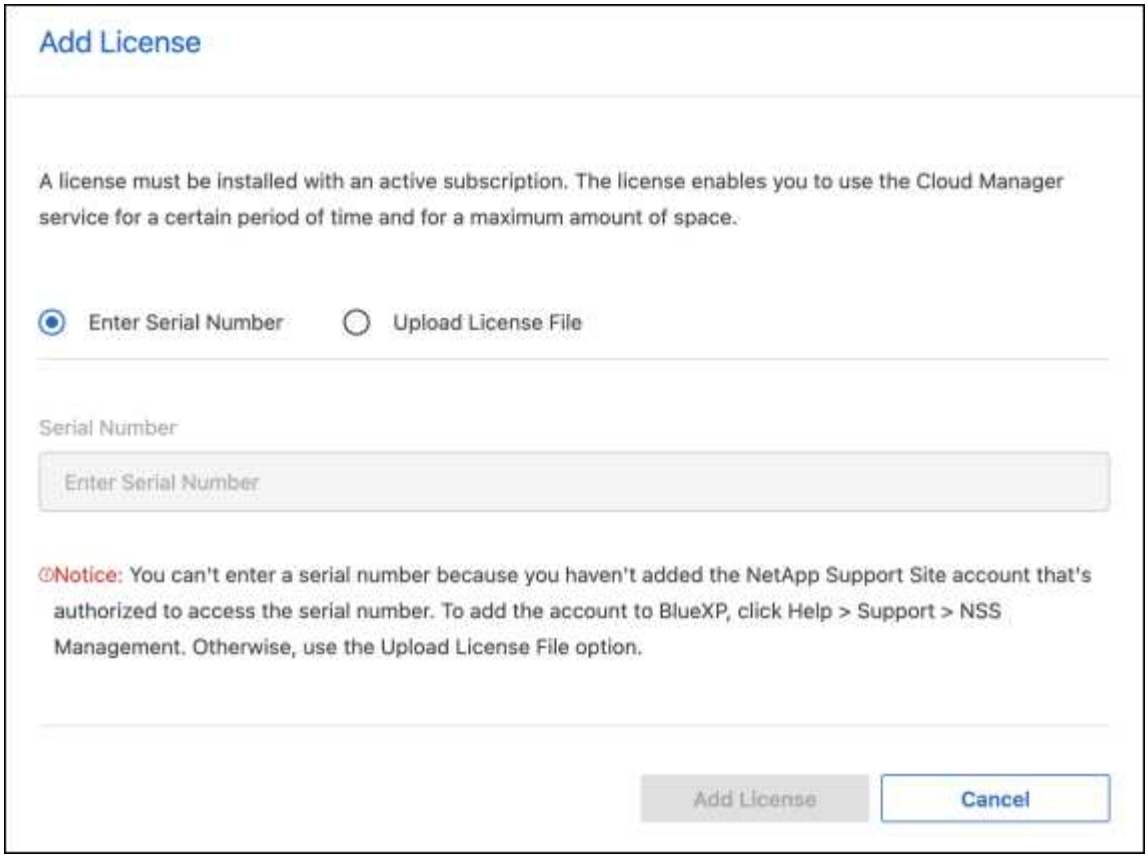
1. Führen Sie in Ransomware Resilience einen der folgenden Schritte aus:
   - Wenn Sie eine Meldung erhalten, dass die kostenlose Testversion abläuft, wählen Sie **Zahlungsmethoden anzeigen**.
   - Wenn Sie die Testversion noch nicht gestartet haben, wählen Sie oben rechts den Hinweis **Kostenlose Testversion** und dann **Zahlungsmethoden anzeigen**.



2. Wählen Sie auf der Seite „Zahlungsmethoden“ **Abonnieren** für **Microsoft Azure Marketplace** aus.
3. Wählen Sie im Azure Marketplace **Kaufoptionen anzeigen** aus.
4. Verwenden Sie Azure Marketplace, um * NetApp Intelligent Services* und * Ransomware Resilience* zu abonnieren.
5. Wenn Sie zu Ransomware Resilience zurückkehren, wird eine Meldung angezeigt, dass Sie abonniert sind.

> Sie erhalten eine E-Mail mit der Seriennummer von Ransomware Resilience und dem Hinweis, dass Ransomware Resilience im Azure Marketplace abonniert ist.

6. Kehren Sie zur Seite mit den Zahlungsmethoden für Ransomware Resilience zurück.
7. Um die Lizenz hinzuzufügen, wählen Sie **Lizenz hinzufügen**.



8. Wählen Sie auf der Seite „Lizenz hinzufügen“ die Option „Seriennummer eingeben“ aus und geben Sie dann die Seriennummer aus der E-Mail ein, die Sie erhalten haben. Wählen Sie **Lizenz hinzufügen**.
9. Um Lizenzdetails unter „Lizenzen und Abonnements“ anzuzeigen, wählen Sie in der linken Navigation der Konsole „Governance“ > „Lizenzen und Abonnements“ aus.
   - Um Abonnementinformationen anzuzeigen, wählen Sie **Abonnements**.
   - Um BYOL-Lizenzen anzuzeigen, wählen Sie **Data Services-Lizenzen**.
10. Zurück zur Ransomware-Resilienz. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz** aus.

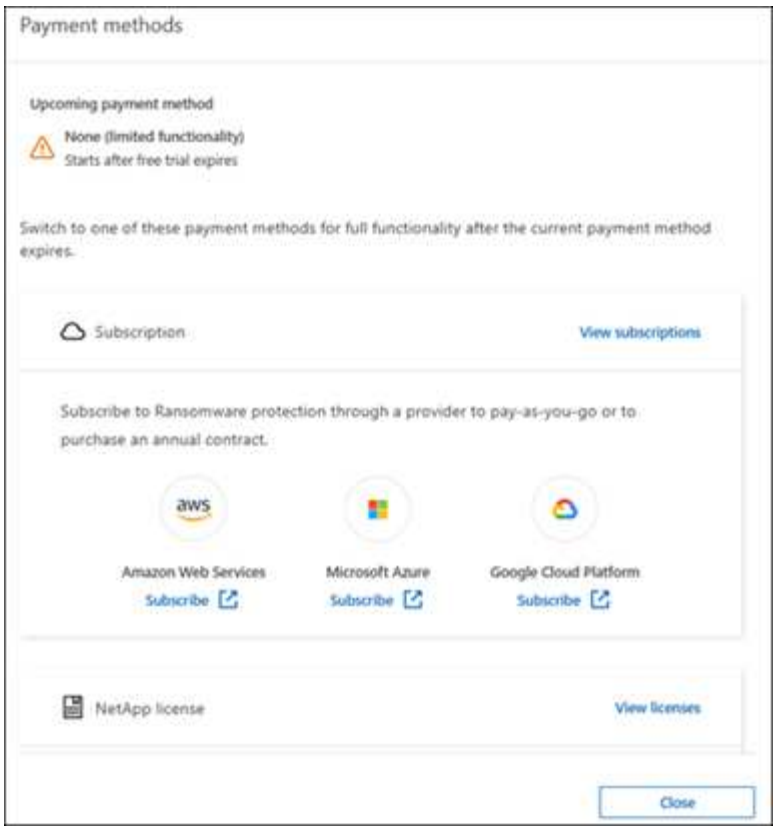
    Es wird eine Meldung angezeigt, dass eine Lizenz hinzugefügt wurde.

Abonnieren Sie über den Google Cloud Platform Marketplace

Dieses Verfahren bietet einen allgemeinen Überblick darüber, wie Sie sich direkt im Google Cloud Platform Marketplace anmelden können.

Schritte

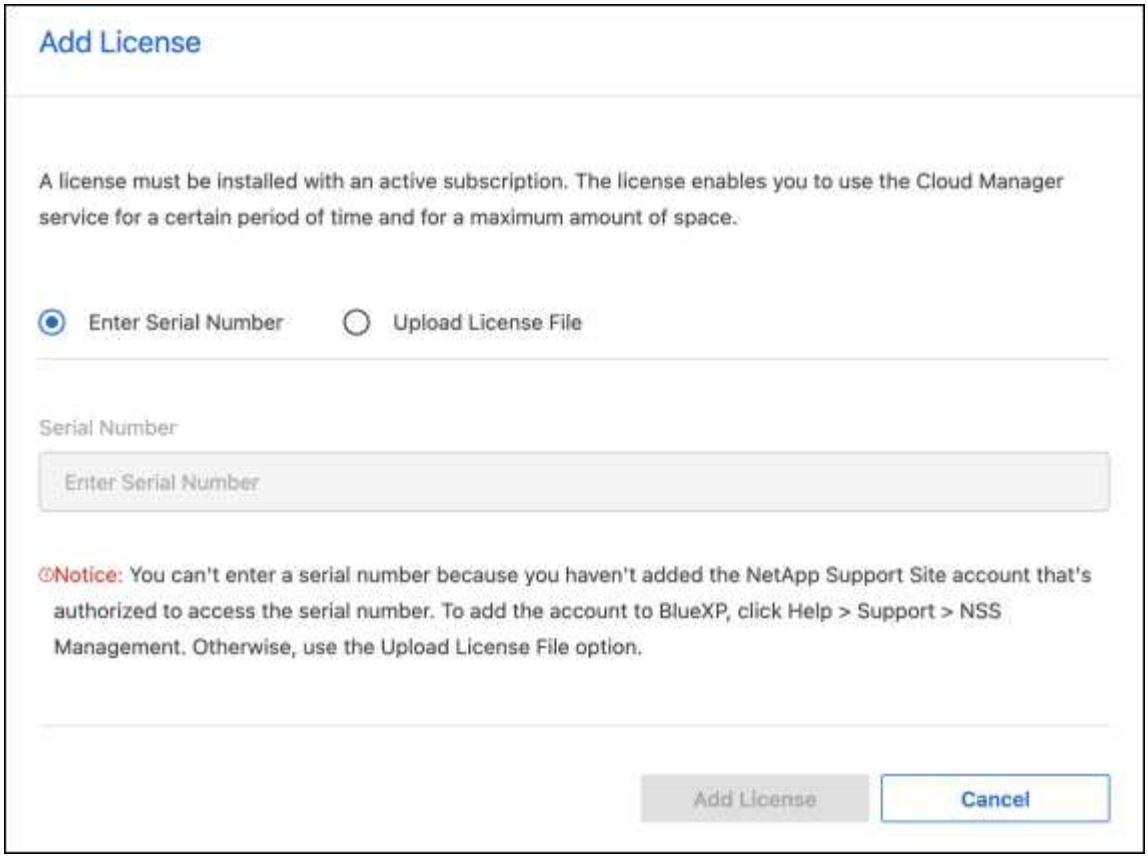
1. Führen Sie in der Ransomware-Resilienz einen der folgenden Schritte aus:
   - Wenn Sie eine Meldung erhalten, dass die kostenlose Testversion abläuft, wählen Sie **Zahlungsmethoden anzeigen**.
   - Wenn Sie die Testversion noch nicht gestartet haben, wählen Sie oben rechts den Hinweis **Kostenlose Testversion** und dann **Zahlungsmethoden anzeigen**.



2. Wählen Sie auf der Seite „Zahlungsmethoden“ die Option „Abonnieren“ für Google Cloud Platform Marketplace* aus.
3. Wählen Sie im Google Cloud Platform Marketplace **Abonnieren** aus.
4. Verwenden Sie den Google Cloud Platform Marketplace, um * NetApp Intelligent Services* und **Ransomware Resilience** zu abonnieren.
5. Wenn Sie zu Ransomware Resilience zurückkehren, wird eine Meldung angezeigt, dass Sie abonniert sind.

> Sie erhalten eine E-Mail mit der Seriennummer von Ransomware Resilience und dem Hinweis, dass Ransomware Resilience im Google Cloud Platform Marketplace abonniert ist.

6. Kehren Sie zur Seite mit den Zahlungsmethoden für Ransomware Resilience zurück.
7. Um die Lizenz zur Konsole hinzuzufügen, wählen Sie **Lizenz hinzufügen**.



8. Wählen Sie auf der Seite „Lizenz hinzufügen“ die Option „Seriennummer eingeben“ aus. Geben Sie die Seriennummer in der E-Mail ein, die Sie erhalten haben. Wählen Sie **Lizenz hinzufügen**.
9. Um Lizenzdetails anzuzeigen, wählen Sie in der linken Navigation der Konsole **Governance** > **Lizenzen und Abonnements**.
   - Um Abonnementinformationen anzuzeigen, wählen Sie **Abonnements**.
   - Um BYOL-Lizenzen anzuzeigen, wählen Sie **Data Services-Lizenzen**.
10. Zurück zur Ransomware-Resilienz. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz** aus.

    Es wird eine Meldung angezeigt, dass eine Lizenz hinzugefügt wurde.

Bringen Sie Ihre eigene Lizenz mit (BYOL)

Wenn Sie Ihre eigene Lizenz mitbringen möchten (BYOL), müssen Sie die Lizenz erwerben, die NetApp -Lizenzdatei (NLF) abrufen und dann die Lizenz zur Konsole hinzufügen.

Fügen Sie Ihre Lizenzdatei zur Konsole hinzu

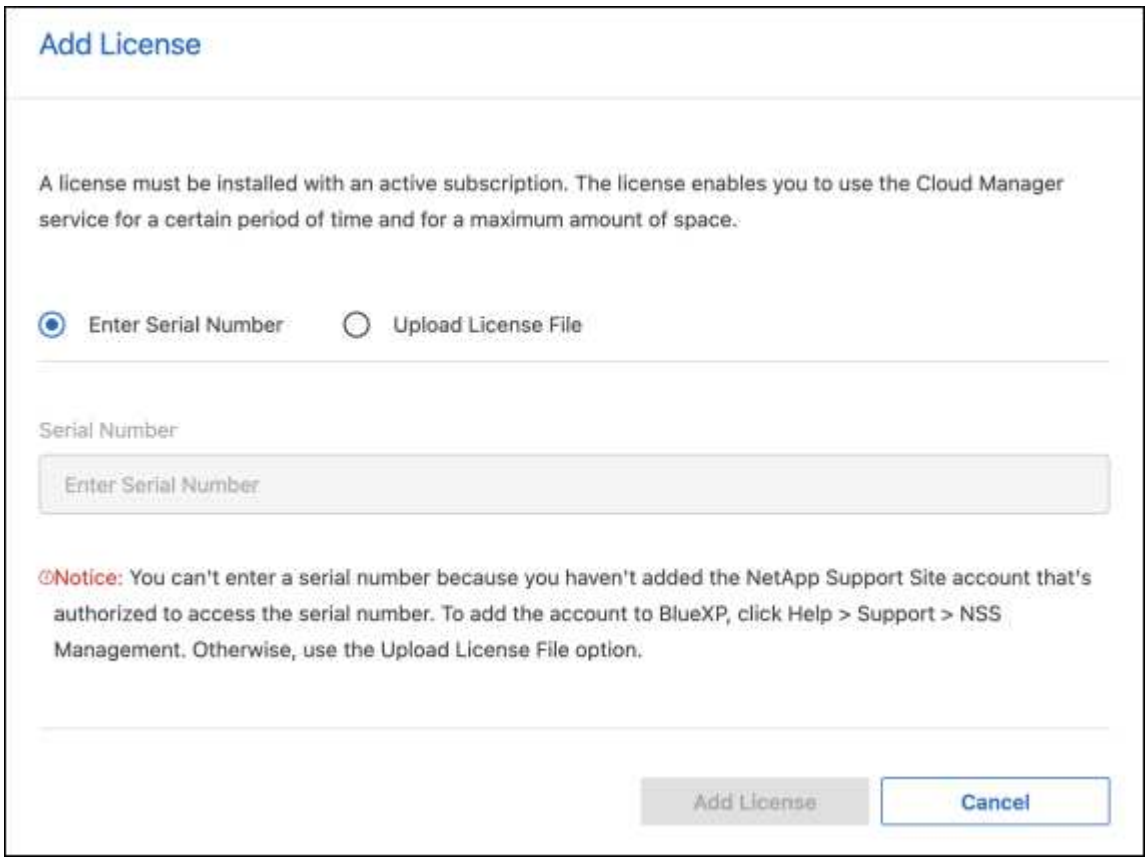
Nachdem Sie Ihre Ransomware Resilience-Lizenz von Ihrem NetApp Vertriebsmitarbeiter erworben haben, aktivieren Sie die Lizenz, indem Sie die Seriennummer von Ransomware Resilience und die Kontoinformationen der NetApp Support Site (NSS) eingeben.

Bevor Sie beginnen

Sie benötigen die Seriennummer von Ransomware Resilience. Suchen Sie diese Nummer in Ihrem Verkaufsauftrag oder wenden Sie sich für diese Informationen an das Kundenteam.

Schritte

1. Nachdem Sie die Lizenz erhalten haben, kehren Sie zu Ransomware Resilience zurück. Wählen Sie oben rechts die Option **Zahlungsmethoden anzeigen**. Oder wählen Sie in der Meldung, dass die kostenlose Testversion abläuft, **Abonnieren oder Lizenz kaufen** aus.
2. Wählen Sie **Lizenz hinzufügen**, um zur Seite „Konsolenlizenzen und -abonnements“ zu gelangen.
3. Wählen Sie auf der Registerkarte **Data Services-Lizenzen** die Option **Lizenz hinzufügen** aus.



4. Geben Sie auf der Seite „Lizenz hinzufügen“ die Seriennummer und die Kontoinformationen der NetApp -Support-Site ein.
   - Wenn Sie die Seriennummer der Konsolenlizenz haben und Ihr NSS-Konto kennen, wählen Sie die Option **Seriennummer eingeben** und geben Sie diese Informationen ein.

     Wenn Ihr NetApp Support Site-Konto nicht in der Dropdown-Liste verfügbar ist, "Fügen Sie das NSS-Konto zur Konsole hinzu" .

   - Wenn Sie über die zvondolr-Lizenzdatei verfügen (erforderlich bei Installation auf einer Dark Site), wählen Sie die Option **Lizenzdatei hochladen** und folgen Sie den Anweisungen zum Anhängen der Datei.
5. Wählen Sie **Lizenz hinzufügen**.

Ergebnis

Auf der Seite „Lizenzen und Abonnements“ wird angezeigt, dass Ransomware Resilience über eine Lizenz verfügt.

Aktualisieren Sie Ihre Konsolenlizenz, wenn sie abläuft

Wenn sich Ihre Lizenzlaufzeit dem Ablaufdatum nähert oder Ihre lizenzierte Kapazität das Limit erreicht, werden Sie in der Ransomware Resilience-Benutzeroberfläche benachrichtigt. Sie können Ihre Ransomware Resilience-Lizenz vor Ablauf aktualisieren, sodass Ihr Zugriff auf die gescannten Daten ohne Unterbrechung möglich ist.

Diese Meldung erscheint auch in Licenses and subscriptions und in "Benachrichtigungseinstellungen" .

Schritte

1. Sie können eine E-Mail an den Support senden, um eine Aktualisierung Ihrer Lizenz anzufordern.

   Nachdem Sie die Lizenz bezahlt haben und sie bei der NetApp -Support-Site registriert ist, aktualisiert die Konsole die Lizenz automatisch. Auf der Seite „Data Services-Lizenzen“ wird die Änderung in 5 bis 10 Minuten angezeigt.

2. Wenn die Konsole die Lizenz nicht automatisch aktualisieren kann, müssen Sie die Lizenzdatei manuell hochladen.
   a. Sie können die Lizenzdatei von der NetApp Support-Site beziehen.
   b. Wählen Sie in der Konsole **Verwaltung** > **Lizenzen und Abonnements**.
   c. Wählen Sie die Registerkarte **Data Services-Lizenzen**, wählen Sie das Symbol **Aktionen …** für die Seriennummer, die Sie aktualisieren, und wählen Sie dann **Lizenz aktualisieren**.

Beenden Sie das PAYGO-Abonnement

Wenn Sie Ihr PAYGO-Abonnement beenden möchten, können Sie dies jederzeit tun.

Schritte

1. Wählen Sie in Ransomware Resilience oben rechts die Lizenzoption aus.
2. Wählen Sie **Zahlungsmethoden anzeigen**.
3. Deaktivieren Sie in den Dropdown-Details das Kontrollkästchen **Nach Ablauf der aktuellen Zahlungsmethode verwenden**.
4. Wählen Sie **Speichern**.

Entdecken Sie Workloads in NetApp Ransomware Resilience

Bevor Sie NetApp Ransomware Resilience verwenden können, müssen zunächst Daten erkannt werden. Während der Erkennung analysiert Ransomware Resilience alle Volumes und Dateien in Systemen über alle Konsolenagenten und Projekte innerhalb einer Organisation hinweg.

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

Was erkennt Ransomware Resilience? Ransomware Resilience bewertet MySQL-Anwendungen, Oracle-Anwendungen, VMware-Datenspeicher, Dateifreigaben und Blockspeicher.

Ransomware Resilience erkennt keine Workloads mit Volumes, die FlexGroup verwenden.

Ransomware Resilience erkennt und zeigt sowohl unterstützte als auch nicht unterstützte Systemkonfigurationen im Dashboard an.

Ransomware Resilience überprüft Ihren aktuellen Backup-Schutz, Snapshot-Kopien und die Optionen für den autonomen Ransomware-Schutz von NetApp . Anschließend werden Ihnen Möglichkeiten zur Verbesserung Ihres Ransomware-Schutzes empfohlen.

Wie können Sie Arbeitslasten ermitteln? Sie können Folgendes tun:

- Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten. Sie können von dieser Funktion profitieren, wenn Sie bestimmte Workloads in Ihrer Umgebung schützen möchten und andere nicht.
- Entdecken Sie neu erstellte Workloads für zuvor ausgewählte Systeme.
- Entdecken Sie neue Systeme.

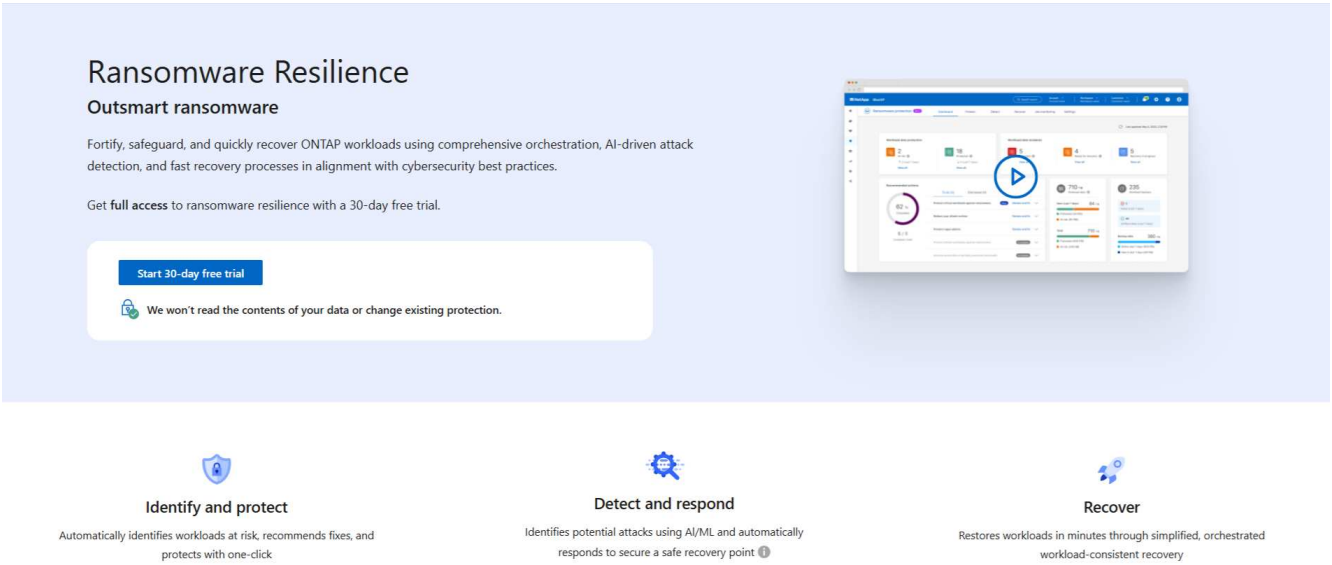
Auswählen von Workloads zum Erkennen und Schützen

Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten.

Schritte

1. Wählen Sie in der NetApp Konsole **Schutz** > **Ransomware-Schutz**.

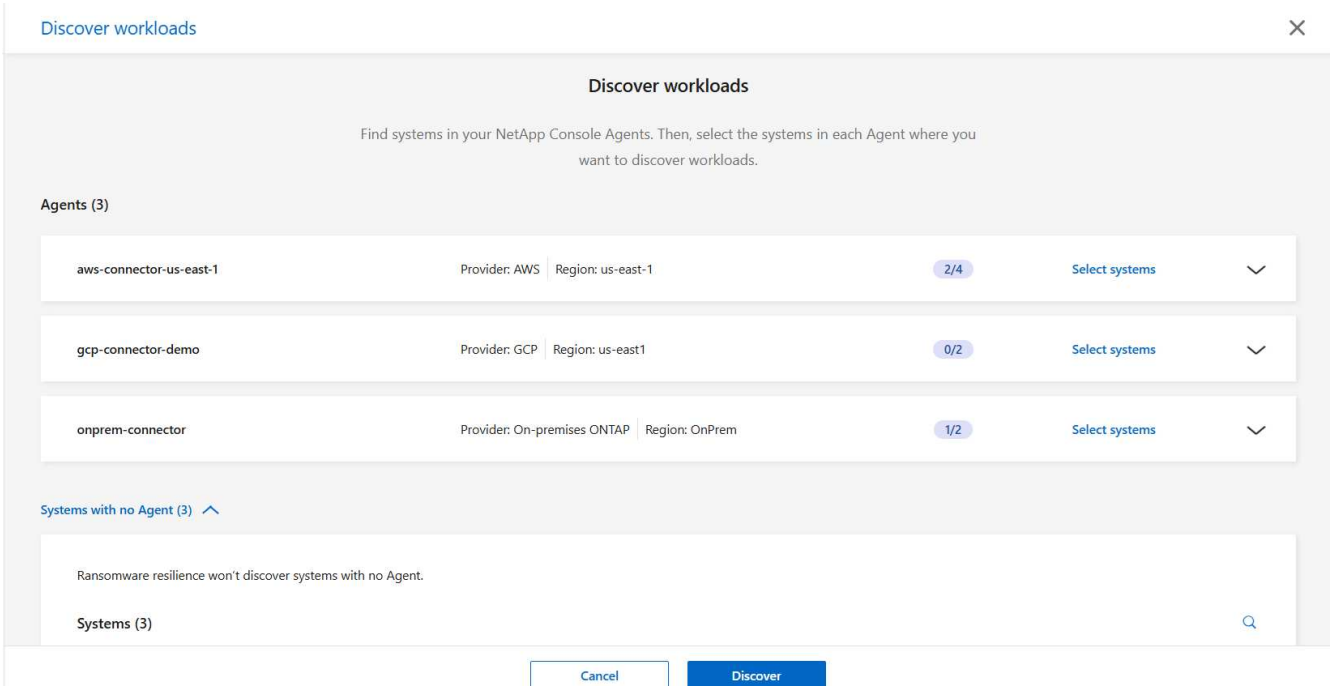
   Wenn dies Ihre erste Anmeldung ist, wird die Zielseite angezeigt.



   Wenn Sie die kostenlose Testversion gestartet haben, ändert sich die Beschriftung der Schaltfläche **30-tägige kostenlose Testversion starten** in **Mit der Ermittlung von Workloads beginnen**.

2. Wählen Sie auf der ersten Zielseite **Beginnen Sie mit der Ermittlung von Workloads** aus.

   Ransomware Resilience findet sowohl unterstützte als auch nicht unterstützte Systeme. Dieser Vorgang kann einige Minuten dauern.

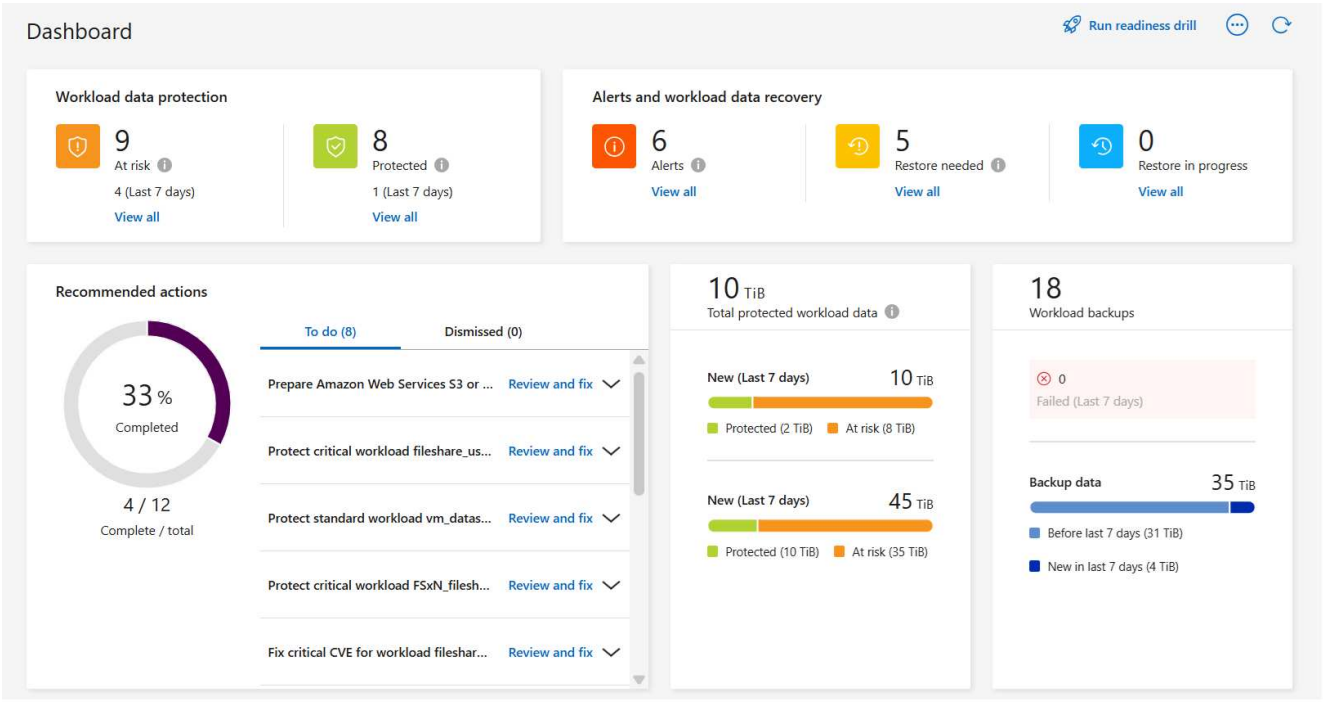


3. Um Workloads für einen bestimmten Konsolenagenten zu ermitteln, wählen Sie **Systeme auswählen** neben dem Konsolenagenten aus, für den Sie Workloads ermitteln möchten.
4. Wählen Sie die Systeme aus, auf denen Sie Workloads ermitteln möchten.
5. Wählen Sie **Entdecken**.

   Ransomware Resilience erkennt Workload-Daten nur für die Konsolenagenten mit ausgewählten Systemen. Dieser Vorgang kann einige Minuten dauern.

6. Um die Liste der erkannten Workloads herunterzuladen, wählen Sie **Ergebnisse herunterladen**.
7. Um das Ransomware Resilience-Dashboard anzuzeigen, wählen Sie **Zum Dashboard gehen**.

   Das Dashboard zeigt den Datenschutzzustand an. Die Anzahl der gefährdeten oder geschützten Workloads wird aktualisiert, wenn neue Workloads erkannt werden.



"Erfahren Sie, was Ihnen das Dashboard anzeigt."

Entdecken Sie neu erstellte Workloads für zuvor ausgewählte Systeme

Wenn Sie bereits Systeme zur Erkennung ausgewählt haben, können Sie über das Dashboard neu erstellte Workloads für diese Umgebungen erkennen.

Schritte

1. Um das Datum der letzten Entdeckung zu ermitteln, sehen Sie sich den Datums- und Zeitstempel neben dem Symbol **Aktualisieren** oben rechts im Ransomware Resilience-Dashboard an.
2. Wählen Sie im Dashboard das **Aktualisierungssymbol** aus, um neue Workloads zu finden.

Entdecken Sie neue Systeme

Wenn Sie bereits Systeme entdeckt haben, können Sie neue oder bisher nicht ausgewählte Systeme finden.

Schritte

1. Wählen Sie im Menü Ransomware Resilience die vertikale … Option oben rechts. Wählen Sie im Dropdown-Menü **Einstellungen** aus.
2. Wählen Sie auf der Workload-Erkennungskarte **Workloads erkennen** aus.

   Dieser Vorgang kann einige Minuten dauern und ein Ladesymbol zeigt den Fortschritt an.

3. Ransomware Resilience erkennt sowohl unterstützte als auch nicht unterstützte Systeme. Ransomware Resilience unterstützt ein System nicht, wenn seine ONTAP Version unter der erforderlichen Version liegt. Wenn Sie mit der Maus über ein nicht unterstütztes System fahren, wird in einem Tooltip der Grund angezeigt. Wählen Sie die Systeme aus, auf denen Sie Workloads ermitteln möchten.
4. Wählen Sie **Entdecken**.

Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe in NetApp Ransomware Resilience durch

Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch, indem Sie einen Angriff auf eine neue Beispiel-Workload simulieren. Untersuchen Sie den simulierten Angriff und stellen Sie die Arbeitslast wieder her. Verwenden Sie diese Funktion, um Warnbenachrichtigungen, Reaktionen und Wiederherstellungen zu testen. Führen Sie die Übung so oft wie nötig durch.

Ihre tatsächlichen Arbeitslastdaten sind davon nicht betroffen.

Sie können Bereitschaftsübungen für NFS- und CIFS-Workloads (SMB) durchführen.

Konfigurieren Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe

Bevor Sie eine Simulation ausführen, richten Sie auf der Seite „Einstellungen“ eine Übung ein. Greifen Sie über die Option „Aktionen“ im oberen Menü auf die Seite „Einstellungen“ zu.

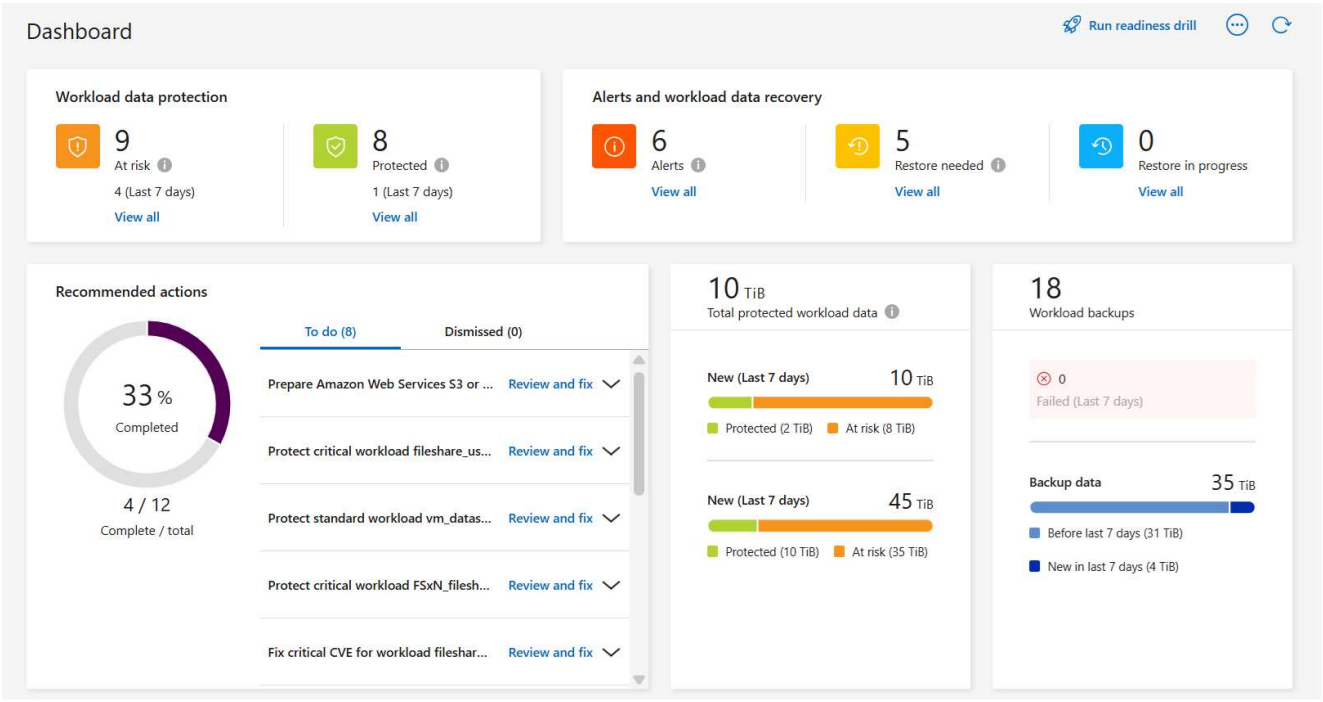
In den folgenden Situationen müssen Sie einen Benutzernamen und ein Kennwort eingeben:

- Wenn für die zuvor ausgewählte Storage-VM Änderungen am Benutzernamen oder Passwort vorgenommen wurden
- Wenn Sie eine andere CIFS (SMB)-Speicher-VM auswählen
- Wenn Sie einen anderen Test-Workload-Namen eingeben

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

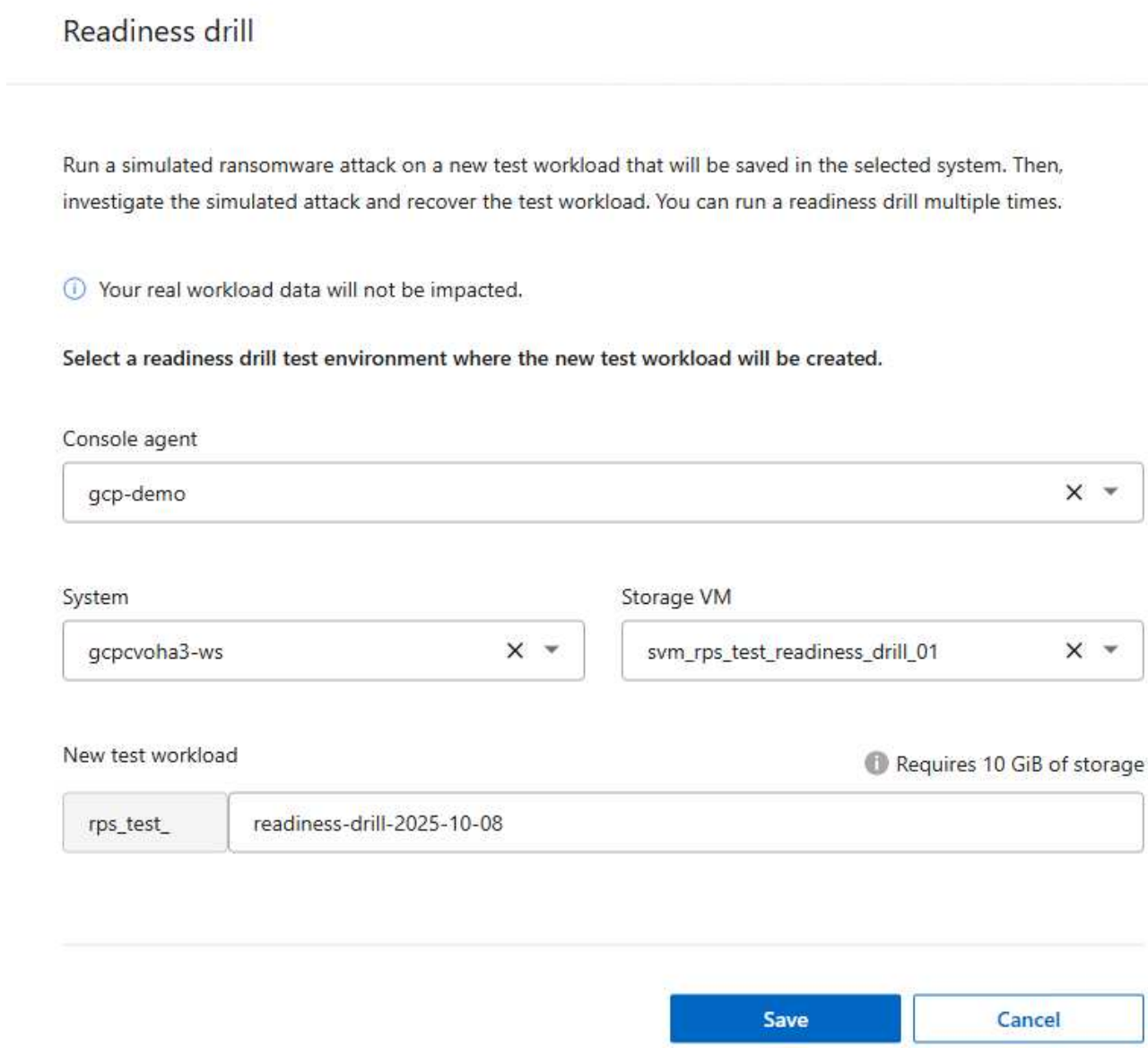
Schritte

1. Wählen Sie im NetApp Ransomware Resilience-Menü oben rechts die Schaltfläche **Bereitschaftsübung ausführen**.



2. Wählen Sie auf der Seite „Einstellungen“ in der Karte „Bereitschaftsübung“ die Option „Konfigurieren“ aus.

   Die Konsole zeigt die Seite „Bereitschaftsübung konfigurieren“ an.



3. Gehen Sie folgendermaßen vor:
   a. Wählen Sie den Konsolenagenten aus, den Sie für die Bereitschaftsübung verwenden möchten.
   b. Wählen Sie ein Testsystem aus.
   c. Wählen Sie eine Testspeicher-SVM aus.
   d. Wenn Sie eine CIFS (SMB)-Speicher-VM ausgewählt haben, werden die Felder **Benutzername** und **Passwort** angezeigt. Geben Sie den Benutzernamen und das Kennwort für die Speicher-VM ein.
   e. Geben Sie den Namen einer neuen Test-Workload ein, die erstellt werden soll. Der Name darf keine Bindestriche enthalten.
4. Wählen Sie **Speichern**.

Sie können die Konfiguration der Bereitschaftsübung später auf der Seite „Einstellungen“ bearbeiten.

Starten Sie eine Bereitschaftsübung

Nachdem Sie die Bereitschaftsübung konfiguriert haben, können Sie mit der Übung beginnen.

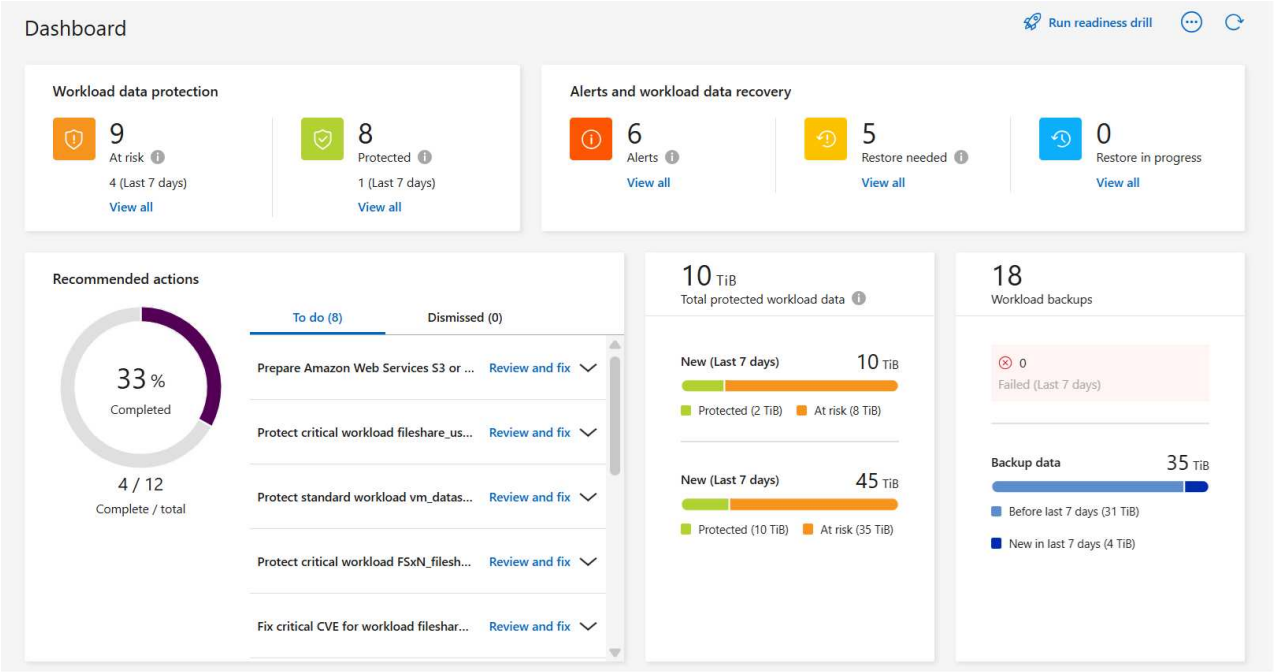
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

Wenn Sie die Bereitschaftsübung starten, überspringt Ransomware Resilience den Lernmodus und startet die Übung im aktiven Modus. Der Erkennungsstatus der Arbeitslast ist „Aktiv“.

Eine Arbeitslast kann den Status „Lernmodus“ zur Ransomware-Erkennung haben, wenn vor Kurzem eine Erkennungsrichtlinie zugewiesen wurde und Ransomware Resilience Arbeitslasten scannt.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie im Menü „Ransomware Resilience“ oben rechts die Schaltfläche „Bereitschaftsübung ausführen“ aus.



   - ODER wählen Sie auf der Seite „Einstellungen“ in der Karte „Bereitschaftsübung“ die Option „Start“ aus.
2. Wenn Sie die Bereitschaftsübung bereits konfiguriert haben, beginnt sie nach Auswahl von **Start**.

Nachdem die Übung begonnen hat, können Sie die Konfiguration der Bereitschaftsübung nicht mehr bearbeiten. Sie können es zurücksetzen, um erneut zu starten.

Auf einen Alarm einer Bereitschaftsübung reagieren

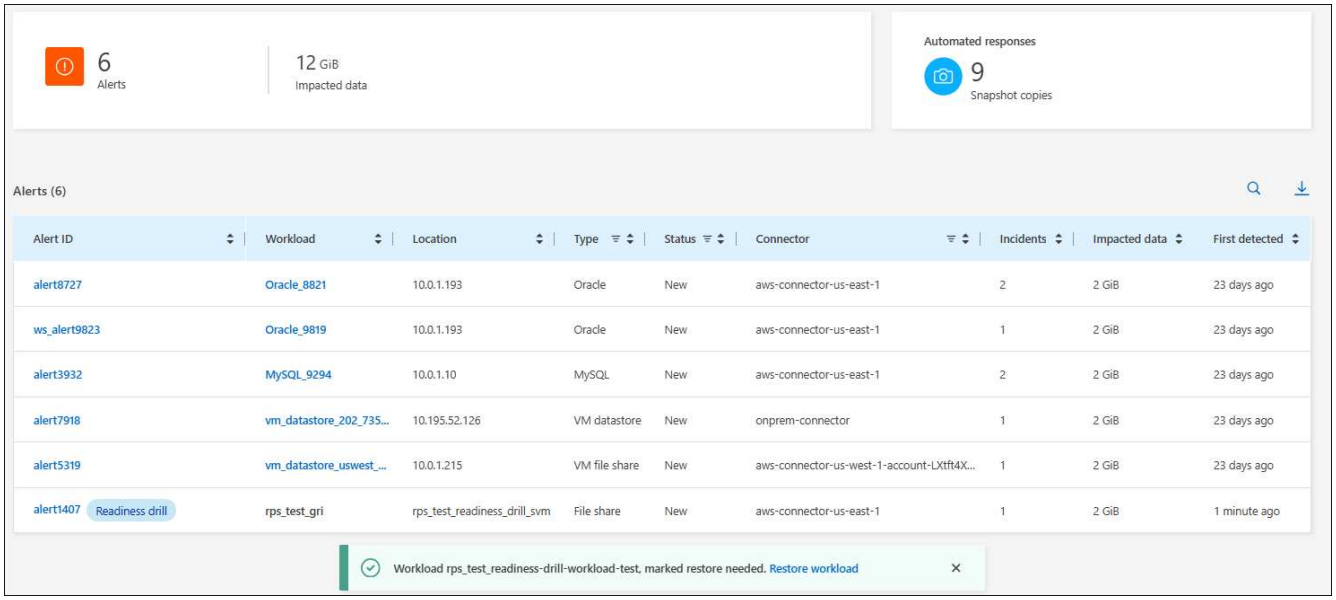
Testen Sie Ihre Bereitschaft, indem Sie auf eine Bereitschaftsübungswarnung reagieren.

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

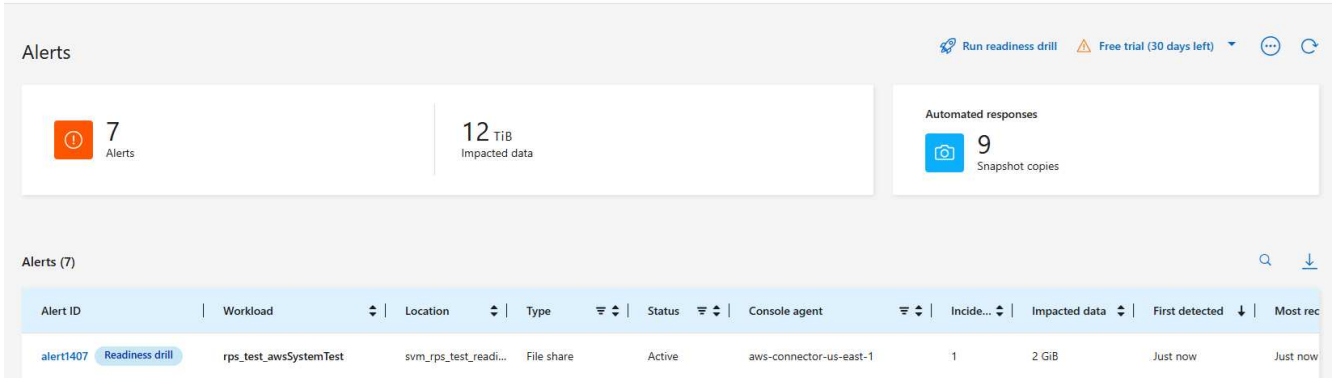
Schritte

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

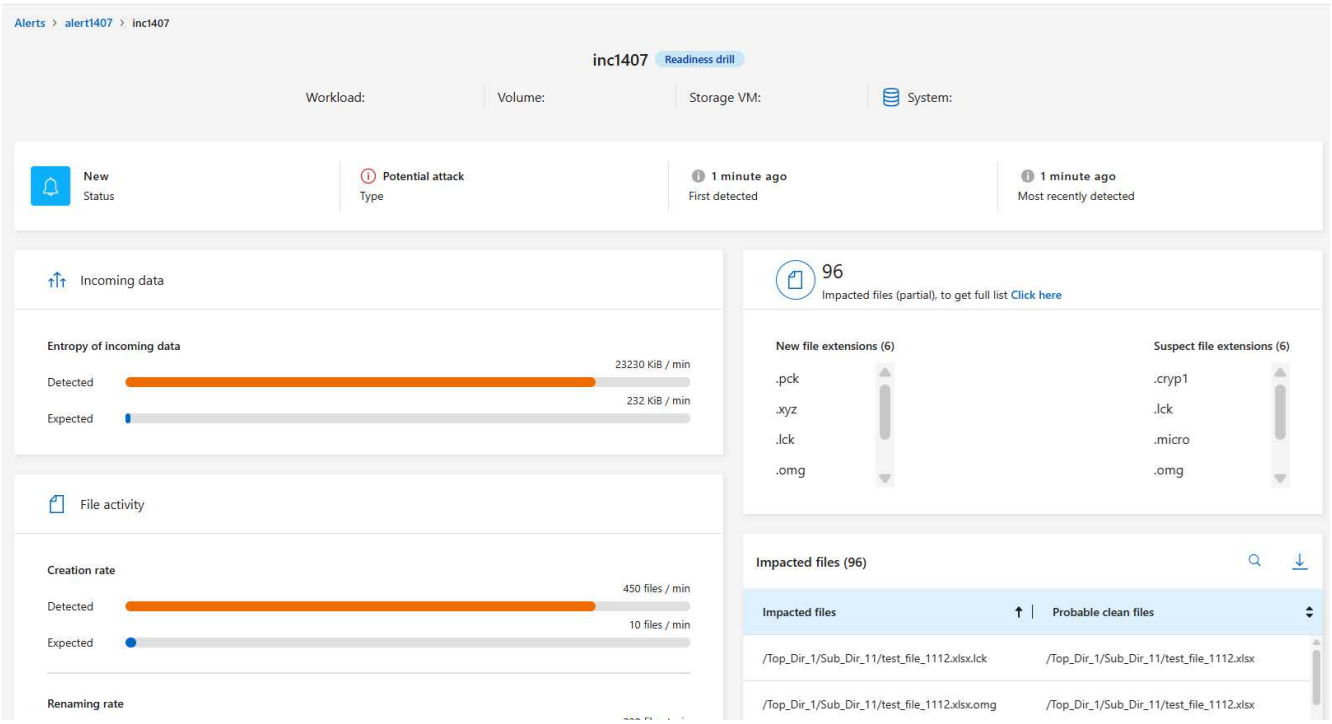
   Die Konsole zeigt die Seite „Warnungen“ an. In der Spalte „Alarm-ID“ sehen Sie neben der ID „Bereitschaftsübung“.



2. Wählen Sie den Alarm mit der Angabe „Bereitschaftsübung“ aus. Auf der Detailseite der Warnungen wird eine Liste der Vorfallwarnungen angezeigt.



3. Überprüfen Sie die Alarmvorfälle.
4. Wählen Sie einen Alarmvorfall aus.



Hier sind einige Dinge, auf die Sie achten sollten:

- Sehen Sie sich die potenzielle Schwere des Angriffs an.

  Wenn der Schweregrad darauf hindeutet, dass ein Benutzer böswilliger Aktivitäten verdächtigt wird, überprüfen Sie den Benutzernamen. Sie können auch"den Benutzer blockieren."

- Sehen Sie sich die Dateiaktivität und verdächtigen Prozesse an:
  - Vergleichen Sie die eingehenden erkannten Daten mit den erwarteten Daten.
  - Sehen Sie sich die Erstellungsrate der erkannten Dateien im Vergleich zur erwarteten Rate an.
  - Sehen Sie sich die erkannte Dateiumbenennungsrate im Vergleich zur erwarteten Rate an.
  - Vergleichen Sie die Löschrate mit der erwarteten Rate.
- Sehen Sie sich die Liste der betroffenen Dateien an. Sehen Sie sich die Erweiterungen an, die den Angriff verursachen könnten.
- Bestimmen Sie die Auswirkungen und das Ausmaß des Angriffs, indem Sie die Anzahl der betroffenen Dateien und Verzeichnisse überprüfen.

Wiederherstellen der Test-Workload

Stellen Sie nach der Überprüfung der Warnung zur Bereitschaftsübung bei Bedarf die Testarbeitslast wieder her.

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

Schritte

1. Kehren Sie zur Seite mit den Alarmdetails zurück.

2. Wenn die Test-Workload wiederhergestellt werden soll, gehen Sie wie folgt vor:
   - Wählen Sie **Als Wiederherstellung erforderlich markieren**.
   - Überprüfen Sie die Bestätigung und wählen Sie im Bestätigungsfeld **Als Wiederherstellung erforderlich markieren** aus.
     - Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
     - Wählen Sie den mit „Readiness Drill“ gekennzeichneten Test-Workload aus, den Sie wiederherstellen möchten.
     - Wählen Sie **Wiederherstellen**.
     - Geben Sie auf der Seite „Wiederherstellen“ Informationen zur Wiederherstellung ein:
   - Wählen Sie die Quell-Snapshot-Kopie aus.
   - Wählen Sie das Zielvolume aus.
3. Wählen Sie auf der Überprüfungsseite der Wiederherstellung **Wiederherstellen** aus.

   Die Konsole zeigt den Status der Wiederherstellung der Bereitschaftsübung auf der Wiederherstellungsseite als „In Bearbeitung“ an.

   Nachdem die Wiederherstellung abgeschlossen ist, ändert die Konsole den Status der Arbeitslast in **Wiederhergestellt**.

4. Überprüfen Sie die wiederhergestellte Arbeitslast.

Einzelheiten zum Wiederherstellungsvorgang finden Sie unter"Wiederherstellung nach einem Ransomware-Angriff (nachdem die Vorfälle neutralisiert wurden)" .

Ändern Sie den Alarmstatus nach der Bereitschaftsübung

Nachdem Sie die Warnung zur Bereitschaftsübung überprüft und die Arbeitslast wiederhergestellt haben, ändern Sie bei Bedarf den Warnungsstatus.

Die Konsolenrolle ist erforderlich Organisationsadministrator, Ordner- oder Projektadministrator oder Ransomware-Resilience-Administrator. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

Schritte

1. Kehren Sie zur Seite mit den Alarmdetails zurück.
2. Wählen Sie die Warnung erneut aus.
3. Geben Sie den Status an, indem Sie **Status bearbeiten** auswählen und den Status in einen der folgenden Werte ändern:
   - Abgelehnt: Wenn Sie vermuten, dass es sich bei der Aktivität nicht um einen Ransomware-Angriff handelt, ändern Sie den Status in „Abgelehnt“.

     Nachdem Sie einen Angriff abgewehrt haben, können Sie ihn nicht mehr rückgängig machen. Wenn Sie eine Arbeitslast ablehnen, werden alle Snapshot-Kopien, die automatisch als Reaktion auf den potenziellen Ransomware-Angriff erstellt wurden, dauerhaft gelöscht. Wenn Sie den Alarm verwerfen, gilt die Bereitschaftsübung als abgeschlossen.

   - Behoben: Der Vorfall wurde entschärft.

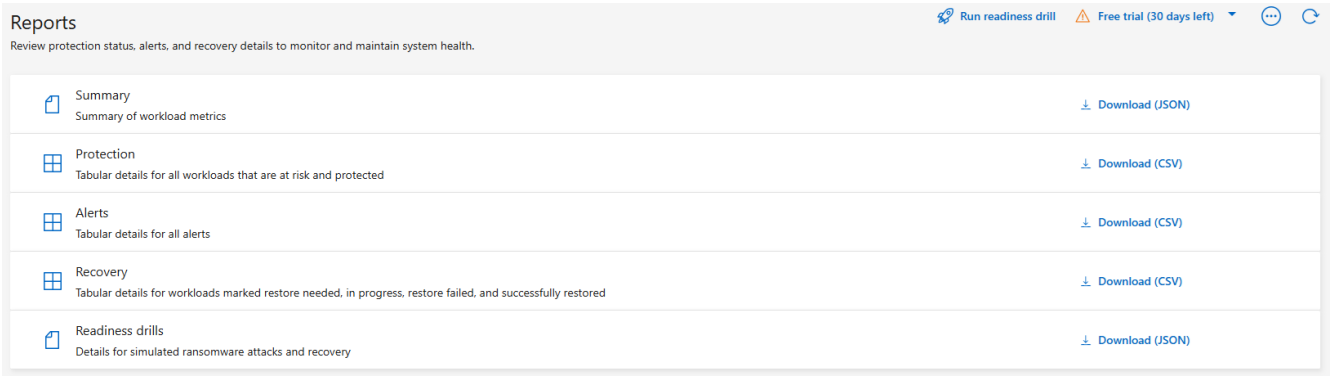
Überprüfen Sie die Berichte zur Bereitschaftsübung

Nachdem die Bereitschaftsübung abgeschlossen ist, möchten Sie möglicherweise einen Bericht über die Übung überprüfen und speichern.

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 BlueXP -Zugriffsrollen für alle Dienste" .

Schritte

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



2. Wählen Sie **Bereitschaftsübungen** und **Herunterladen**, um den Bericht zur Bereitschaftsübung herunterzuladen.

Konfigurieren der Schutzeinstellungen in NetApp Ransomware Resilience

Sie können Sicherungsziele konfigurieren, Daten an ein externes Sicherheits- und Ereignismanagementsystem (SIEM) senden, eine Übung zur Angriffsbereitschaft durchführen, die Workload-Erkennung konfigurieren oder die Erkennung verdächtiger Benutzeraktivitäten konfigurieren, indem Sie auf die Option **Einstellungen** zugreifen.

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

Was können Sie auf der Einstellungsseite tun? Auf der Seite „Einstellungen“ können Sie Folgendes tun:

- Simulieren Sie einen Ransomware-Angriff, indem Sie eine Bereitschaftsübung durchführen und auf eine simulierte Ransomware-Warnung reagieren. Weitere Informationen finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .
- Konfigurieren Sie die Workload-Erkennung.
- Konfigurieren Sie die Meldung verdächtiger Benutzeraktivitäten.
- Fügen Sie ein Sicherungsziel hinzu.
- Verbinden Sie Ihr Sicherheits- und Ereignismanagementsystem (SIEM) zur Bedrohungsanalyse und -erkennung. Durch die Aktivierung der Bedrohungserkennung werden automatisch Daten zur Bedrohungsanalyse an Ihr SIEM gesendet.

Greifen Sie direkt auf die Seite „Einstellungen“ zu

Sie können die Seite „Einstellungen“ ganz einfach über die Option „Aktionen“ im oberen Menü aufrufen.

1. Wählen Sie unter „Ransomware-Resilienz“ die vertikale  … Option oben rechts.
2. Wählen Sie im Dropdown-Menü **Einstellungen** aus.

Simulieren Sie einen Ransomware-Angriff

Führen Sie eine Ransomware-Bereitschaftsübung durch, indem Sie einen Ransomware-Angriff auf eine neu erstellte Beispiel-Workload simulieren. Untersuchen Sie dann den simulierten Angriff und stellen Sie die Beispiel-Arbeitslast wieder her. Mithilfe dieser Funktion können Sie durch das Testen von Warnbenachrichtigungen, Reaktions- und Wiederherstellungsprozessen sicherstellen, dass Sie im Falle eines tatsächlichen Ransomware-Angriffs vorbereitet sind. Sie können eine Ransomware-Bereitschaftsübung mehrmals durchführen.

Weitere Einzelheiten finden Sie unter"Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Konfigurieren der Workload-Erkennung

Sie können die Workload-Erkennung so konfigurieren, dass neue Workloads in Ihrer Umgebung automatisch erkannt werden.

1. Suchen Sie auf der Seite „Einstellungen“ nach der Kachel „Workload-Erkennung“.
2. Wählen Sie in der Kachel **Workload-Erkennung** die Option **Workloads erkennen** aus.

   Auf dieser Seite werden Konsolenagenten mit Systemen angezeigt, die zuvor nicht ausgewählt wurden, neu verfügbare Konsolenagenten und neu verfügbare Systeme. Auf dieser Seite werden die zuvor ausgewählten Systeme nicht angezeigt.

3. Wählen Sie den Konsolenagenten aus, bei dem Sie Workloads ermitteln möchten.
4. Überprüfen Sie die Liste der Systeme.
5. Markieren Sie die Systeme, auf denen Sie Workloads ermitteln möchten, oder aktivieren Sie das Kontrollkästchen oben in der Tabelle, um Workloads in allen ermittelten Workloadumgebungen zu ermitteln.
6. Tun Sie dies bei Bedarf für andere Systeme.
7. Wählen Sie **Erkennen** aus, damit Ransomware Resilience automatisch neue Workloads im ausgewählten Konsolenagenten erkennt.

Verdächtige Benutzeraktivität

Auf der Benutzeraktivitätskarte können Sie den Benutzeraktivitätsagenten erstellen und verwalten, der zum Erkennen verdächtiger Benutzeraktivitäten erforderlich ist.

Weitere Informationen finden Sie unter "Verdächtige Benutzeraktivität" .

Hinzufügen eines Sicherungsziels

Ransomware Resilience kann Workloads identifizieren, für die noch keine Backups vorhanden sind, sowie Workloads, denen noch keine Backup-Ziele zugewiesen sind.

Um diese Workloads zu schützen, sollten Sie ein Sicherungsziel hinzufügen. Sie können eines der folgenden Sicherungsziele auswählen:

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

Für Workloads in Amazon FSx for NetApp ONTAP sind keine Sicherungsziele verfügbar. Führen Sie Sicherungsvorgänge mit dem FSx for ONTAP -Sicherungsdienst durch.

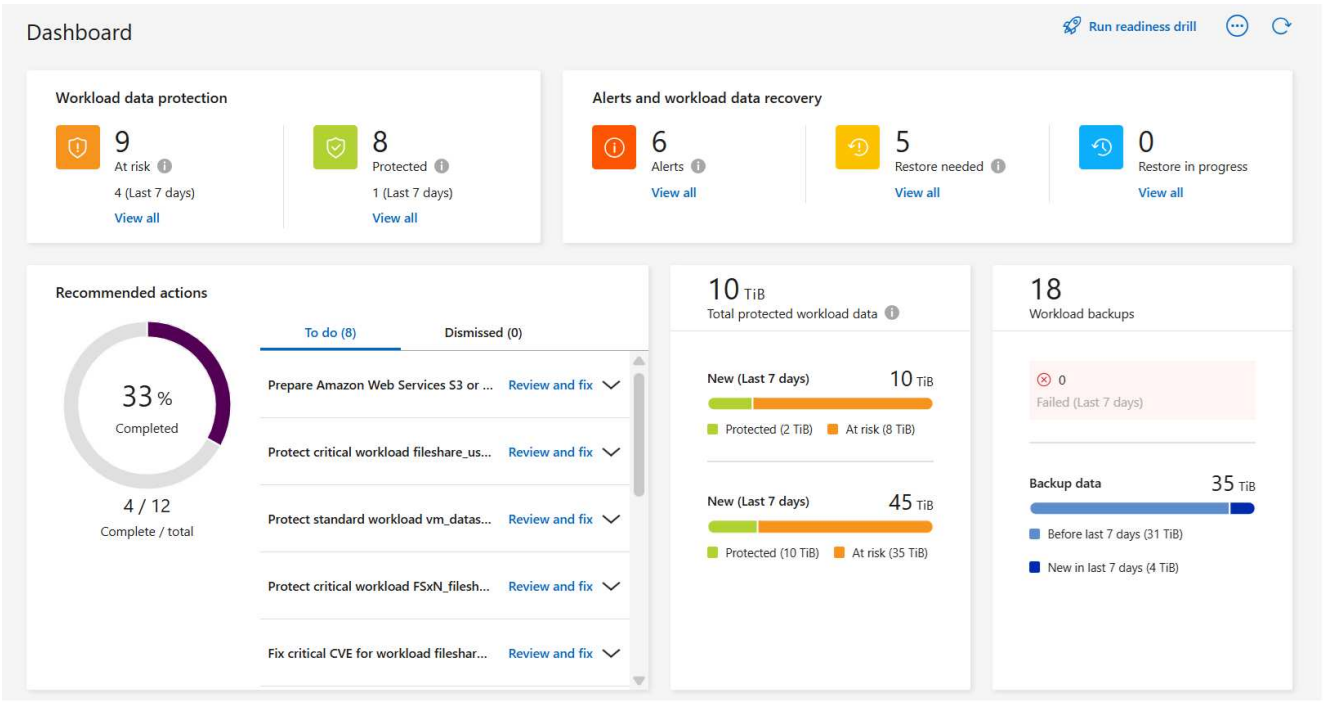
Sie können ein Sicherungsziel basierend auf einer empfohlenen Aktion vom Dashboard oder durch Zugriff auf die Option „Einstellungen“ im Menü hinzufügen.

Greifen Sie über die empfohlenen Aktionen des Dashboards auf die Optionen für das Sicherungsziel zu

Das Dashboard bietet viele Empfehlungen. Eine Empfehlung könnte darin bestehen, ein Sicherungsziel zu konfigurieren.

Schritte

1. Überprüfen Sie im Dashboard „Ransomware Resilience“ den Bereich „Empfohlene Maßnahmen“.



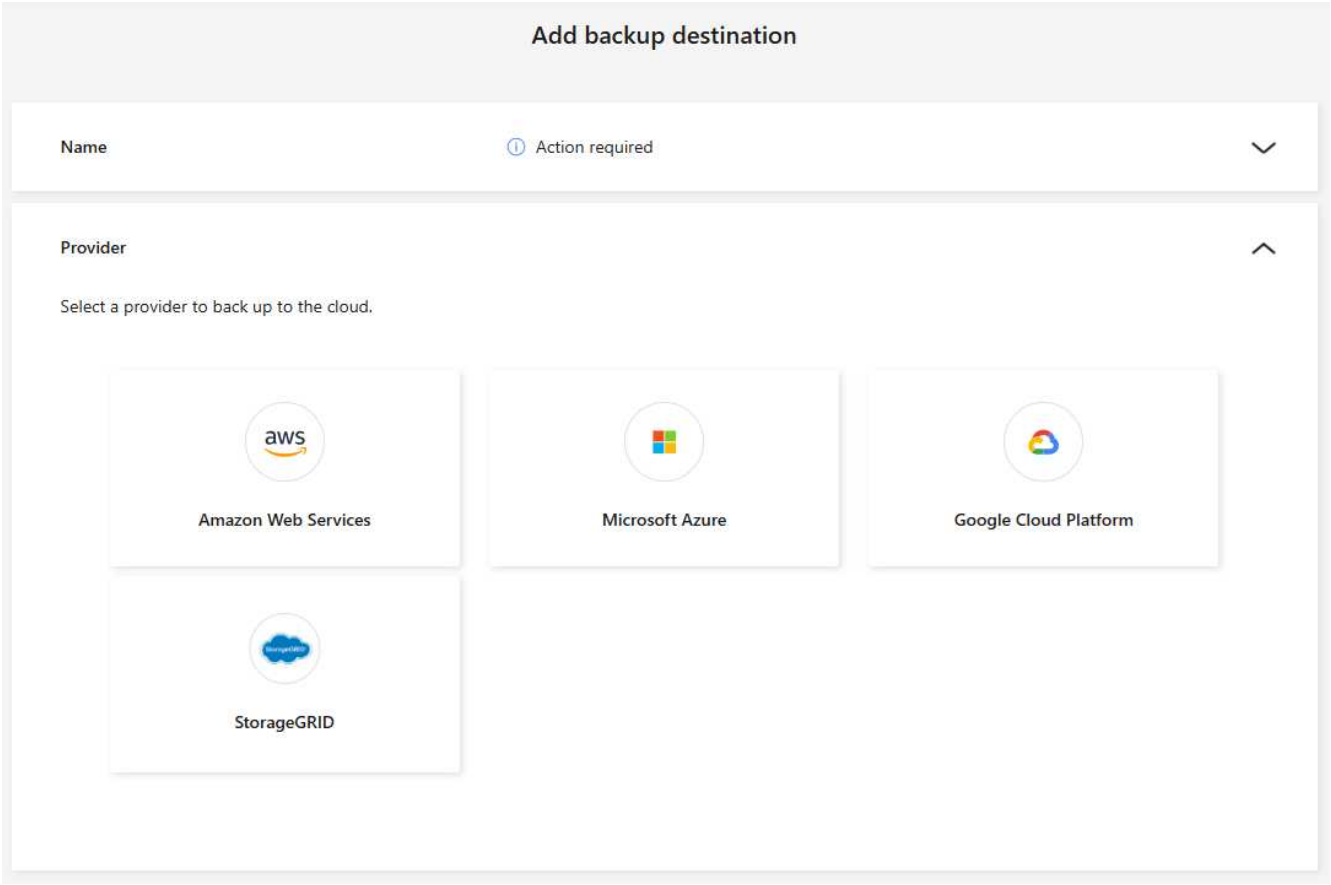
2. Wählen Sie im Dashboard **Überprüfen und beheben** für die Empfehlung „<Sicherungsanbieter> als Sicherungsziel vorbereiten“.
3. Fahren Sie je nach Backup-Anbieter mit den Anweisungen fort.

StorageGRID als Backup-Ziel hinzufügen

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

Schritte

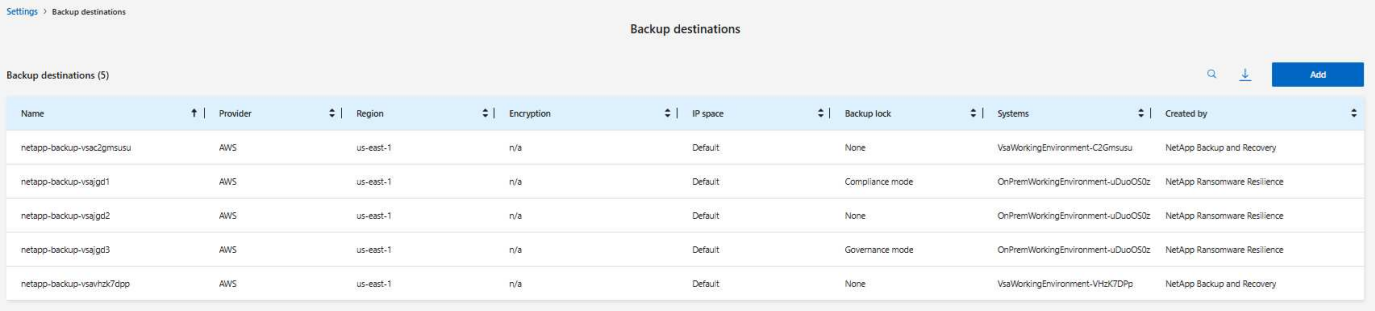
1. Wählen Sie auf der Seite **Einstellungen > Sicherungsziele** die Option **Hinzufügen** aus.
2. Geben Sie einen Namen für das Sicherungsziel ein.



3. Wählen Sie * StorageGRID*.
4. Wählen Sie den Abwärtspfeil neben jeder Einstellung aus und geben Sie Werte ein oder wählen Sie sie aus:
   - **Anbietereinstellungen**:
     - Erstellen Sie einen neuen Bucket oder bringen Sie Ihren eigenen Bucket mit, in dem die Backups gespeichert werden.
     - Vollqualifizierter Domänenname, Port, StorageGRID Zugriffsschlüssel und geheime Schlüsselanmeldeinformationen des StorageGRID Gateway-Knotens.
   - **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.
5. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.



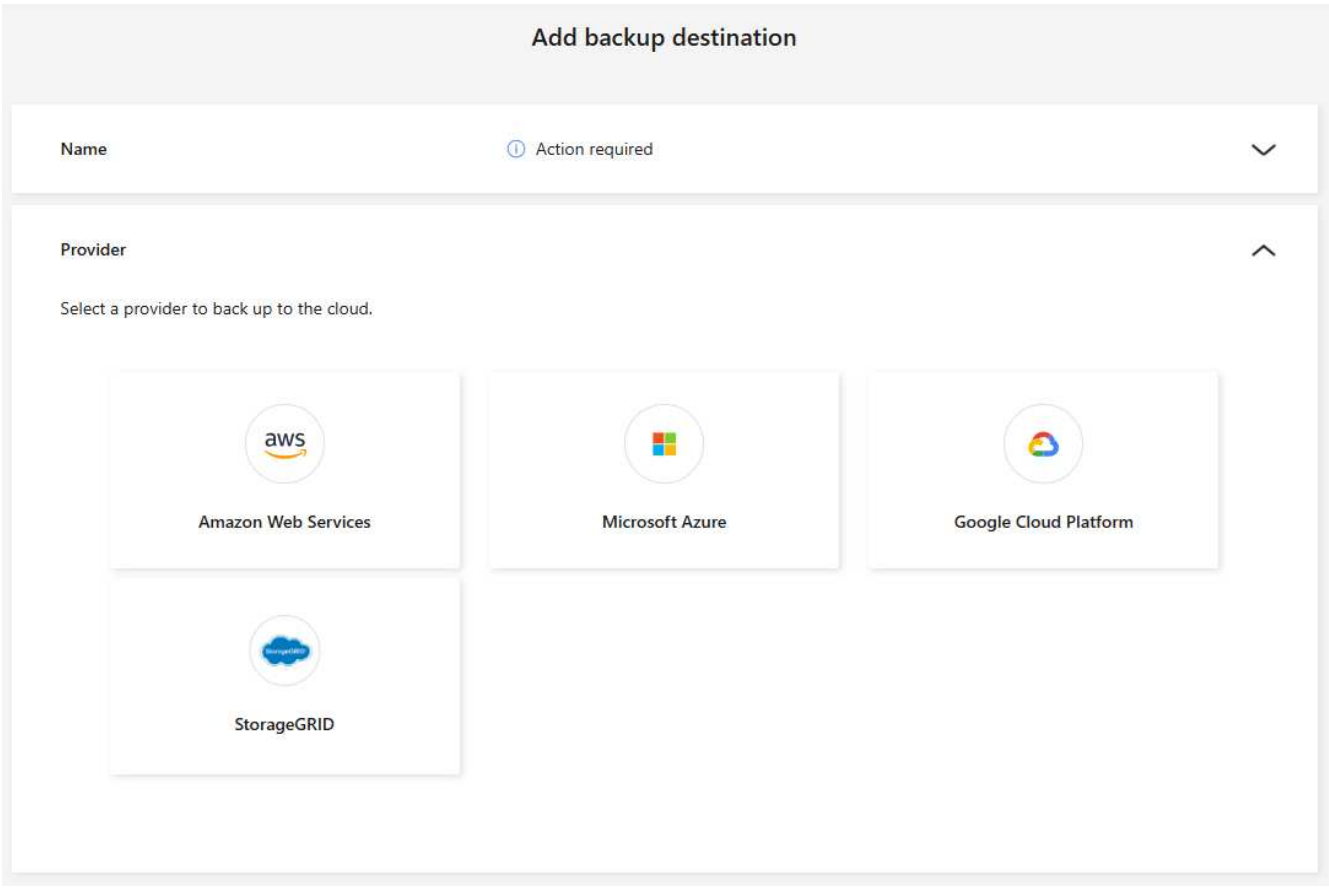
Amazon Web Services als Sicherungsziel hinzufügen

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. Wählen Sie auf der Seite **Einstellungen > Sicherungsziele** die Option **Hinzufügen** aus.
2. Geben Sie einen Namen für das Sicherungsziel ein.



3. Wählen Sie **Amazon Web Services** aus.
4. 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.

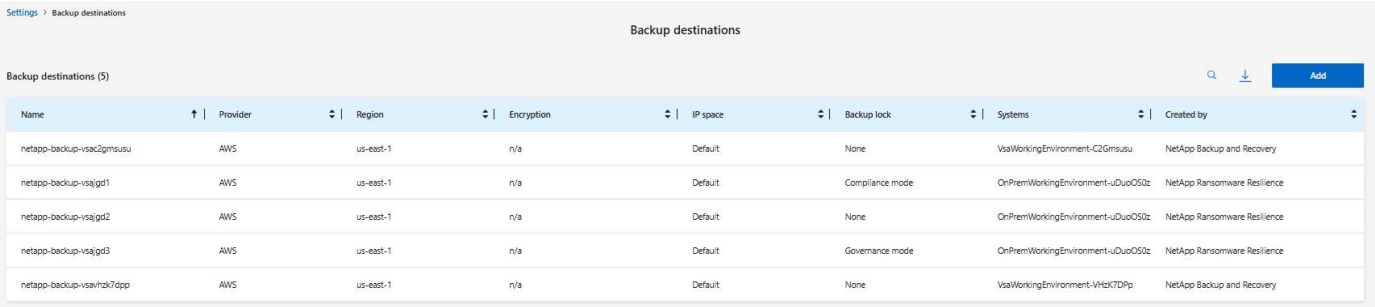
Wenn Sie die Sicherungssperreinstellung jetzt konfigurieren, können Sie die Einstellung später nicht mehr ändern, nachdem das Sicherungsziel konfiguriert wurde.

- **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.

5. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.



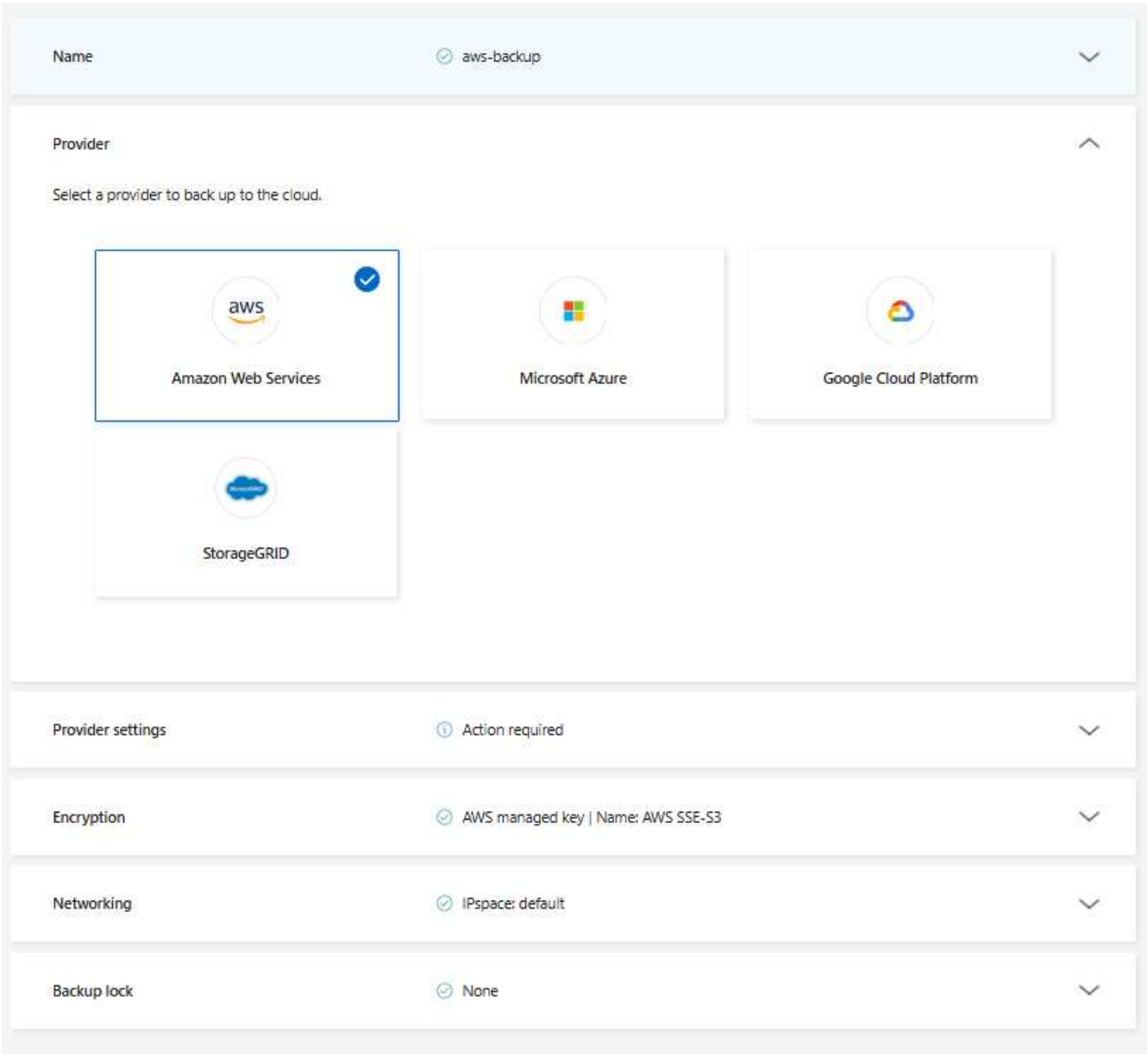
Google Cloud Platform als Backup-Ziel hinzufügen

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. Wählen Sie auf der Seite **Einstellungen > Sicherungsziele** die Option **Hinzufügen** aus.
2. Geben Sie einen Namen für das Sicherungsziel ein.



3. Wählen Sie **Google Cloud Platform** aus.
4. Wählen Sie den Abwärtspfeil neben jeder Einstellung aus und geben Sie Werte ein oder wählen Sie sie aus:
   - **Anbietereinstellungen**:
     - Erstellen Sie einen neuen Bucket. Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel

ein.

- Geben Sie Ihr Google Cloud Platform-Projekt und Ihre Region ein oder wählen Sie sie aus.

◦ **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 weiterhin von Google verwaltete Schlüssel 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 GCP-Endpunkt (PrivateLink) verwenden möchten.

5. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.

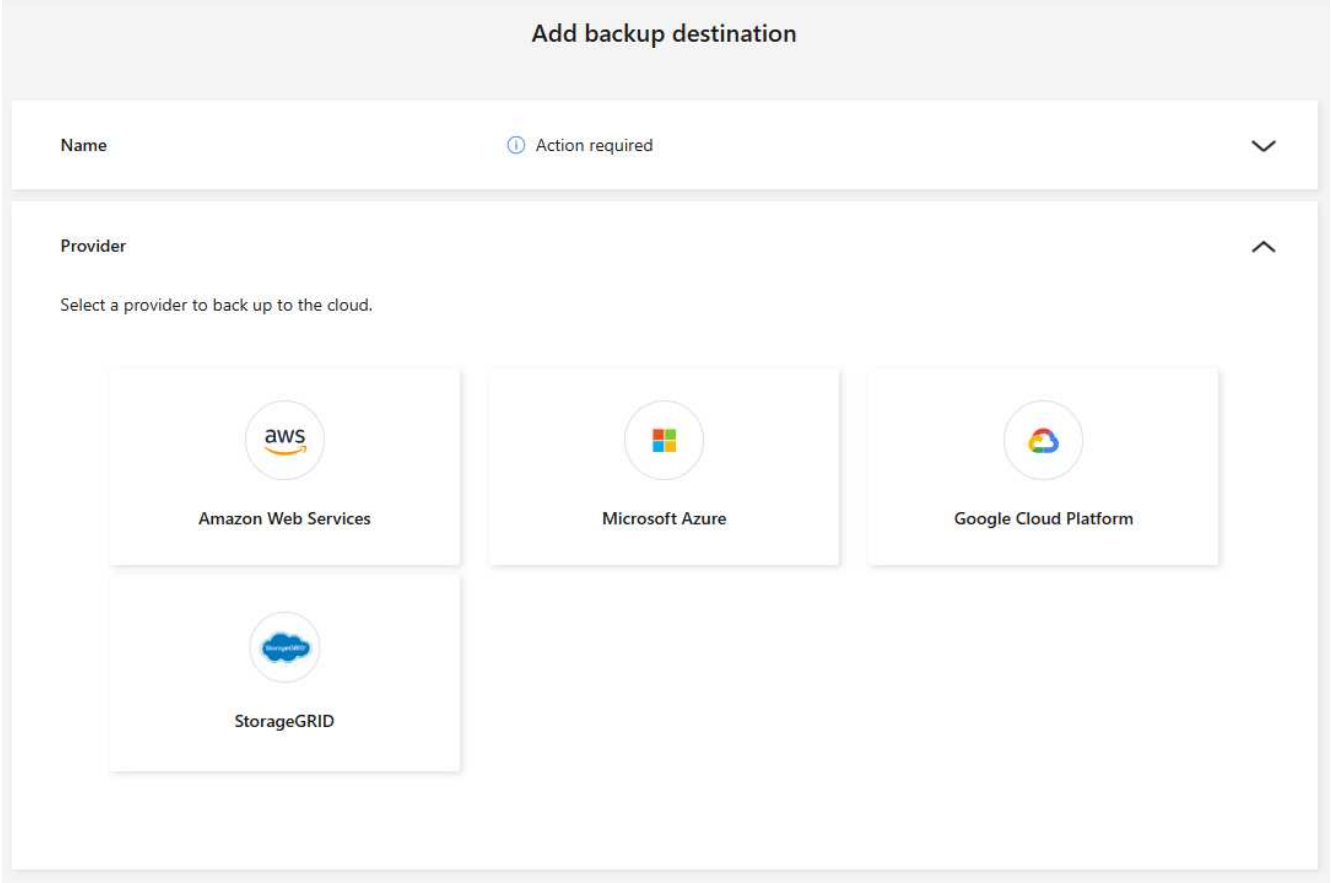
Microsoft Azure als Sicherungsziel hinzufügen

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. Wählen Sie auf der Seite **Einstellungen > Sicherungsziele** die Option **Hinzufügen** aus.
2. Geben Sie einen Namen für das Sicherungsziel ein.



3. Wählen Sie **Azure** aus.
4. 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.
     - Azure-Abonnement, Region und Ressourcengruppe für Azure-Anmeldeinformationen

       "Wenn Sie Ihr eigenes Speicherkonto verwenden möchten, lesen Sie den Abschnitt Azure Blob-Speicherkonten hinzufügen." .
   - **Verschlüsselung**: Wenn Sie ein neues Speicherkonto erstellen, geben Sie die Verschlüsselungsschlüsselinformationen ein, die Sie vom Anbieter erhalten haben. Wenn Sie ein bestehendes Konto auswählen, sind die Verschlüsselungsinformationen bereits verfügbar.

     Daten im Konto werden standardmäßig mit von Microsoft verwalteten Schlüsseln verschlüsselt. Sie können weiterhin von Microsoft 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 Azure-Endpunkt verwenden

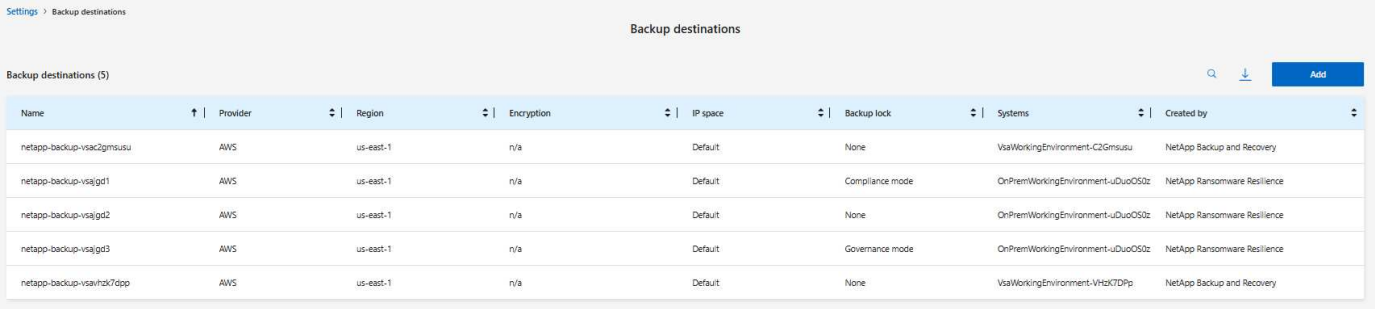
möchten.

Wenn Sie Azure PrivateLink verwenden möchten, lesen Sie "Azure PrivateLink" .

5. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue Sicherungsziel wird der Liste der Sicherungsziele hinzugefügt.



Stellen Sie eine Verbindung zu einem Sicherheits- und Ereignismanagementsystem (SIEM) zur Bedrohungsanalyse und -erkennung her

Sie können Daten zur Bedrohungsanalyse und -erkennung automatisch an Ihr Sicherheits- und Ereignismanagementsystem (SIEM) senden. Sie können AWS Security Hub, Microsoft Sentinel oder Splunk Cloud als Ihr SIEM auswählen.

Bevor Sie SIEM in Ransomware Resilience aktivieren, müssen Sie Ihr SIEM-System konfigurieren.

Informationen zu den an ein SIEM gesendeten Ereignisdaten

Ransomware Resilience kann die folgenden Ereignisdaten an Ihr SIEM-System senden:

- **Kontext**:
  - **os**: Dies ist eine Konstante mit dem Wert von ONTAP.
  - **os_version**: Die auf dem System ausgeführte ONTAP -Version.
  - **connector_id**: Die ID des Konsolenagenten, der das System verwaltet.
  - **cluster_id**: Die von ONTAP für das System gemeldete Cluster-ID.
  - **svm_name**: Der Name der SVM, auf der die Warnung gefunden wurde.
  - **volume_name**: Der Name des Volumes, auf dem sich die Warnung befindet.
  - **volume_id**: Die ID des von ONTAP für das System gemeldeten Volumes.
- **Vorfall**:
  - **incident_id**: Die von Ransomware Resilience für das in Ransomware Resilience angegriffene Volume generierte Vorfall-ID.
  - **alert_id**: Die von Ransomware Resilience für die Arbeitslast generierte ID.
  - **Schweregrad**: Eine der folgenden Warnstufen: „KRITISCH“, „HOCH“, „MITTEL“, „NIEDRIG“.
  - **Beschreibung**: Details zur erkannten Warnung, z. B. „Ein potenzieller Ransomware-Angriff wurde auf Workload arp_learning_mode_test_2630 erkannt.“

Konfigurieren Sie AWS Security Hub für die Bedrohungserkennung

Bevor Sie AWS Security Hub in Ransomware Resilience aktivieren, müssen Sie die folgenden allgemeinen Schritte in AWS Security Hub ausführen:

- Richten Sie Berechtigungen im AWS Security Hub ein.
- Richten Sie den Authentifizierungszugriffsschlüssel und den geheimen Schlüssel im AWS Security Hub ein. (Diese Schritte werden hier nicht bereitgestellt.)

Schritte zum Einrichten von Berechtigungen im AWS Security Hub

1. Gehen Sie zur **AWS IAM-Konsole**.
2. Wählen Sie **Richtlinien** aus.
3. Erstellen Sie eine Richtlinie mit dem folgenden Code im JSON-Format:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

Konfigurieren von Microsoft Sentinel zur Bedrohungserkennung

Bevor Sie Microsoft Sentinel in Ransomware Resilience aktivieren, müssen Sie die folgenden allgemeinen Schritte in Microsoft Sentinel ausführen:

- **Voraussetzungen**
  - Aktivieren Sie Microsoft Sentinel.
  - Erstellen Sie eine benutzerdefinierte Rolle in Microsoft Sentinel.
- **Anmeldung**
  - Registrieren Sie Ransomware Resilience, um Ereignisse von Microsoft Sentinel zu erhalten.
  - Erstellen Sie ein Geheimnis für die Registrierung.
- **Berechtigungen**: Weisen Sie der Anwendung Berechtigungen zu.
- **Authentifizierung**: Geben Sie die Authentifizierungsdaten für die Anwendung ein.

Schritte zum Aktivieren von Microsoft Sentinel

1. Gehen Sie zu Microsoft Sentinel.
2. Erstellen Sie einen **Log Analytics-Arbeitsbereich**.
3. Aktivieren Sie Microsoft Sentinel, um den gerade erstellten Log Analytics-Arbeitsbereich zu verwenden.

Schritte zum Erstellen einer benutzerdefinierten Rolle in Microsoft Sentinel

1. Gehen Sie zu Microsoft Sentinel.
2. Wählen Sie **Abonnement** > **Zugriffskontrolle (IAM)**.
3. Geben Sie einen benutzerdefinierten Rollennamen ein. Verwenden Sie den Namen **Ransomware Resilience Sentinel Configurator**.
4. Kopieren Sie das folgende JSON und fügen Sie es in die Registerkarte **JSON** ein.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Überprüfen und speichern Sie Ihre Einstellungen.

Schritte zum Registrieren von Ransomware Resilience zum Empfangen von Ereignissen von Microsoft Sentinel

1. Gehen Sie zu Microsoft Sentinel.
2. Wählen Sie **Entra ID** > **Anwendungen** > **App-Registrierungen**.
3. Geben Sie als **Anzeigenamen** für die Anwendung „**Ransomware Resilience**“ ein.
4. Wählen Sie im Feld **Unterstützter Kontotyp** die Option **Nur Konten in diesem Organisationsverzeichnis** aus.
5. Wählen Sie einen **Standardindex** aus, in den Ereignisse übertragen werden.
6. Wählen Sie **Überprüfen** aus.
7. Wählen Sie **Registrieren**, um Ihre Einstellungen zu speichern.

   Nach der Registrierung zeigt das Microsoft Entra Admin Center den Anwendungsübersichtsbereich an.

Schritte zum Erstellen eines Geheimnisses für die Registrierung

1. Gehen Sie zu Microsoft Sentinel.
2. Wählen Sie **Zertifikate und Geheimnisse** > **Clientgeheimnisse** > **Neues Clientgeheimnis**.
3. Fügen Sie eine Beschreibung für Ihr Anwendungsgeheimnis hinzu.
4. Wählen Sie ein **Ablaufdatum** für das Geheimnis aus oder geben Sie eine benutzerdefinierte Lebensdauer an.

Die Lebensdauer eines Client-Geheimnisses ist auf zwei Jahre (24 Monate) oder weniger begrenzt. Microsoft empfiehlt, einen Ablaufwert von weniger als 12 Monaten festzulegen.

5. Wählen Sie **Hinzufügen**, um Ihr Geheimnis zu erstellen.
6. Notieren Sie das im Authentifizierungsschritt zu verwendende Geheimnis. Das Geheimnis wird nie wieder angezeigt, nachdem Sie diese Seite verlassen.

Schritte zum Zuweisen von Berechtigungen zur Anwendung

1. Gehen Sie zu Microsoft Sentinel.
2. Wählen Sie **Abonnement** > **Zugriffskontrolle (IAM)**.
3. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen**.
4. Wählen Sie im Feld **Privilegierte Administratorrollen** die Option **Ransomware Resilience Sentinel Configurator** aus.

   Dies ist die benutzerdefinierte Rolle, die Sie zuvor erstellt haben.

5. Wählen Sie **Weiter**.
6. Wählen Sie im Feld **Zugriff zuweisen an** die Option **Benutzer, Gruppe oder Dienstprinzipal** aus.
7. Wählen Sie **Mitglieder auswählen**. Wählen Sie dann **Ransomware Resilience Sentinel Configurator**.
8. Wählen Sie **Weiter**.
9. Wählen Sie im Feld **Was der Benutzer tun kann** die Option **Dem Benutzer erlauben, alle Rollen außer den privilegierten Administratorrollen „Besitzer“, „UAA“ und „RBAC“ zuzuweisen (empfohlen)**.
10. Wählen Sie **Weiter**.
11. Wählen Sie **Überprüfen und zuweisen** aus, um die Berechtigungen zuzuweisen.

Schritte zum Eingeben der Authentifizierungsdaten für die Anwendung

1. Gehen Sie zu Microsoft Sentinel.
2. Geben Sie die Anmeldeinformationen ein:
   a. Geben Sie die Mandanten-ID, die Client-Anwendungs-ID und das Client-Anwendungsgeheimnis ein.
   b. Klicken Sie auf **Authentifizieren**.

      Nach erfolgreicher Authentifizierung wird die Meldung „Authentifiziert“ angezeigt.

3. Geben Sie die Log Analytics-Arbeitsbereichsdetails für die Anwendung ein.
   a. Wählen Sie die Abonnement-ID, die Ressourcengruppe und den Log Analytics-Arbeitsbereich aus.

Konfigurieren Sie Splunk Cloud für die Bedrohungserkennung

Bevor Sie Splunk Cloud in Ransomware Resilience aktivieren, müssen Sie die folgenden allgemeinen Schritte in Splunk Cloud ausführen:

- Aktivieren Sie einen HTTP-Ereignissammler in Splunk Cloud, um Ereignisdaten über HTTP oder HTTPS von der Konsole zu empfangen.
- Erstellen Sie ein Event Collector-Token in Splunk Cloud.

Schritte zum Aktivieren eines HTTP-Ereignissammlers in Splunk

1. Gehen Sie zu Splunk Cloud.
2. Wählen Sie **Einstellungen** > **Dateneingaben**.
3. Wählen Sie **HTTP-Ereignissammler** > **Globale Einstellungen**.
4. Wählen Sie auf dem Umschalter „Alle Token“ die Option **Aktiviert** aus.
5. Damit der Event Collector über HTTPS statt über HTTP lauscht und kommuniziert, wählen Sie **SSL aktivieren**.
6. Geben Sie in **HTTP-Portnummer** einen Port für den HTTP-Ereignissammler ein.

Schritte zum Erstellen eines Event Collector-Tokens in Splunk

1. Gehen Sie zu Splunk Cloud.
2. Wählen Sie **Einstellungen** > **Daten hinzufügen**.
3. Wählen Sie **Monitor** > **HTTP-Ereignissammler**.
4. Geben Sie einen Namen für das Token ein und wählen Sie **Weiter**.
5. Wählen Sie einen **Standardindex** aus, in den Ereignisse übertragen werden, und wählen Sie dann **Überprüfen**.
6. Bestätigen Sie, dass alle Einstellungen für den Endpunkt korrekt sind, und wählen Sie dann **Senden** aus.
7. Kopieren Sie das Token und fügen Sie es in ein anderes Dokument ein, um es für den Authentifizierungsschritt bereit zu haben.

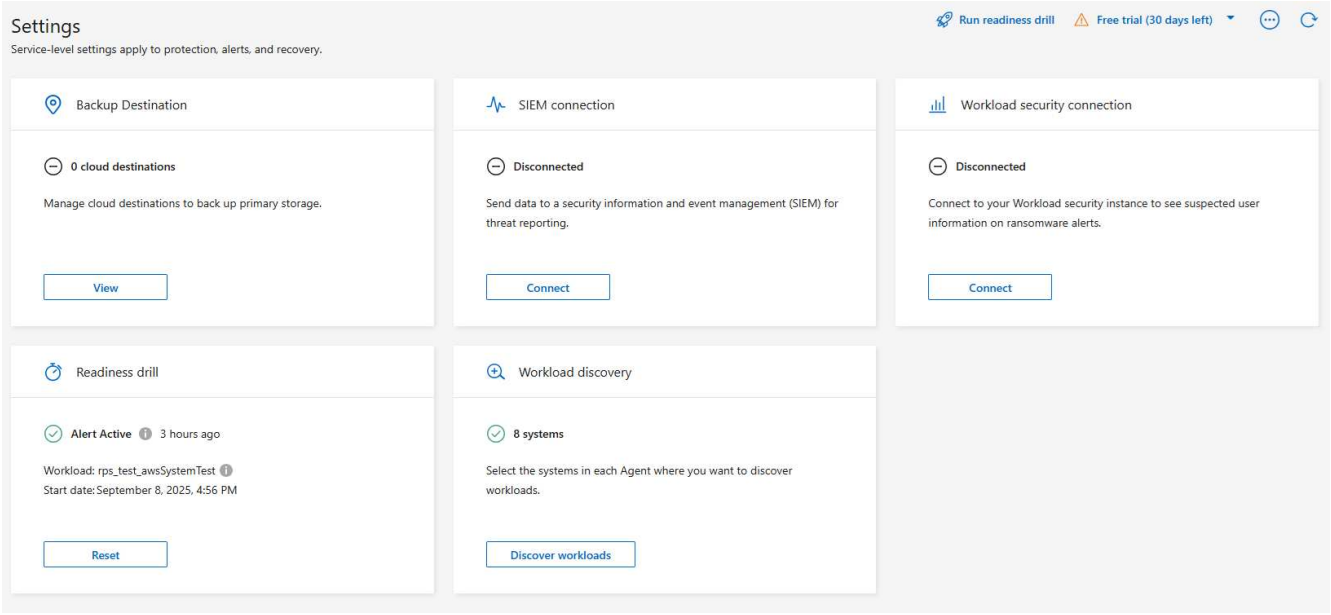
SIEM-Integration in Ransomware-Resilienz

Durch die Aktivierung von SIEM werden Daten von Ransomware Resilience zur Bedrohungsanalyse und -berichterstattung an Ihren SIEM-Server gesendet.

Schritte

1. Wählen Sie im Konsolenmenü **Schutz** > **Ransomware-Resilienz**.
2. Wählen Sie im Menü Ransomware Resilience die vertikale … Option oben rechts.
3. Wählen Sie **Einstellungen**.

   Die Seite „Einstellungen“ wird angezeigt.



4. Wählen Sie auf der Seite „Einstellungen“ in der Kachel „SIEM-Verbindung“ die Option „Verbinden“ aus.

5. Wählen Sie eines der SIEM-Systeme.
6. Geben Sie das Token und die Authentifizierungsdetails ein, die Sie in AWS Security Hub oder Splunk Cloud konfiguriert haben.

   Die von Ihnen eingegebenen Informationen hängen von dem von Ihnen ausgewählten SIEM ab.

7. Wählen Sie **Aktivieren**.

   Auf der Seite „Einstellungen“ wird „Verbunden“ angezeigt.

Konfigurieren der Erkennung verdächtiger Benutzeraktivitäten in NetApp Ransomware Resilience

Ransomware Resilience unterstützt die Erkennung verdächtigen Benutzerverhaltens in Erkennungsrichtlinien und ermöglicht Ihnen, Ransomware-Vorfälle auf Benutzerebene zu bekämpfen.

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.

Agenten und Sammler

Um die Erkennung verdächtiger Benutzeraktivitäten in Ransomware Resilience zu aktivieren, muss mindestens ein Benutzeraktivitätsagent installiert sein. Wenn Sie die Funktion für verdächtige Benutzeraktivitäten über das Ransomware Resilience-Dashboard aktivieren, müssen Sie die Agent-Hostinformationen angeben, um die Funktion zu aktivieren.

Ein Agent kann mehrere Datensammler hosten. Datensammler senden Daten zur Analyse an einen SaaS-Standort. Es gibt zwei Arten von Sammlern:

- Der **Datensammler** sammelt Benutzeraktivitätsdaten von ONTAP.
- Der **Benutzerverzeichnis-Connector** stellt eine Verbindung zu Ihrem Verzeichnis her, um Benutzer-IDs Benutzernamen zuzuordnen.

Collector werden in den Ransomware Resilience-Einstellungen konfiguriert.

Aktivieren Sie die Erkennung verdächtiger Benutzeraktivitäten

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Administratorrolle „Ransomware Resilience-Benutzerverhalten“. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

Hinzufügen eines Benutzeraktivitätsagenten

Benutzeraktivitätsagenten sind ausführbare Umgebungen für Datensammler. Datensammler geben Benutzeraktivitätsereignisse an Ransomware Resilience weiter. Sie müssen mindestens einen Benutzeraktivitäts-Agenten erstellen, um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren.

Anforderungen

Zum Installieren eines Benutzeraktivitätsagenten benötigen Sie einen Host oder eine VM mit einem der folgenden unterstützten Betriebssystem- und Serveranforderungen.

Betriebssystemanforderungen

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
RedHat	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)

Serveranforderungen

Der Server muss die folgenden Mindestanforderungen erfüllen:

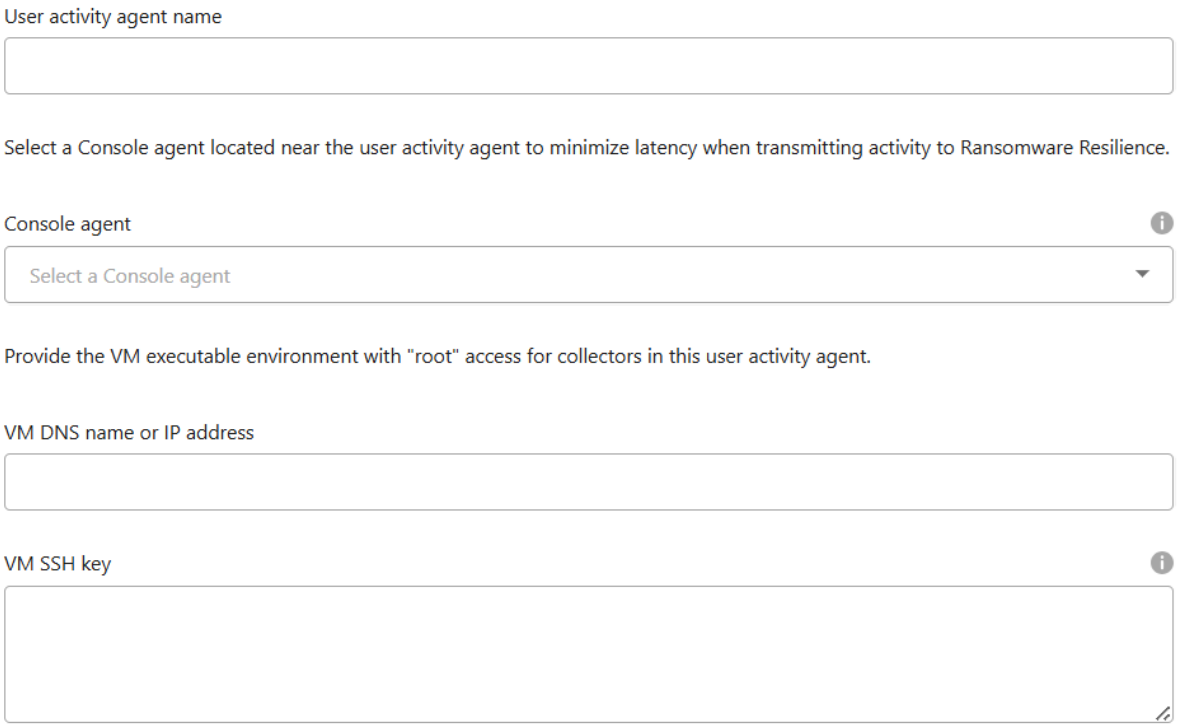
- **CPU**: 4 KERNE
- **RAM**: 16 GB RAM
- **Speicherplatz**: 35 GB freier Speicherplatz

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-Schlüssel**



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

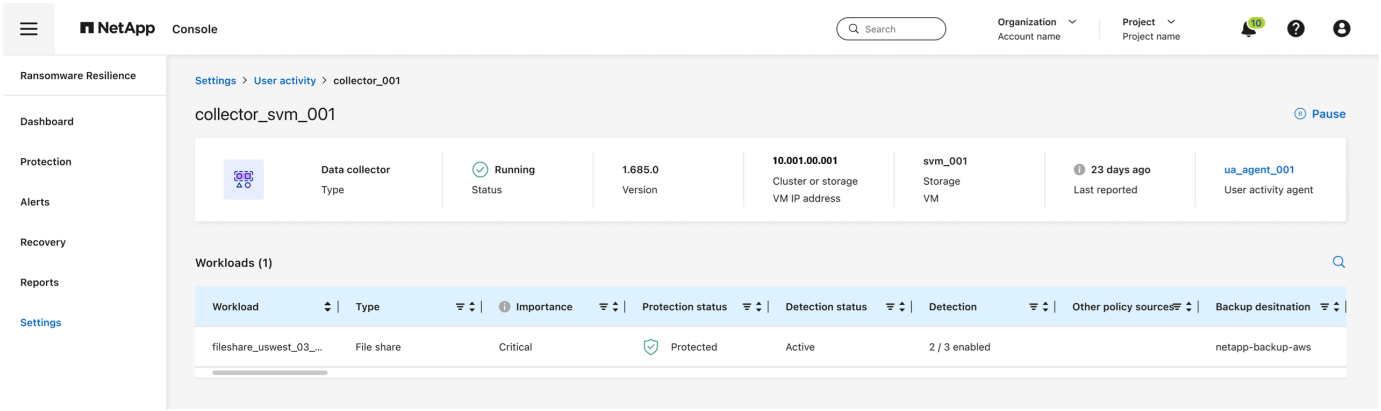
Ergebnis

Nachdem der Benutzeraktivitäts-Agent erfolgreich erstellt wurde, kehren Sie zum Menü **Einstellungen** zurück und wählen Sie dann in der Kachel „Benutzeraktivität“ **Verwalten** aus. Wählen Sie die Registerkarte **Benutzeraktivitätsagent** und dann den Benutzeraktivitätsagenten aus, um Details dazu anzuzeigen, einschließlich Datensammlern und Benutzerverzeichniskonnektoren.

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.

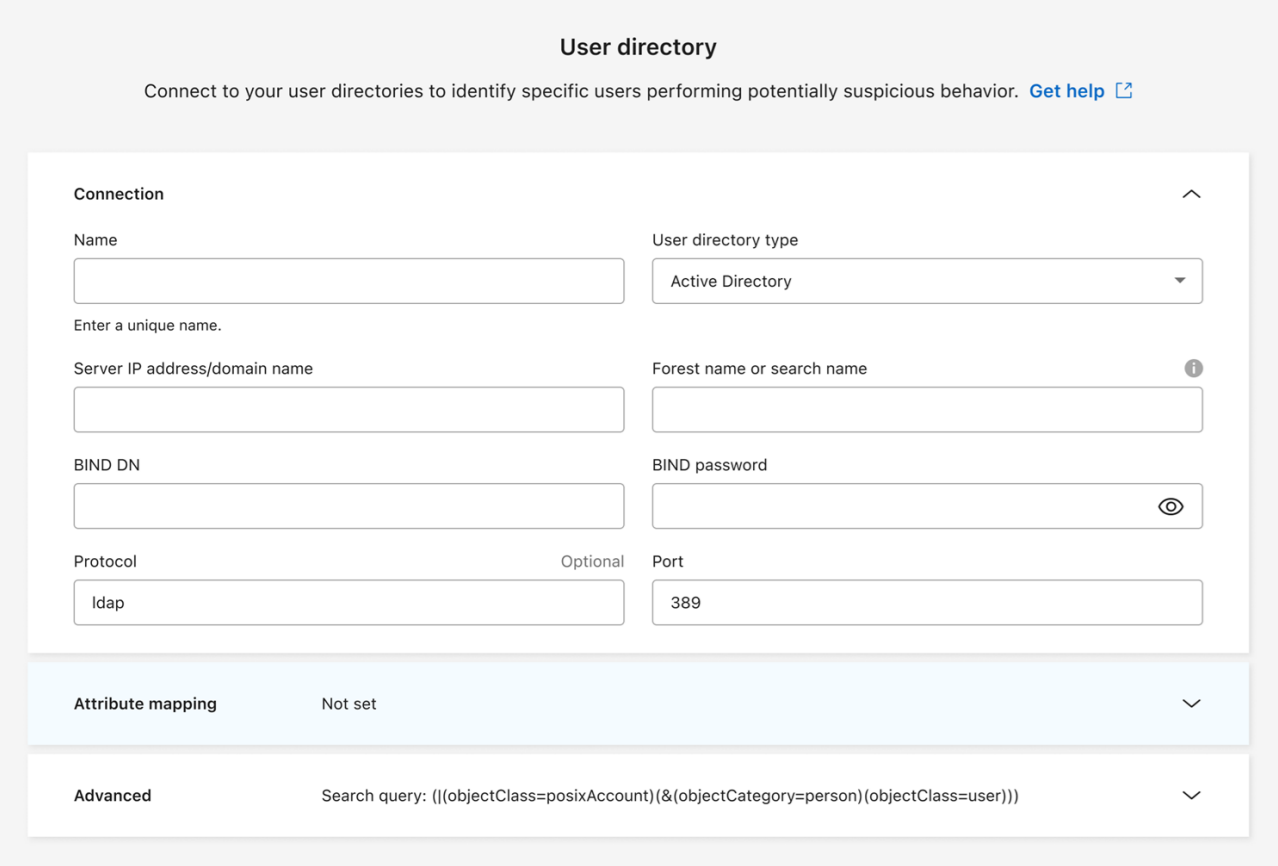


Hinzufügen eines Benutzerverzeichnis-Connectors

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. Geben Sie die Details der Verbindung an:
    - **Name**
    - **Benutzerverzeichnistyp**
    - **Server-IP-Adresse oder Domänenname**
    - **Waldname oder Suchname**
    - **BIND-Domänenname**
    - **BIND-Passwort**
    - **Protokoll** (dies ist optional)
    - **Hafen**



Geben Sie die Details zur Attributzuordnung an:

- **Anzeigename**
- **SID** (wenn Sie LDAP verwenden)
- **Benutzername**
- **Unix-ID** (wenn Sie NFS verwenden)
- Wählen Sie **Optionale Attribute einschließen**. Sie können auch E-Mail-Adresse, Telefonnummer, Rolle, Bundesland, Land, Abteilung, Foto, Manager-DN oder Gruppen angeben.

  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

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 Ihre Aktionen zu bestätigen.

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 böswillige Aktivitäten und anomales Benutzerverhalten" .

Nutzen Sie Ransomware-Resilienz

Nutzen Sie NetApp Ransomware Resilience

Mit NetApp Ransomware Resilience können Sie den Zustand Ihrer Workloads einsehen und diese schützen.

- "Entdecken Sie Workloads in Ransomware Resilience" .
- "Schutz und Workload-Integrität vom Dashboard aus anzeigen" .
  - Lesen Sie die Empfehlungen zum Schutz vor Ransomware und setzen Sie diese um.
- "Workloads schützen":
  - Weisen Sie Workloads eine Ransomware-Schutzstrategie zu.
  - Erhöhen Sie den Anwendungsschutz, um zukünftige Ransomware-Angriffe zu verhindern.
  - Erstellen, ändern oder löschen Sie eine Schutzstrategie.
- "Reagieren Sie auf die Erkennung potenzieller Ransomware-Angriffe" .
- "Wiederherstellung nach einem Angriff"(nachdem Vorfälle neutralisiert wurden).
- "Konfigurieren der Schutzeinstellungen" .

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.

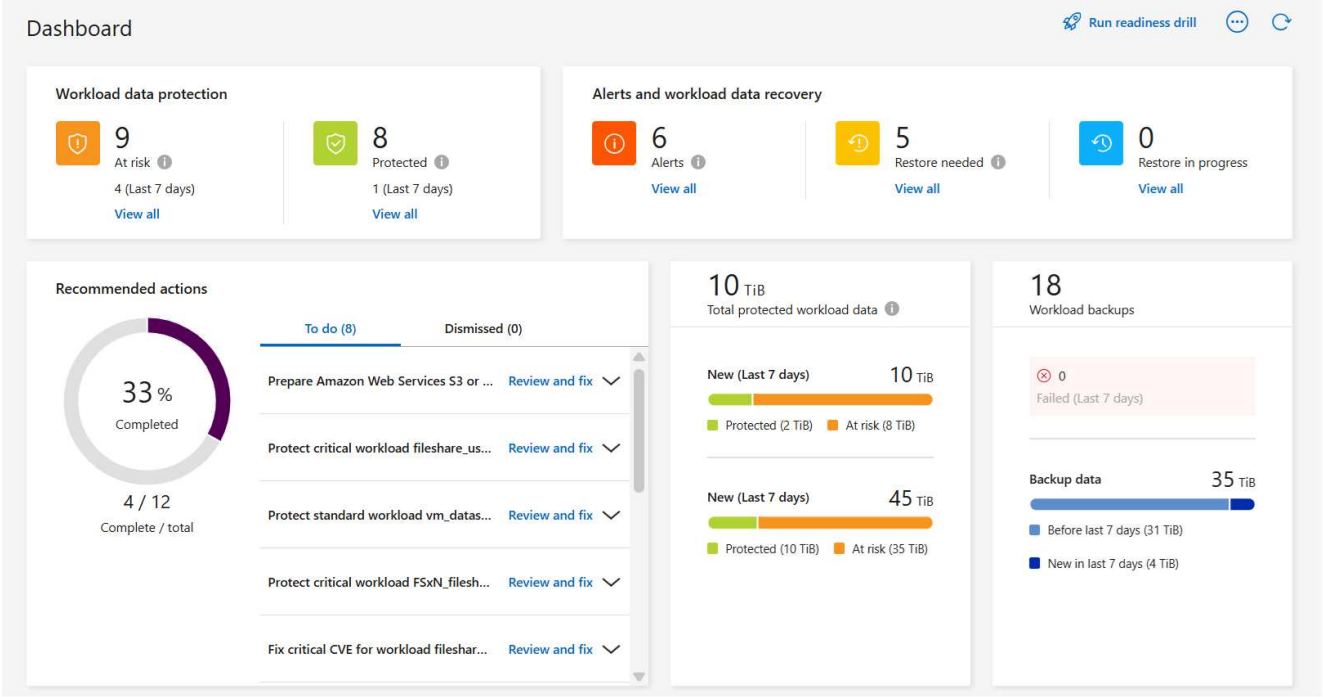
Verwenden Sie das Dashboard, um Schutzvorschläge zu prüfen, Einstellungen zu ändern, Berichte herunterzuladen und Dokumentationen anzuzeigen.

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 BlueXP -Zugriffsrollen für alle Dienste" .

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" .

Empfehlung	Beschreibung	So lösen Sie
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" .
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.

Das Herunterladen einer CSV-Datei von einer Seite umfasst nur die Daten dieser Seite.

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

Schritte

1. Wählen Sie im Ransomware Resilience-Dashboard die Option *Aktualisieren* Klicken Sie oben rechts auf die Option, um die in den Dateien angezeigten Daten zu aktualisieren.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie auf der Seite *Download* 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 die Konsolenzugriffsrollen für alle Dienste" .

Strategien zum Schutz vor Ransomware verstehen

Strategien zum Schutz vor Ransomware umfassen sowohl Erkennungs- als auch Schutzrichtlinien.

- **Erkennungsrichtlinien** erkennen 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.

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 und Recovery für Dateifreigaben, VM-Dateifreigaben
- SnapCenter für VMware für VM-Datenspeicher
- SnapCenter für Oracle und MySQL

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

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

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

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

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

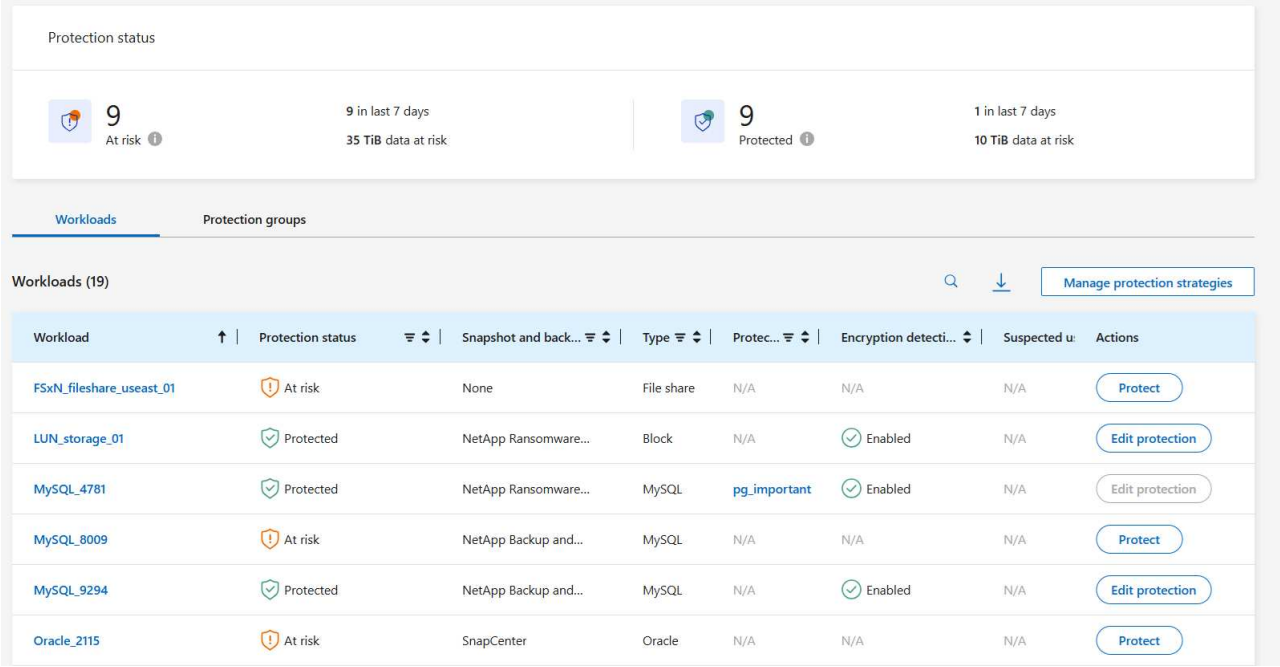
Anzeigen des Ransomware-Schutzes für eine Arbeitslast

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

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

Schritte

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

Erkennungsrichtlinie: Der Name der Ransomware-Erkennungsrichtlinie wird angezeigt, sofern eine zugewiesen wurde. Wenn die Erkennungsrichtlinie nicht zugewiesen wurde, wird „N/A“ 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 1 Snapshot-Kopien pro Stunde erstellt (sehr aggressiver Schutzplan)
- **Wichtig**: Es werden weniger als 1 Snapshot-Kopien pro Stunde, aber mehr als 1 pro Tag erstellt
- **Standard**: Mehr als eine Snapshot-Kopie pro Tag

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.

Richtlinie nebene	Schnappschuss	Frequenz	Aufbewahrung (Tage)	Anzahl der Snapshot-Kopien	Maximale Gesamtzahl der 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	Aufbewahrung (Tage)	Anzahl der Snapshot-Kopien	Maximale Gesamtzahl der 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

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 Konsole registrieren
   - Verfügbares SnapCenter Plug-in for VMware vSphere (SCV) mit der NetApp Konsole 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)

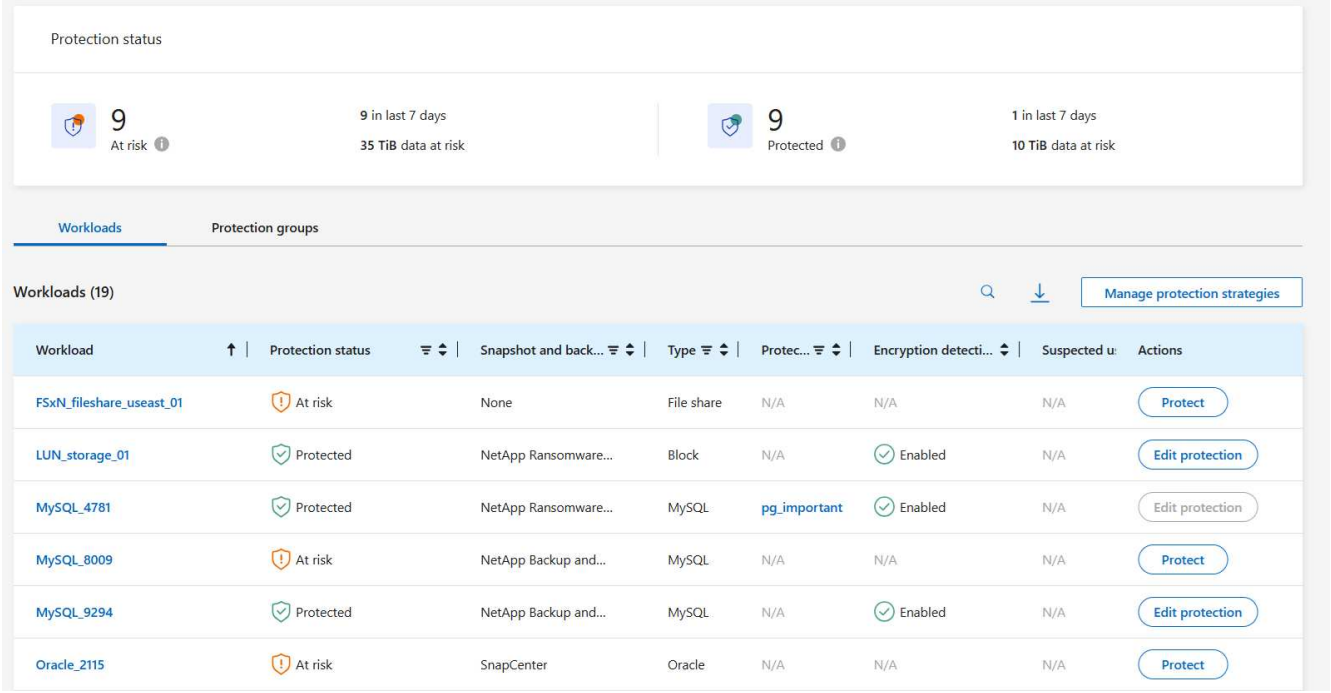
Wenn für die Arbeitslast keine Snapshot- oder Sicherungsrichtlinien vorhanden sind, können Sie eine Ransomware-Schutzstrategie erstellen, die die folgenden Richtlinien enthalten kann, die Sie in Ransomware

Resilience erstellen:

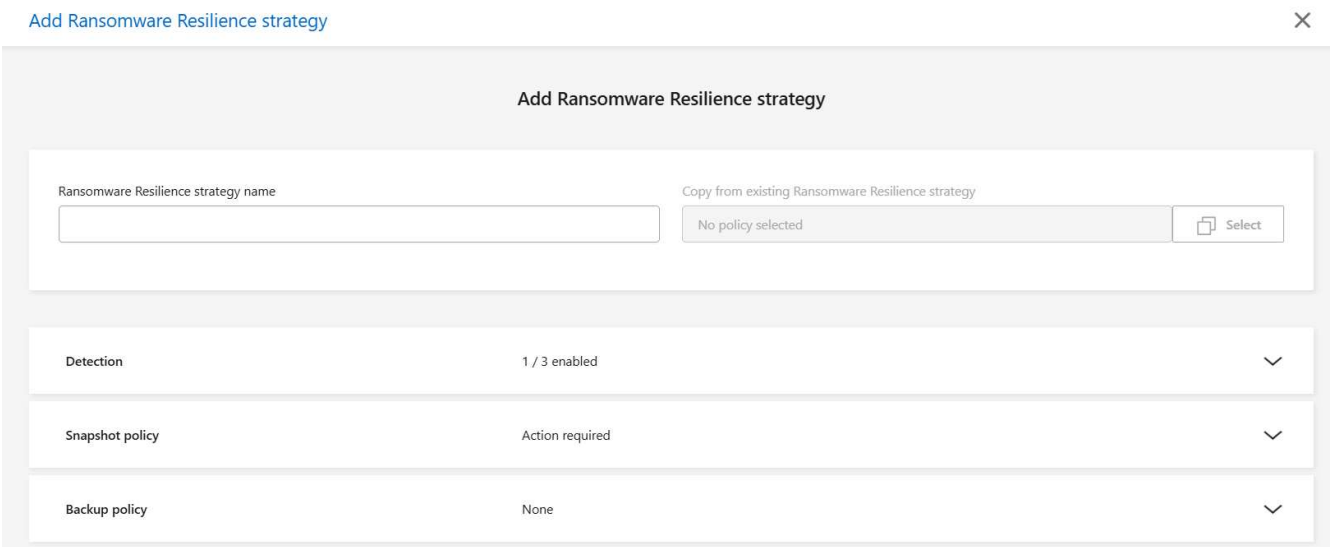
- Snapshot-Richtlinie
- Sicherungsrichtlinie
- Richtlinie zur Ransomware-Erkennung

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-Erkennung, damit Ransomware Resilience potenzielle Ransomware-Angriffe erkennt.
     - **Erkennung verdächtigen Benutzerverhaltens**: Aktivieren Sie die Erkennung des Benutzerverhaltens, um Benutzeraktivitätsereignisse an Ransomware Resilience zu übertragen und verdächtige Ereignisse wie Datenschutzverletzungen zu erkennen.
     - **Dateierweiterungen blockieren**: Aktivieren Sie diese Option, damit Ransomware Resilience bekannte verdächtige Dateierweiterungen blockiert. 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.
   - **Backup-Richtlinie**:
     - **Basisname der Sicherungsrichtlinie**: Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Namen.
     - **Sicherungszeitpläne**: Wählen Sie Zeitplanoptionen für den sekundären Speicher und aktivieren Sie den Zeitplan.

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

6. Wählen Sie **Hinzufügen**.

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

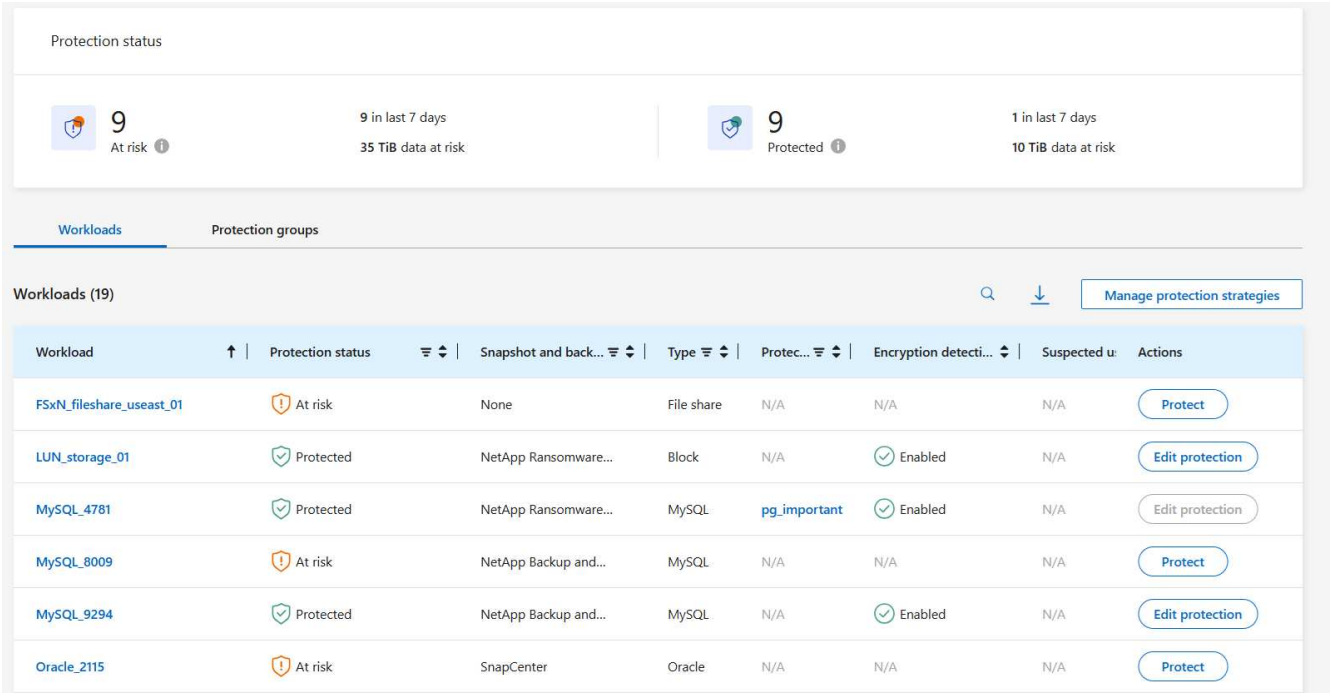
Mit Ransomware Resilience können Sie Workloads mit vorhandenem Snapshot- und Backup-Schutz, der in anderen NetApp -Produkten oder -Services verwaltet wird, entweder eine Erkennungsrichtlinie oder eine Schutzrichtlinie zuweisen. Andere Dienste wie Backup and Recovery und SnapCenter verwenden Richtlinien,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

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

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

Schritte

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



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

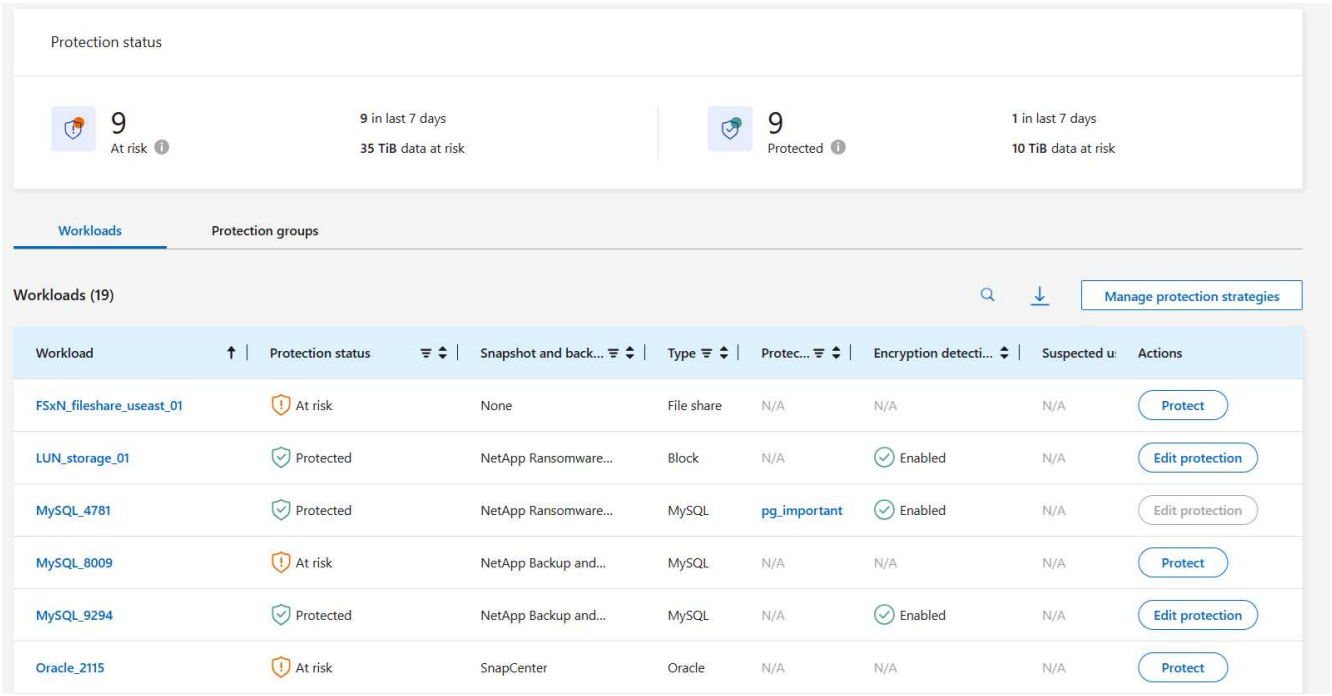
9. Wählen Sie **Weiter**.
10. Überprüfen Sie Ihre Auswahl. Wählen Sie **Erstellen**, um die Erkennung zu aktivieren.
11. Überprüfen Sie auf der Seite „Schutz“ den **Erkennungsstatus**, um zu bestätigen, dass die Erkennung aktiv ist.

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. 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.

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

Zuweisen einer anderen Richtlinie

Sie können die bestehende Richtlinie durch eine andere ersetzen.

Schritte

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

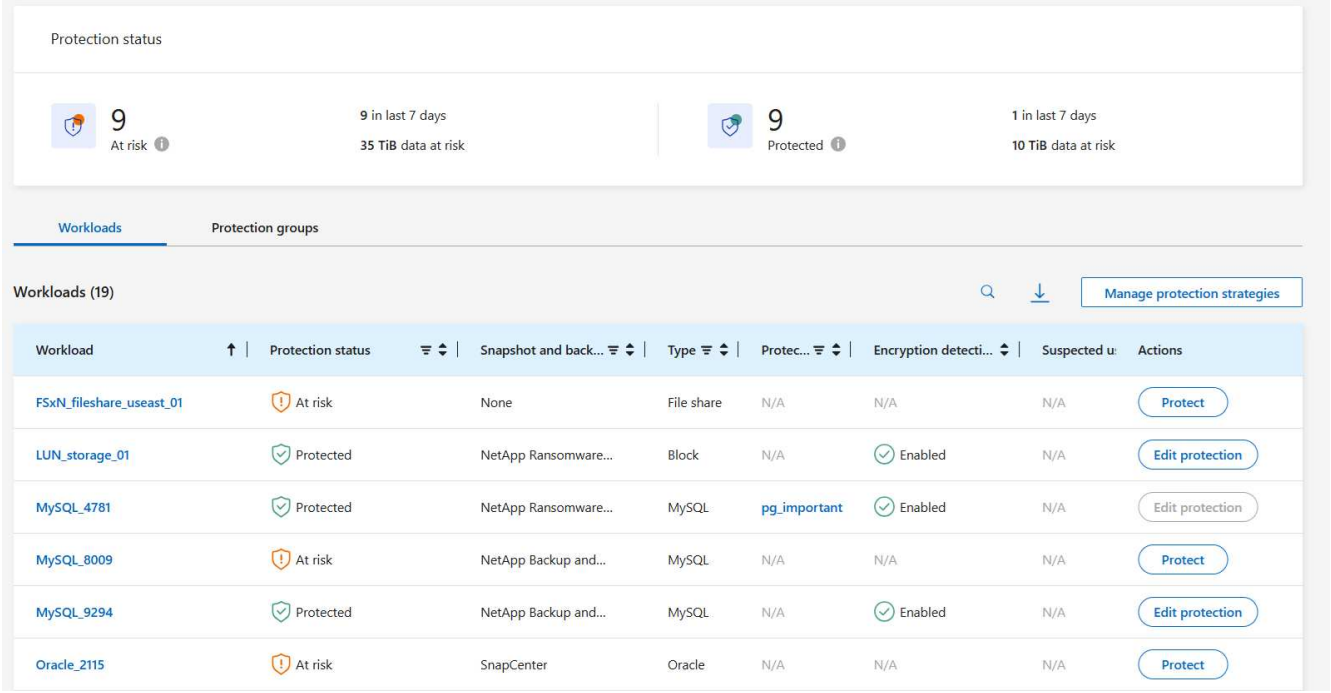
Erstellen einer Schutzgruppe

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

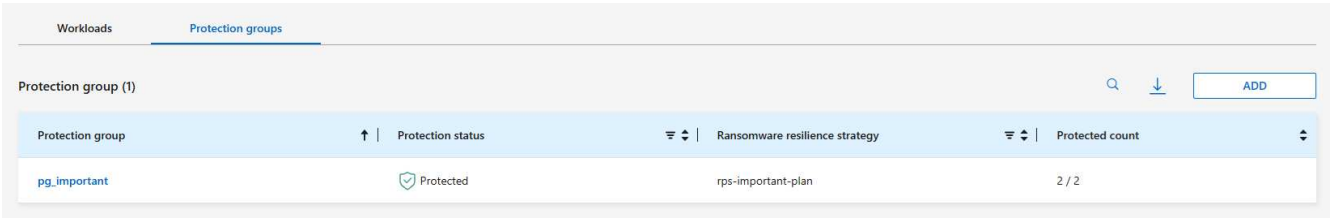
Sie können Gruppen unabhängig von ihrem Schutzstatus erstellen (d. h. nicht geschützte Gruppen und geschützte Gruppen). Wenn Sie einer Schutzgruppe eine Schutzrichtlinie hinzufügen, ersetzt die neue Schutzrichtlinie alle vorhandenen Richtlinien, einschließlich der von SnapCenter und NetApp Backup and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

Schritte

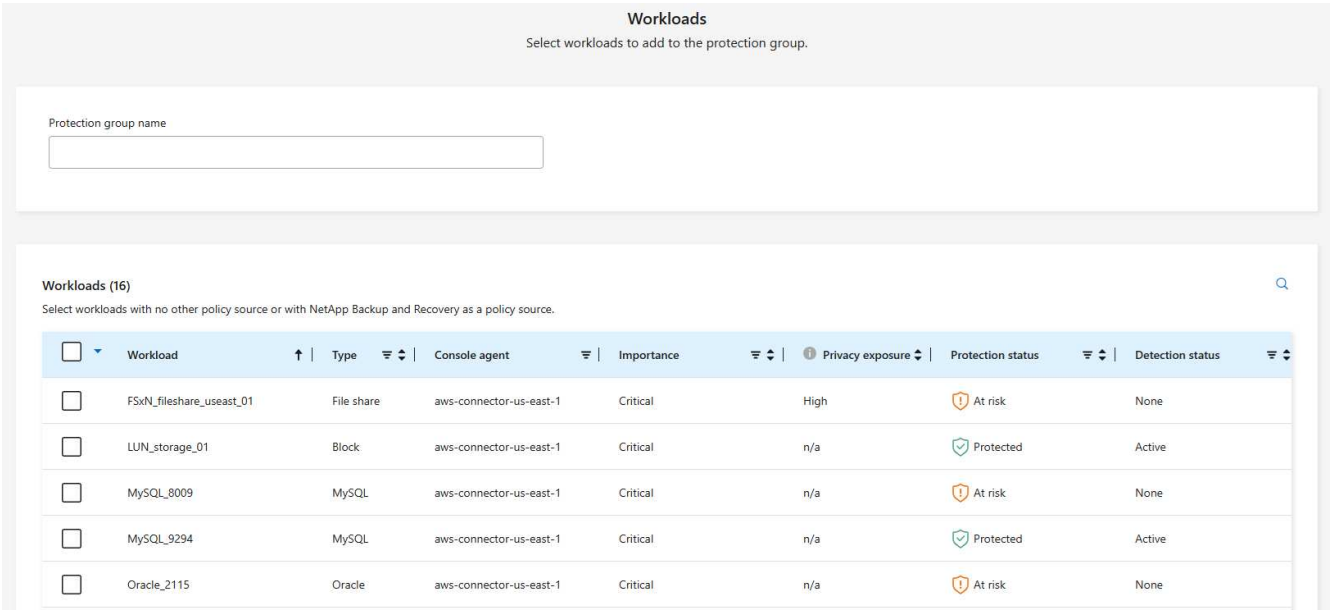
1. Wählen Sie im Menü „Ransomware-Resilienz“ die Option „Schutz“ aus.



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



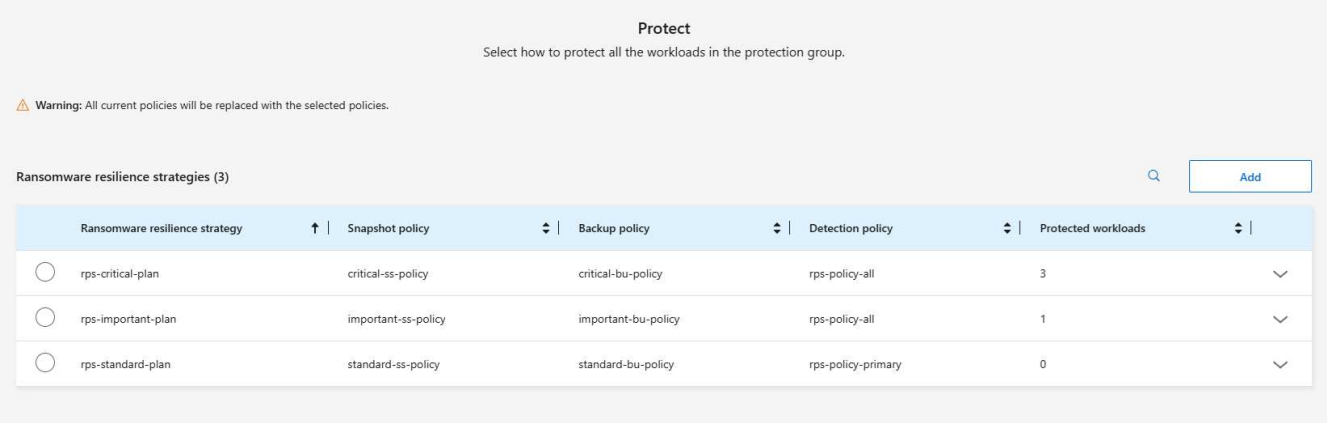
3. Wählen Sie **Hinzufügen**.



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

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

6. Wählen Sie **Weiter**.



7. Wählen Sie die Richtlinie aus, die den Schutz für diese Gruppe regelt. Wählen Sie zur Bestätigung **Weiter**.
   a. Wenn Sie eine Sicherungsrichtlinie konfigurieren müssen, wählen Sie eine aus und klicken Sie dann auf **Weiter**.
   b. Wenn Ihre Erkennungsrichtlinie die Erkennung des Benutzerverhaltens umfasst, wählen Sie den Datensammler aus, den Sie verwenden möchten, und klicken Sie dann auf **Weiter**.
8. Überprüfen Sie die Auswahl für die Schutzgruppe.
9. 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.

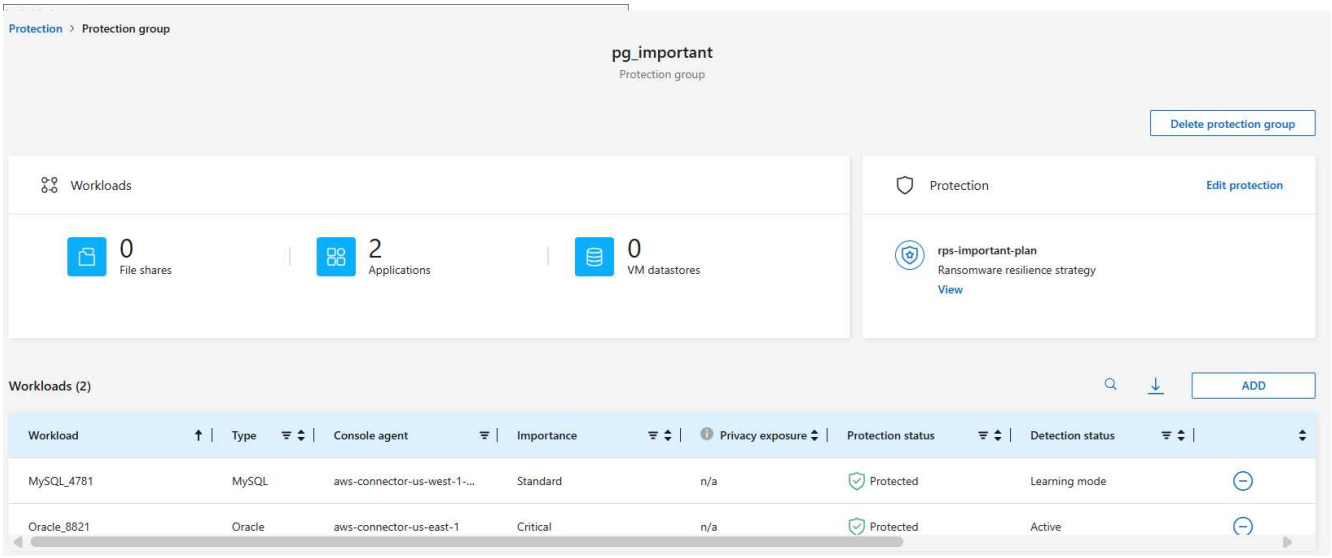
Entfernen von Workloads aus einer Gruppe

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.



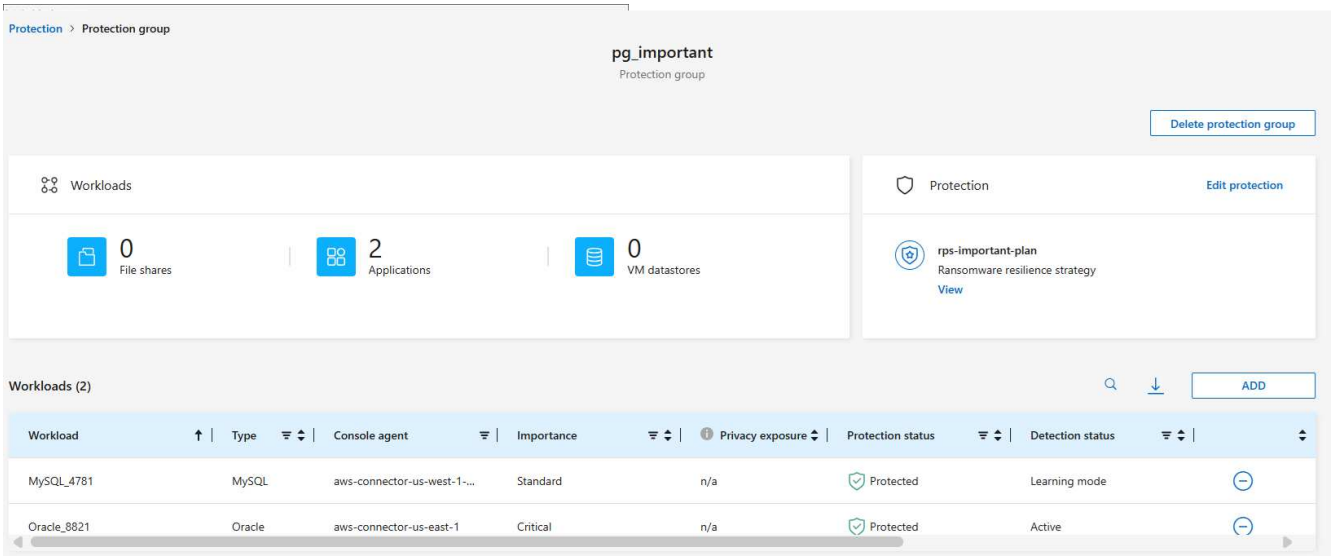
4. Wählen Sie auf der Seite der ausgewählten Schutzgruppe die Arbeitslast aus, die Sie aus der Gruppe entfernen möchten, und wählen Sie die *Aktionen*••• Option.
5. Wählen Sie im Menü „Aktionen“ die Option „Arbeitslast entfernen“ aus.
6. Bestätigen Sie, dass Sie die Arbeitslast entfernen möchten, und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

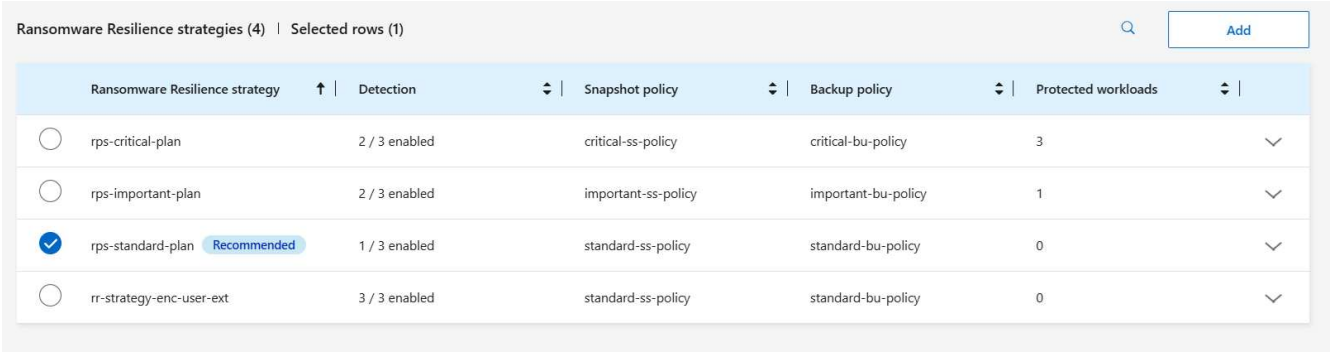
Bevor Sie eine Ransomware-Schutzstrategie löschen, möchten Sie möglicherweise prüfen, welche Workloads durch diese Strategie geschützt sind.

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 Konsole 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 die Konsolenzugriffsrollen für alle Dienste" .

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:

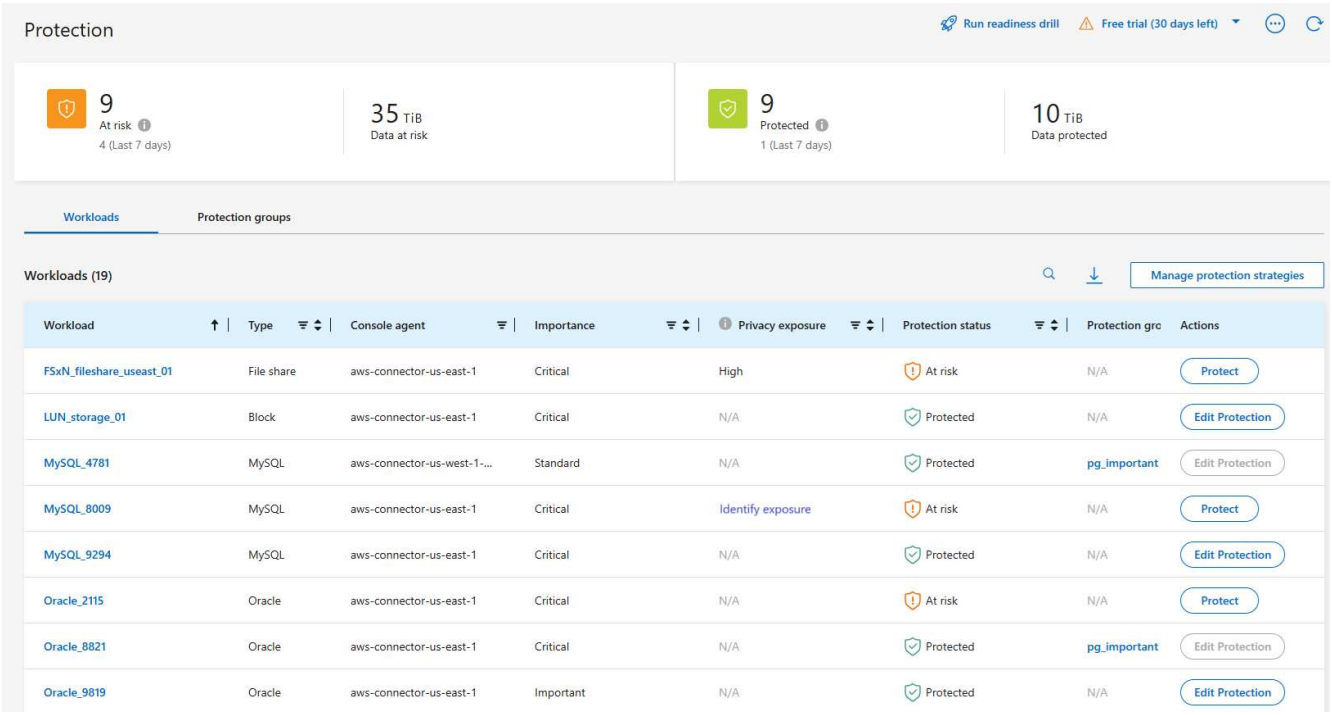
- "Erfahren Sie mehr über die Datenklassifizierung"
- "Kategorien personenbezogener Daten"
- "Untersuchen Sie die in Ihrer Organisation gespeicherten Daten"

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

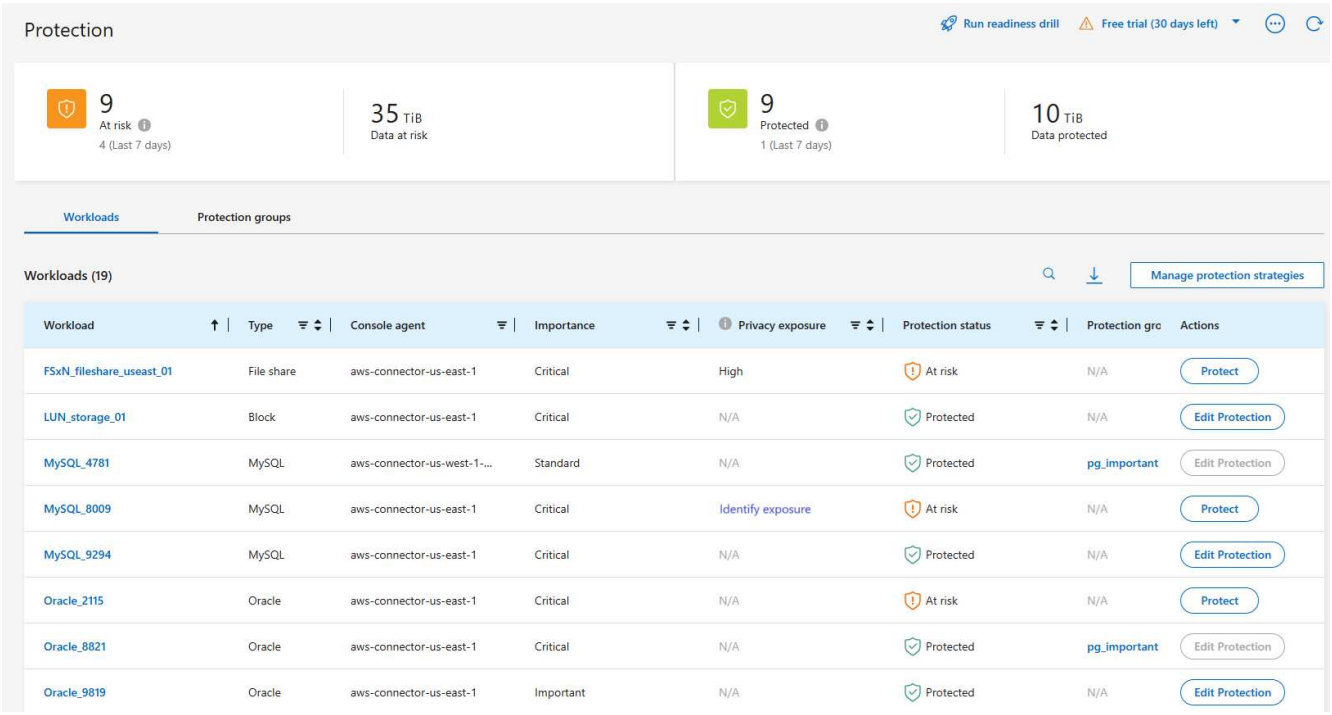
Bewerten Sie das Risiko, nachdem die Datenklassifizierung nach PII gesucht hat.

PII-Daten werden einer von drei Kategorien zugeordnet:

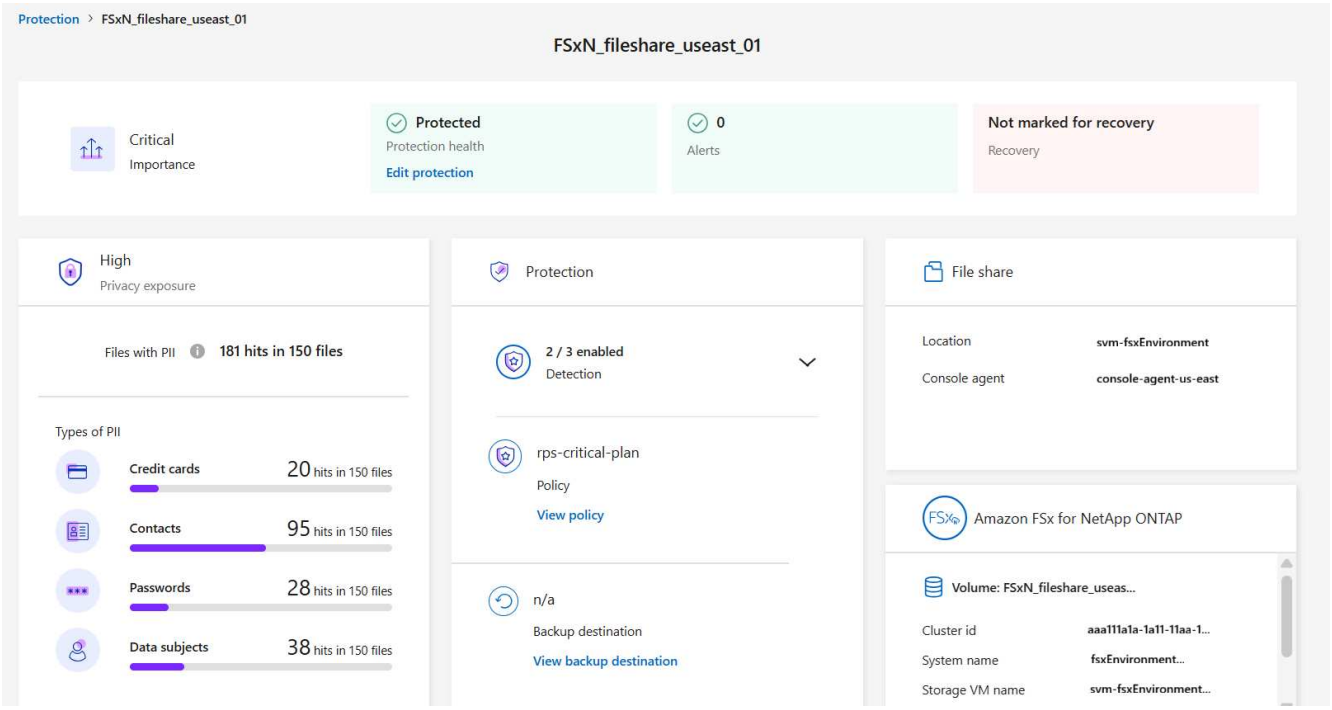
- **Hoch**: Mehr als 70 % der Dateien enthalten PII
- **Mittel**: Mehr als 30 % und weniger als 70 % der Dateien enthalten PII
- **Niedrig**: Mehr als 0 % und weniger als 30 % der Dateien enthalten PII

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"

Behandeln Sie erkannte Ransomware-Warnmeldungen mit NetApp Ransomware Resilience

Wenn NetApp Ransomware Resilience einen möglichen Angriff erkennt, wird auf dem Dashboard und im Benachrichtigungsbereich eine Warnung 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, wird in den Benachrichtigungseinstellungen der Konsole eine Benachrichtigung angezeigt und eine E-Mail an die konfigurierte Adresse gesendet. Die E-Mail enthält Informationen zum Schweregrad, zur betroffenen Arbeitslast und einen Link zur Warnung auf der Registerkarte „Ransomware Resilience **Warnungen**“.

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.

Jeder Alarm 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.

Bei SAN-Umgebungen basieren Warnungen nur 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 Alarmvorfall kann einen der folgenden Zustände haben:

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

Nachdem Sie einen Angriff abgewehrt haben, können Sie dies nicht mehr rückgängig machen. Wenn Sie eine Arbeitslast ablehnen, werden alle Snapshot-Kopien, die automatisch als Reaktion auf den potenziellen Ransomware-Angriff erstellt wurden, dauerhaft 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.

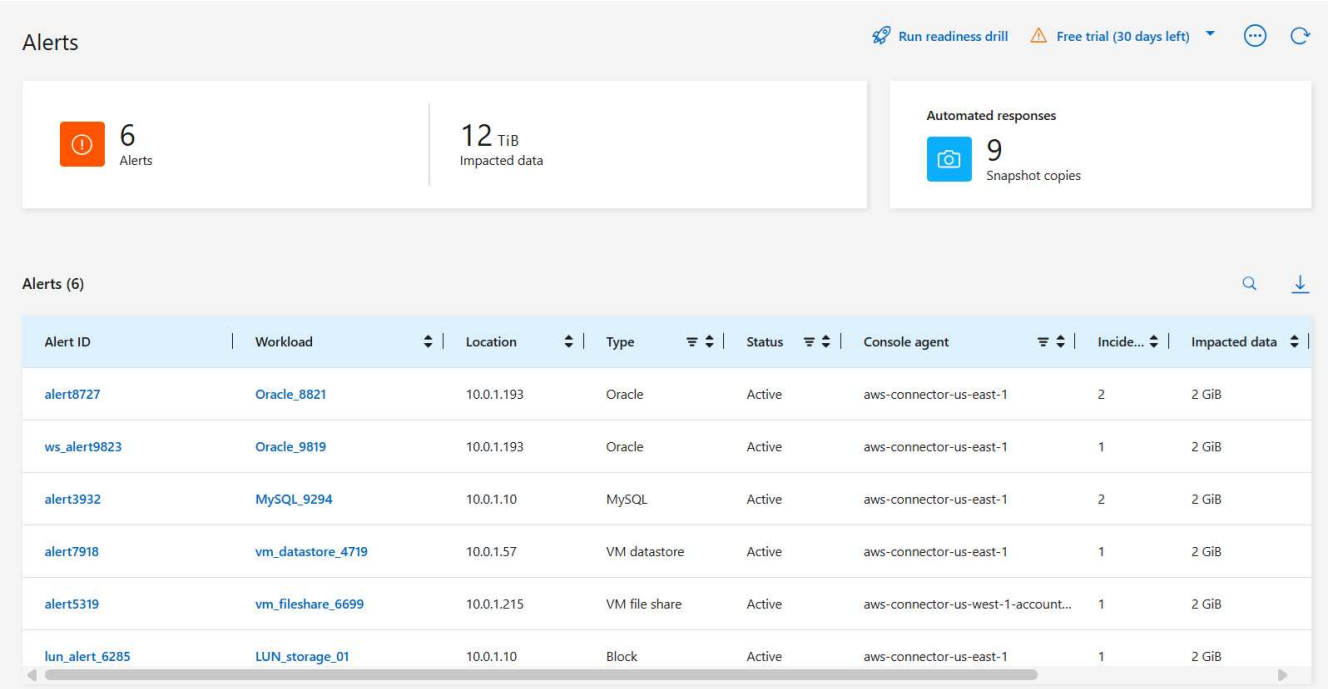
Warnungen anzeigen

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 BlueXP -Zugriffsrollen für alle Dienste" .

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 den angemeldeten Benutzern eine E-Mail-Benachrichtigung basierend auf ihren Abonnement-Benachrichtigungseinstellungen. Die E-Mail enthält Informationen zur Warnung, einschließlich des Schweregrads und der betroffenen Ressourcen.

Sie können E-Mail-Benachrichtigungen zu Ransomware-Resilience-Warnmeldungen erhalten. Mithilfe dieser Funktion bleiben Sie über Warnungen, deren Schweregrad und betroffene Ressourcen auf dem Laufenden.

Um E-Mail-Benachrichtigungen zu abonnieren, lesen Sie bitte "E-Mail-Benachrichtigungseinstellungen festlegen" .

1. Gehen Sie in Ransomware Resilience zur Seite **Einstellungen**.
2. Suchen Sie unter **Benachrichtigungen** die Einstellungen für E-Mail-Benachrichtigungen.
3. Geben Sie die E-Mail-Adresse ein, an die Sie Benachrichtigungen erhalten möchten.
4. Speichern Sie Ihre Änderungen.

Sie erhalten jetzt E-Mail-Benachrichtigungen, wenn neue Warnungen generiert werden.

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 BlueXP -Zugriffsrollen für alle Dienste" .

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 Schutzrichtlinie mit Benutzerverhaltenserkennung aktiviert haben, um die Erkennung auf Benutzerebene anzuzeigen. Wenn die Erkennung des Benutzerverhaltens aktiviert ist, wird die Spalte **Verdächtiger Benutzer** im Dashboard „Warnungen“ angezeigt. Sie wird nicht angezeigt, wenn die Erkennung des Benutzerverhaltens nicht aktiviert ist. Informationen zum Aktivieren der Erkennung verdächtiger Benutzer finden Sie unter"Verdächtige Benutzeraktivität" .

Wenn Sie NetApp Data Infrastructure Insights (DII) Workload Security verwenden, wird empfohlen, dieselben Workload Security-Agenten für Ransomware Resilience zu verwenden. Sie müssen keine separaten Workload Security-Agenten für Ransomware Resilience bereitstellen. Die Verwendung derselben Workload Security-Agenten erfordert jedoch eine Paarungsbeziehung zwischen der Ransomware Resilience Console-Organisation und dem DII Storage Workload Security-Mandanten. Wenden Sie sich an Ihren Kundenbetreuer, um diese Kopplung zu aktivieren.

Anzeigen böswilliger Aktivitäten

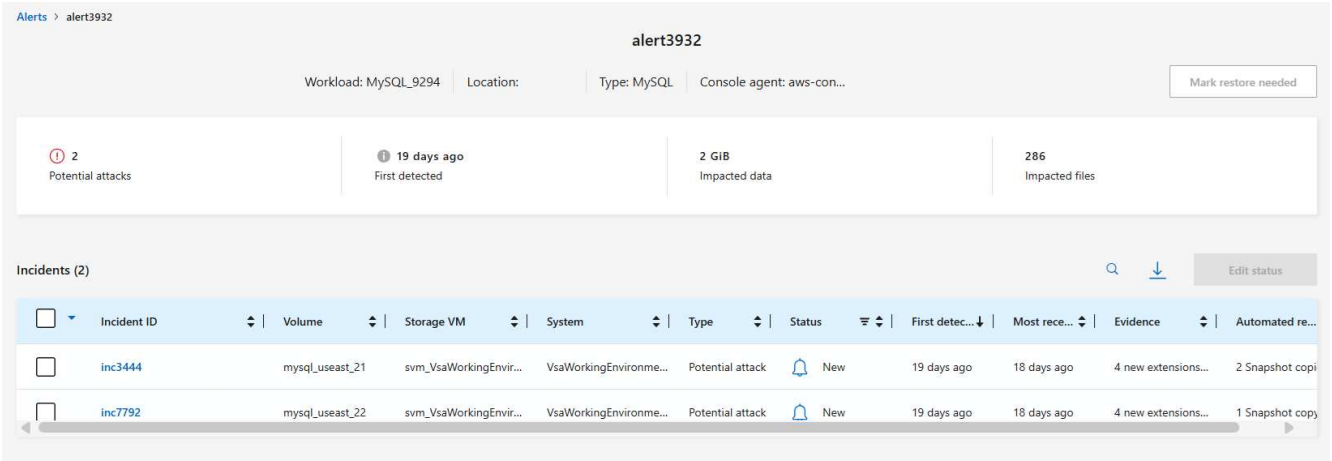
Wenn Autonomous Ransomware Protection eine Warnung in Ransomware Resilience auslöst, können Sie die folgenden Details anzeigen:

- 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.
4. Um einem verdächtigen Benutzer den weiteren Zugriff auf Ihre von der Konsole überwachte Umgebung zu verweigern, wählen Sie unter dem Namen des Benutzers **Blockieren** aus.

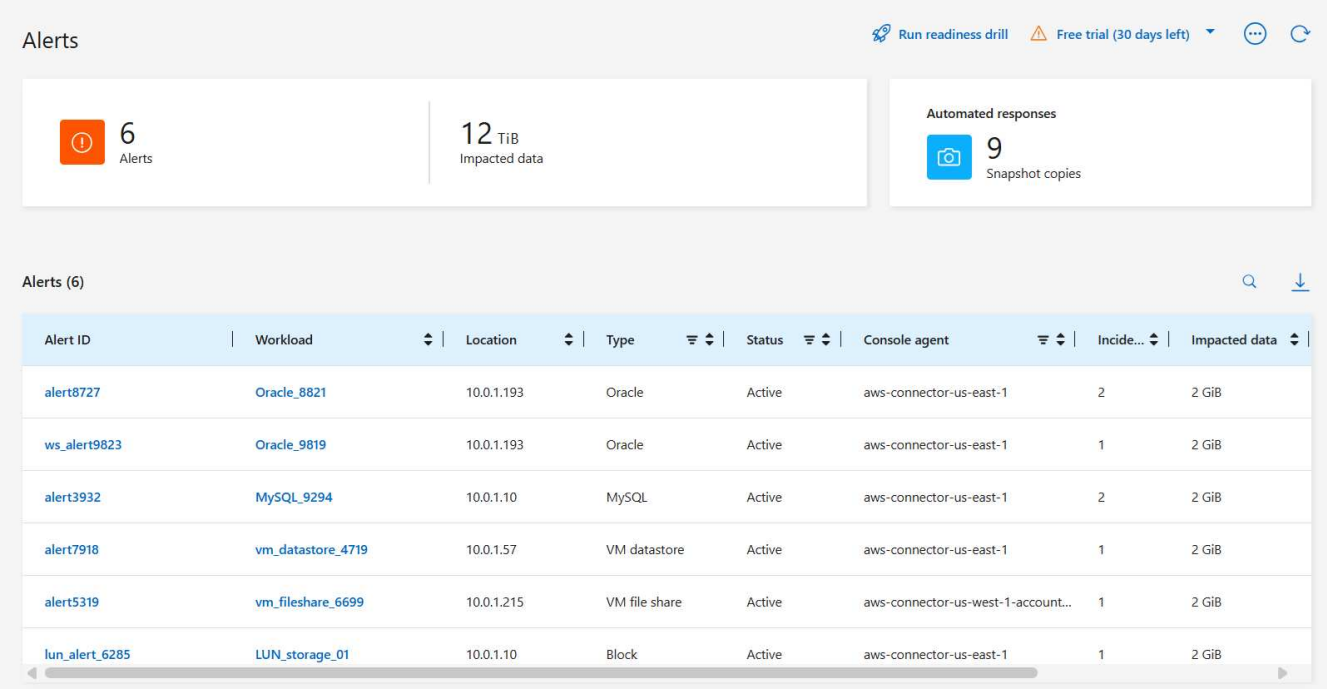
Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden).

Benachrichtigen Sie nach dem Stoppen des Angriffs Ihren Speicheradministrator, dass die Daten bereit sind, damit er mit der Wiederherstellung beginnen kann.

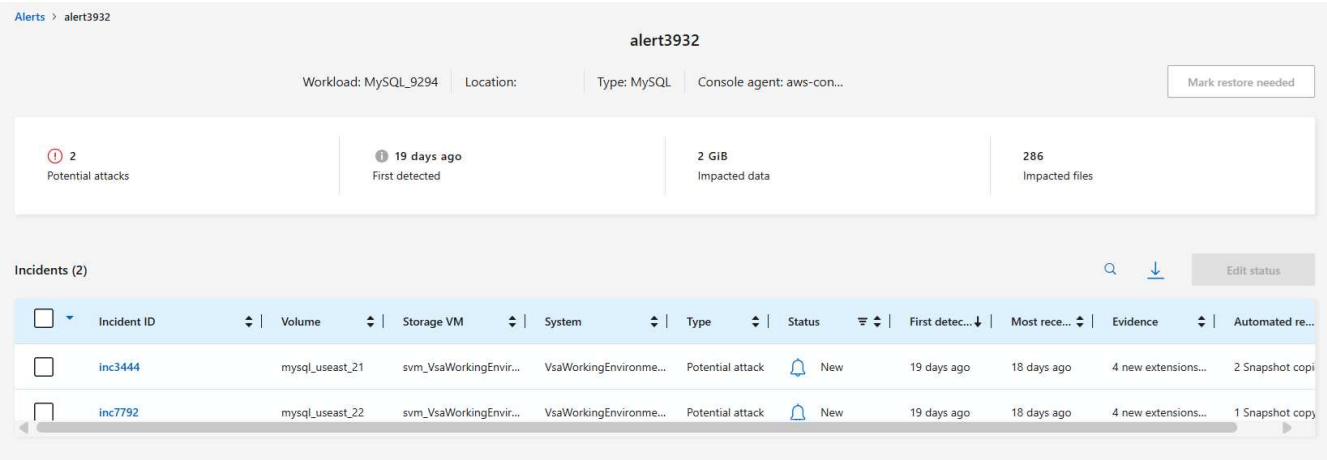
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

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. Handelt es sich nicht um tatsächliche Drohungen, können sie abgewiesen werden.

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 bei einem solchen Verhalten keine weitere Warnung aus.

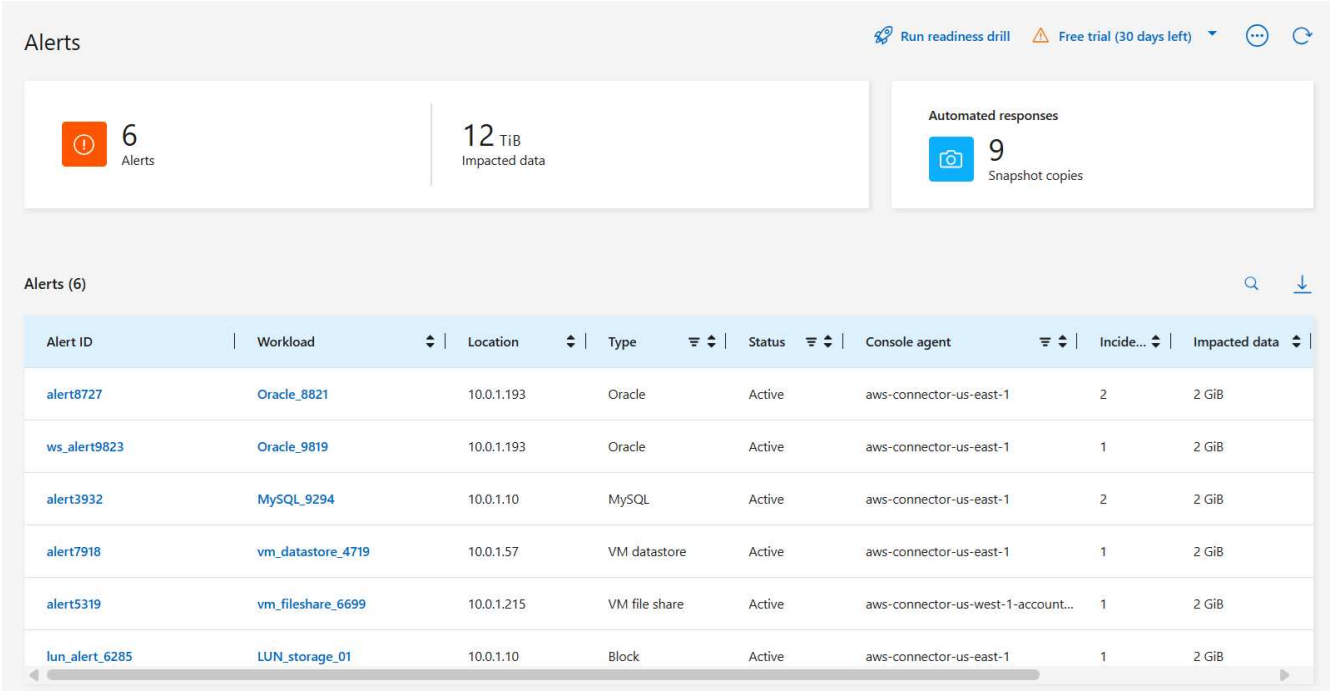
Wenn Sie eine Arbeitslast verwerfen, werden alle Snapshot-Kopien, die automatisch als Reaktion auf einen potenziellen Ransomware-Angriff erstellt wurden, dauerhaft gelöscht.

Wenn Sie eine Warnung verwerfen, können Sie diesen Status nicht wieder in einen anderen Status ändern und diese Änderung auch nicht rückgängig machen.

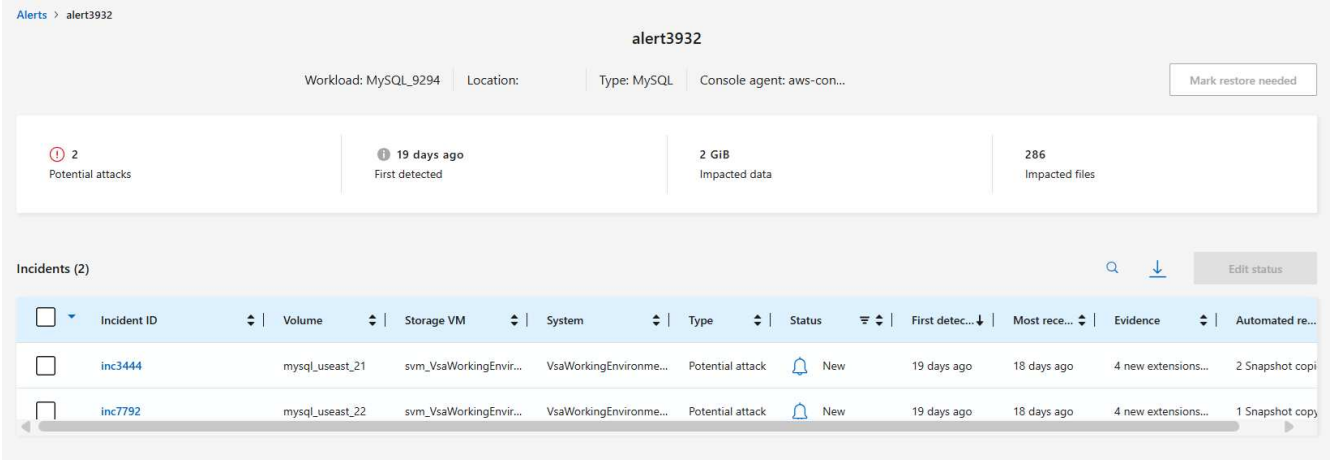
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

Schritte

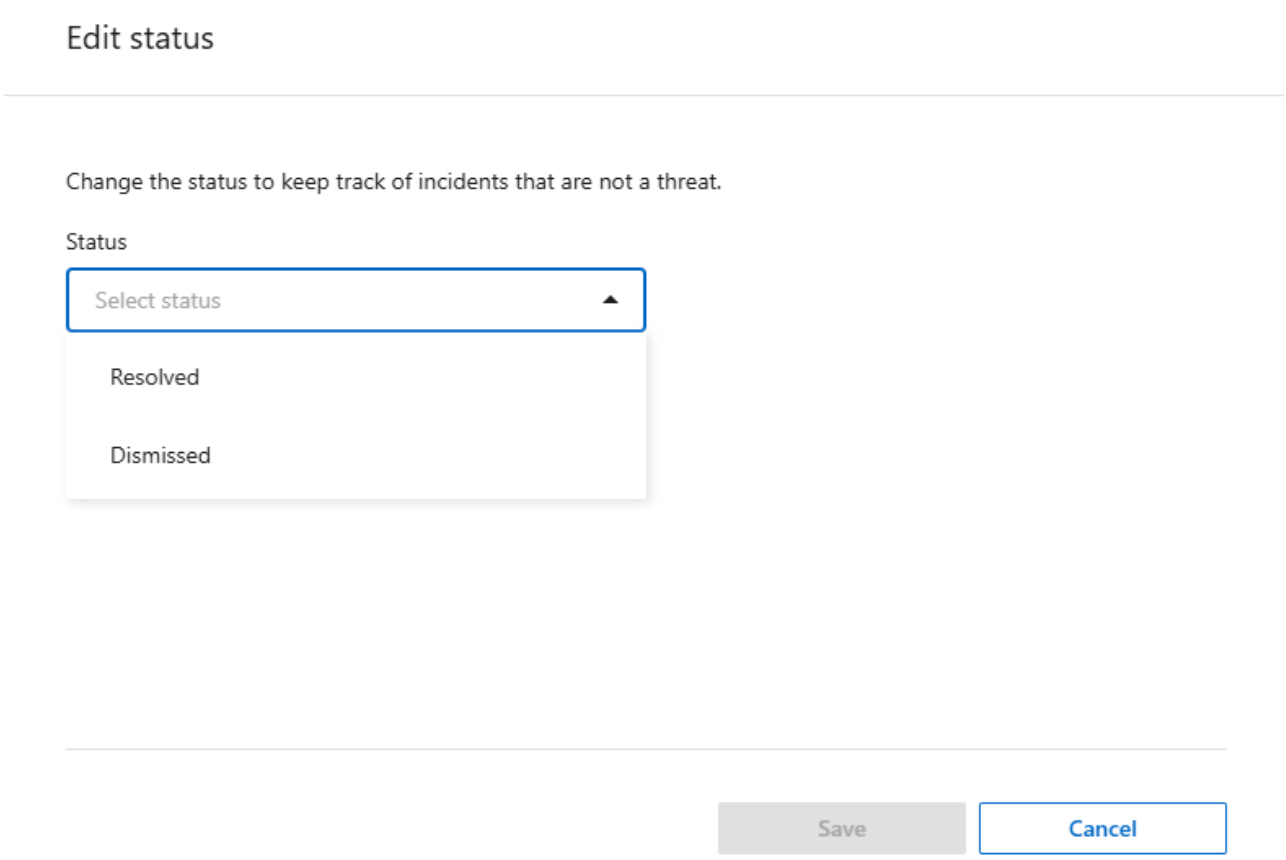
1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.



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



3. Wählen Sie einen oder mehrere Vorfälle aus. Oder wählen Sie alle Vorfälle aus, indem Sie das Feld „Vorfall-ID“ oben links in der Tabelle auswählen.
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 Feld „Status bearbeiten“ den Status **„Abgelehnt“** aus.

   Es werden zusätzliche Informationen zur Arbeitslast und zum Löschen von Snapshot-Kopien angezeigt.

6. Wählen Sie **Speichern**.

   Der Status des Vorfalls bzw. der Vorfälle ändert sich in „Abgelehnt“.

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.

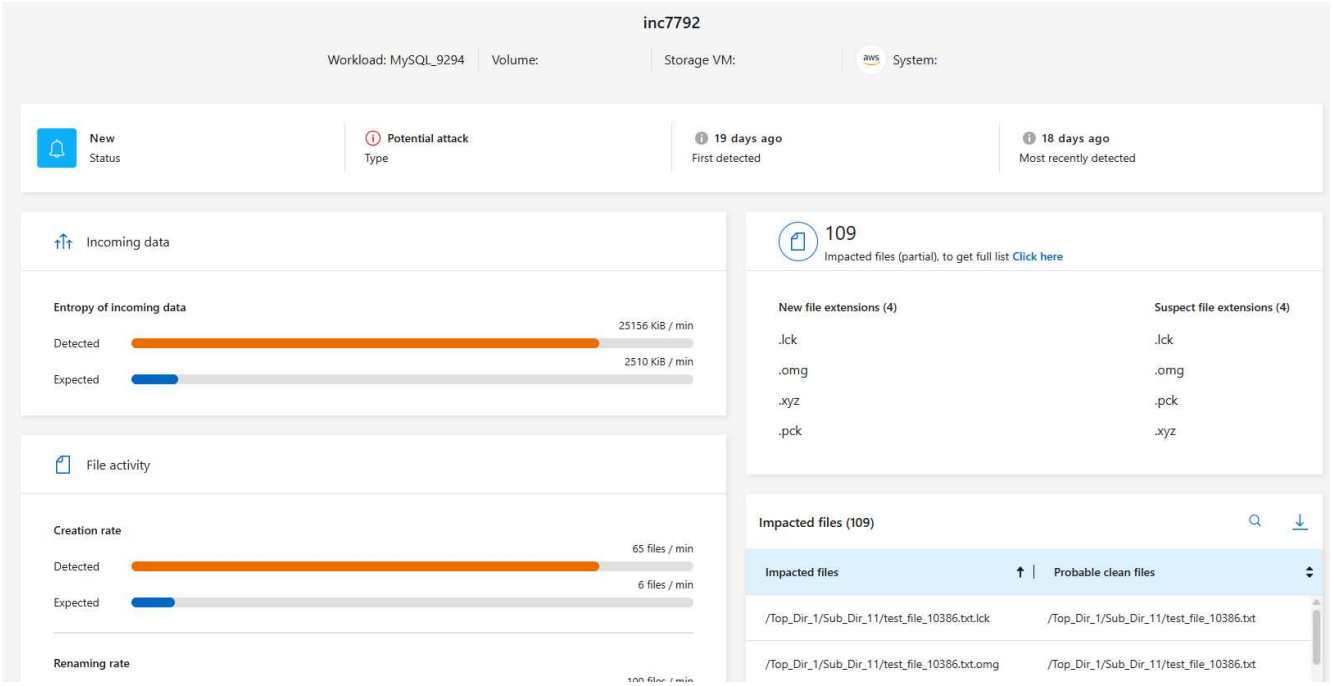
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

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 und laden Sie die Liste der betroffenen Dateien im CSV-Format herunter.

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:

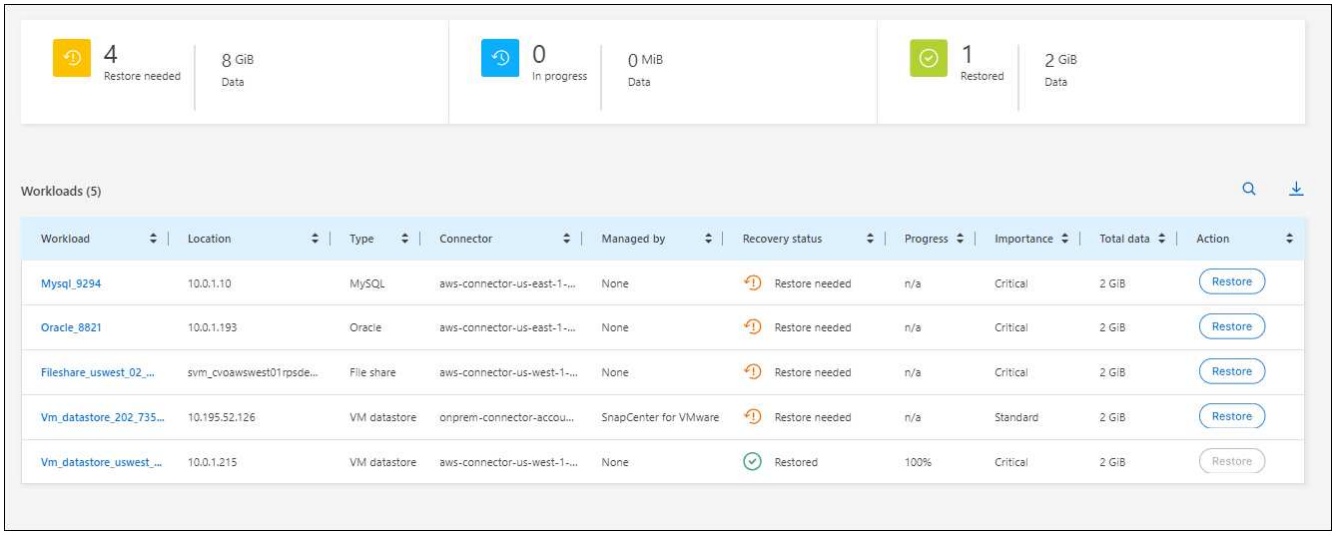
- **Wiederherstellung erforderlich**: Die Arbeitslast muss wiederhergestellt werden.
- **In Bearbeitung**: Der Wiederherstellungsvorgang ist derzeit im Gange.
- **Wiederhergestellt**: Die Arbeitslast wurde wiederhergestellt.
- **Fehlgeschlagen**: Der Workload-Wiederherstellungsprozess konnte nicht abgeschlossen 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 für „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 die Konsolenzugriffsrollen für alle Dienste" .

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 die Konsolenzugriffsrollen für alle Dienste" .

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

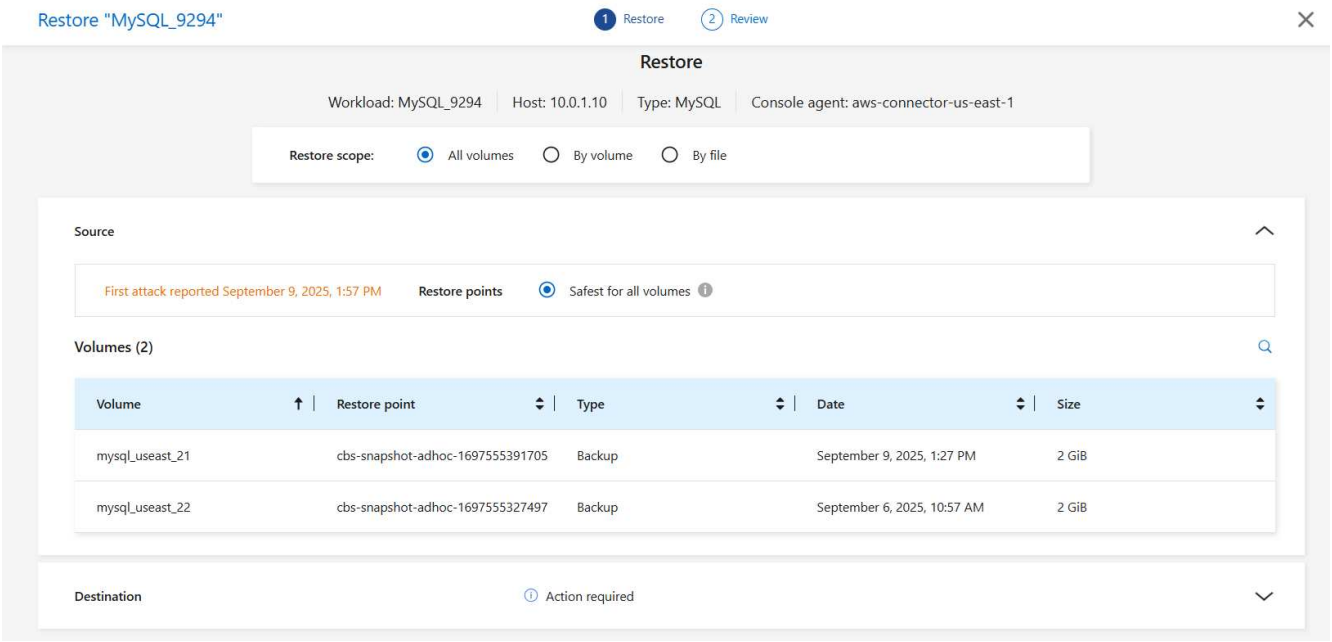
1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
2. Überprüfen Sie die Arbeitslastinformationen auf der Seite **Wiederherstellung**.
3. Wählen Sie eine Arbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.
4. Wählen Sie zum Wiederherstellen **Wiederherstellen**.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

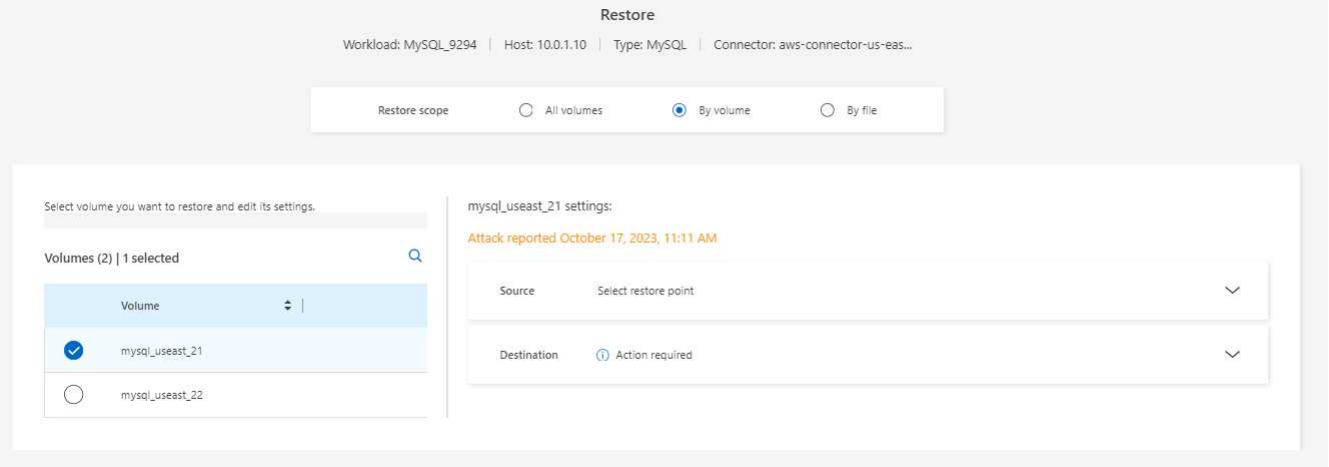
> Der neue Datenträgername wird als Präfix + ursprünglicher Datenträgername + Sicherungsname + Sicherungsdatum angezeigt.

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.

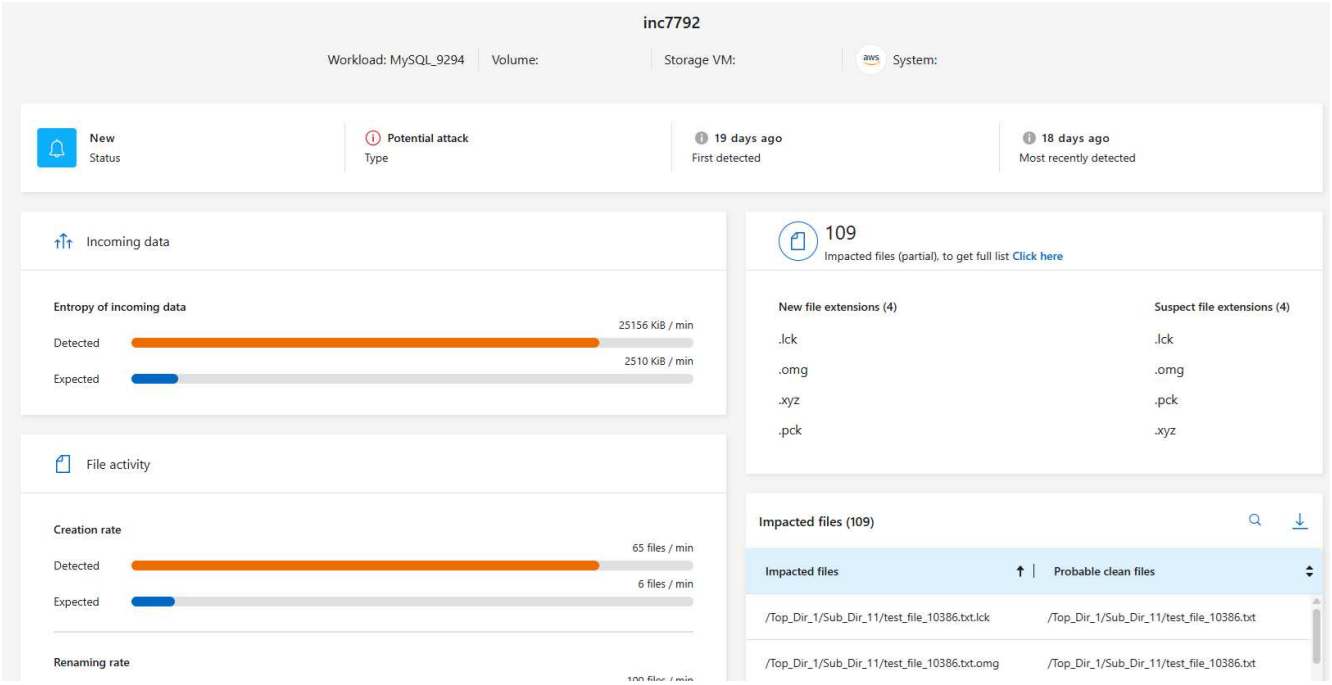
Sie können eine Anwendungs-Workload auf Dateiebene auf demselben oder einem anderen System wiederherstellen.

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.

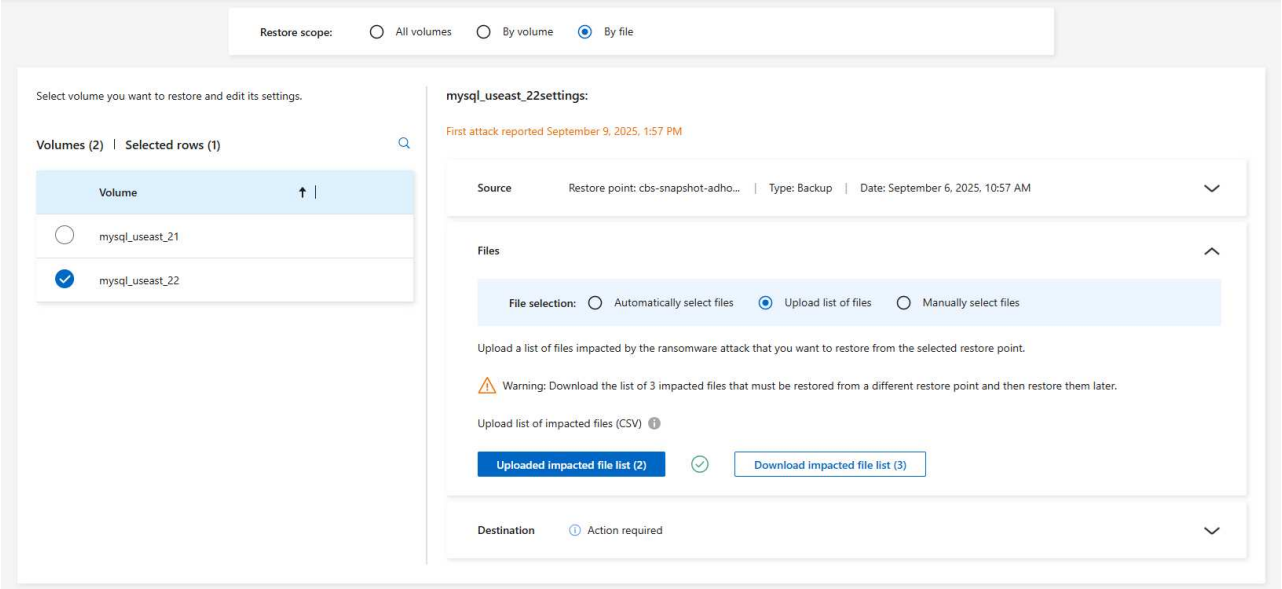
Schritte zum Wiederherstellen dieser Dateien

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Wiederherstellung“ aus.
2. Wählen Sie eine Anwendungsarbeitslast aus, die sich im Status „Wiederherstellung erforderlich“ befindet.

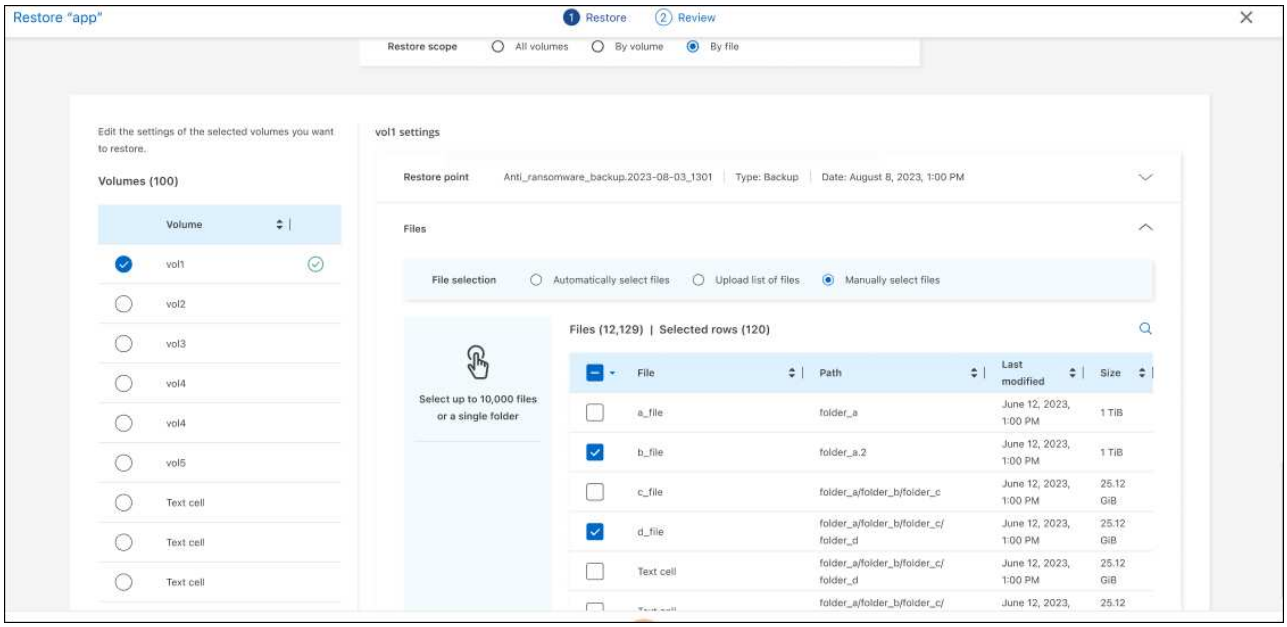
3. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
4. Wählen Sie auf der Seite „Wiederherstellen“ im Wiederherstellungsbereich die Option „Nach Datei“ aus.
5. Wählen Sie in der Volumeliste das Volume aus, das die Dateien enthält, die Sie wiederherstellen möchten.
6. **Wiederherstellungspunkt**: 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.

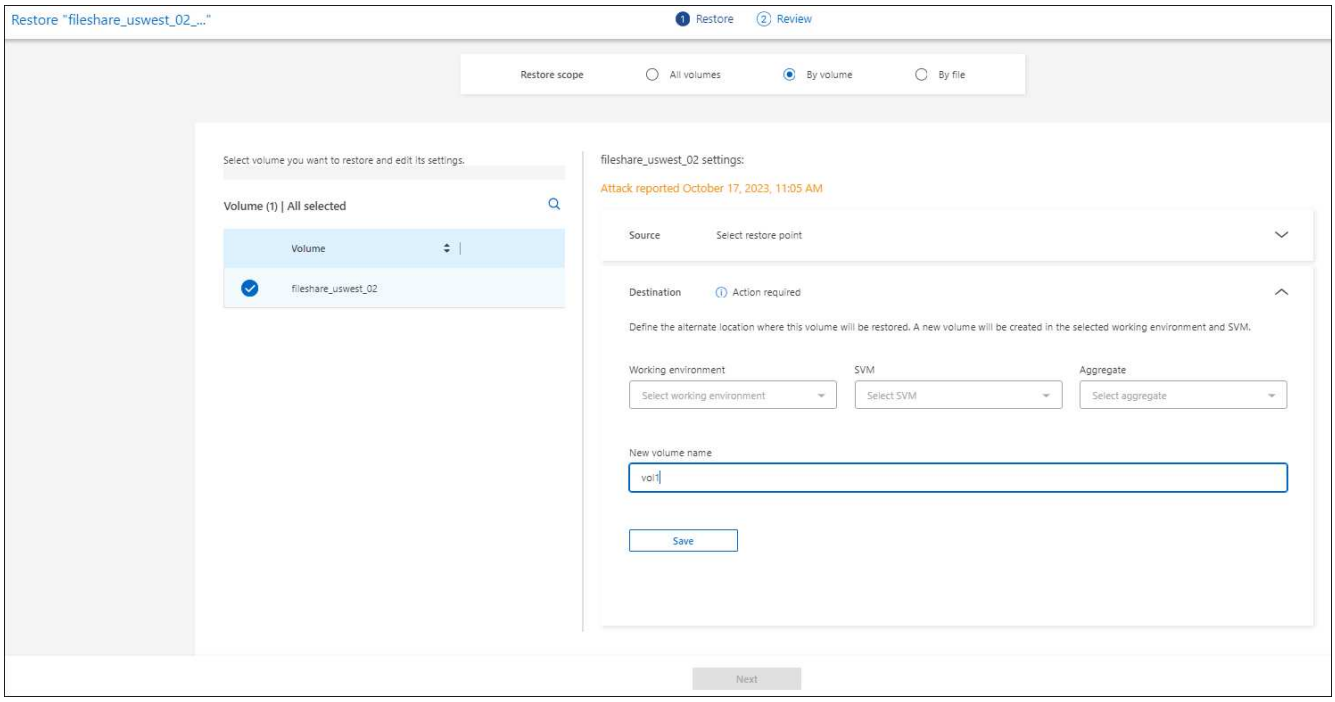
   b. Wählen Sie das System aus.
   c. Wählen Sie die Speicher-VM aus.
   d. Geben Sie optional den Pfad ein.

      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.

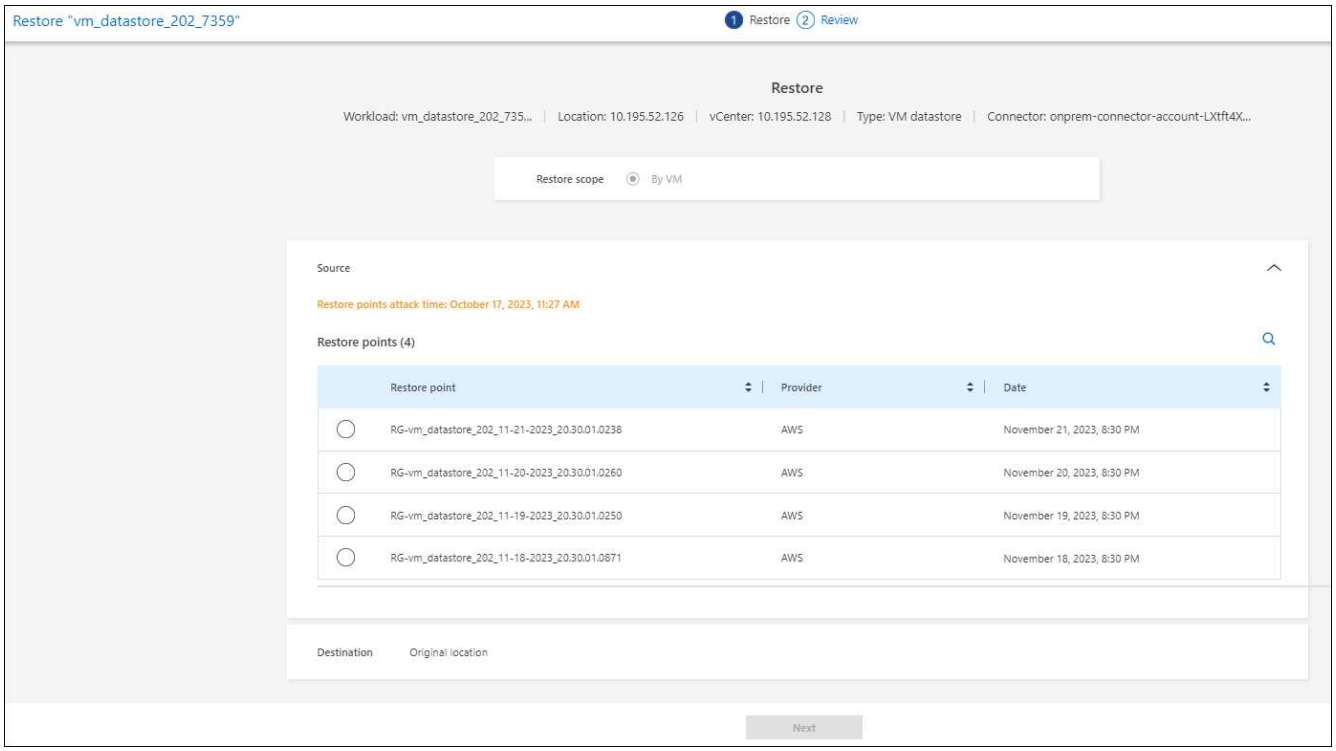
5. Wählen Sie **Speichern**.

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

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 Seite „Wiederherstellung“ zu überprüfen, auf der der Status des Vorgangs durch die verschiedenen Zustände geht.

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, sollten Sie die Daten aktualisieren. Dadurch werden auch die in den Dateien angezeigten Daten aktualisiert.

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 BlueXP -Zugriffsrollen für alle Dienste" .

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

- **Schutz**: Enthält 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.

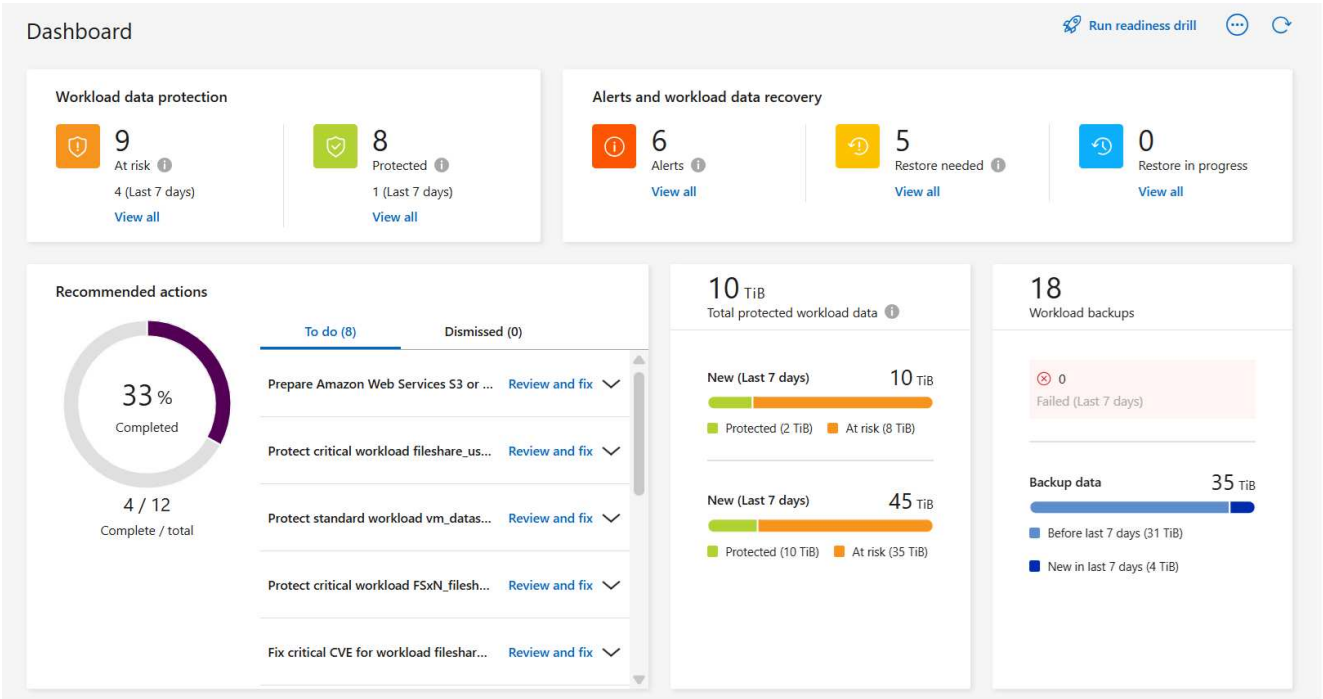
Sie können Bereitschaftsübungsberichte nur von der Seite **Berichte** herunterladen.

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

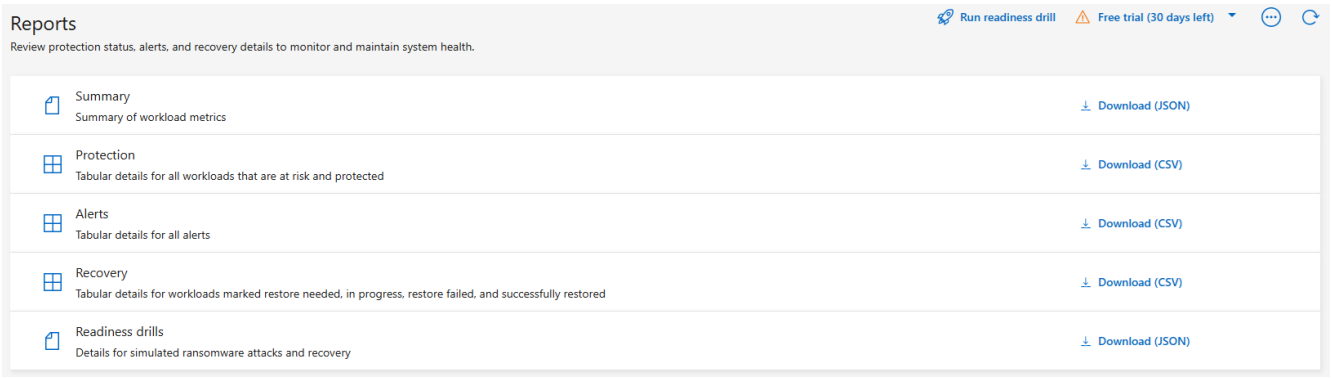
1. Wählen Sie in der linken Navigationsleiste der Konsole **Schutz** > **Ransomware-Resilienz** aus.



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**.



Wissen und Unterstützung

Für Support registrieren

Um technischen Support speziell für BlueXP und seine Speicherlösungen und -dienste zu erhalten, ist eine Support-Registrierung erforderlich. Eine Support-Registrierung ist auch erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu aktivieren.

Durch die Registrierung für den Support wird kein NetApp Support für den Dateidienst eines Cloud-Anbieters aktiviert. Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der BlueXP -Dokumentation für das jeweilige Produkt.

- "Amazon FSx für ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Übersicht zur Support-Registrierung

Zur Aktivierung des Supportanspruchs stehen zwei Registrierungsformen zur Verfügung:

- Registrieren Sie die Seriennummer Ihres BlueXP Kontos (Ihre 20-stellige Seriennummer 960xxxxxxxx, die Sie auf der Support-Ressourcenseite in BlueXP finden).

  Dies dient als Ihre einzige Support-Abonnement-ID für alle Dienste innerhalb von BlueXP. Jedes Support-Abonnement auf BlueXP -Kontoebene muss registriert werden.

- Registrieren Sie die mit einem Abonnement verknüpften Cloud Volumes ONTAP Seriennummern im Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxxx-Seriennummern).

  Diese Seriennummern werden allgemein als *PAYGO-Seriennummern* bezeichnet und von BlueXP zum Zeitpunkt der Bereitstellung von Cloud Volumes ONTAP generiert.

Durch die Registrierung beider Seriennummerntypen werden Funktionen wie das Öffnen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird abgeschlossen, indem Sie wie unten beschrieben NetApp Support Site (NSS)-Konten zu BlueXP hinzufügen.

Registrieren Sie BlueXP für NetApp Support

Um sich für den Support zu registrieren und den Supportanspruch zu aktivieren, muss ein Benutzer in Ihrer BlueXP -Organisation (oder Ihrem Konto) ein NetApp Support Site-Konto mit seinem BlueXP Login verknüpfen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über ein NetApp Support Site (NSS)-Konto verfügen.

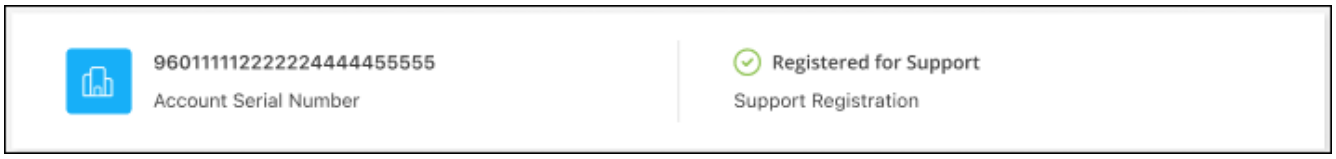
Bestandskunde mit NSS-Konto

Wenn Sie NetApp -Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Authentifizierungsaufforderung der NetApp Support Site (NSS).
4. Um zu bestätigen, dass der Registrierungsvorgang erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihre BlueXP -Organisation für den Support registriert ist.

   Beachten Sie, dass anderen BlueXP Benutzern dieser Support-Registrierungsstatus nicht angezeigt wird, wenn sie ihrem BlueXP Login kein NetApp -Support-Site-Konto zugeordnet haben. Dies bedeutet jedoch nicht, dass Ihre BlueXP -Organisation nicht für den Support registriert ist. Sofern ein Benutzer in der Organisation diese Schritte befolgt hat, ist Ihre Organisation registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp -Kunde mit vorhandenen Lizenzen und Seriennummern, aber *keinem* NSS-Konto sind, müssen Sie ein NSS-Konto erstellen und es mit Ihrem BlueXP Login verknüpfen.

Schritte

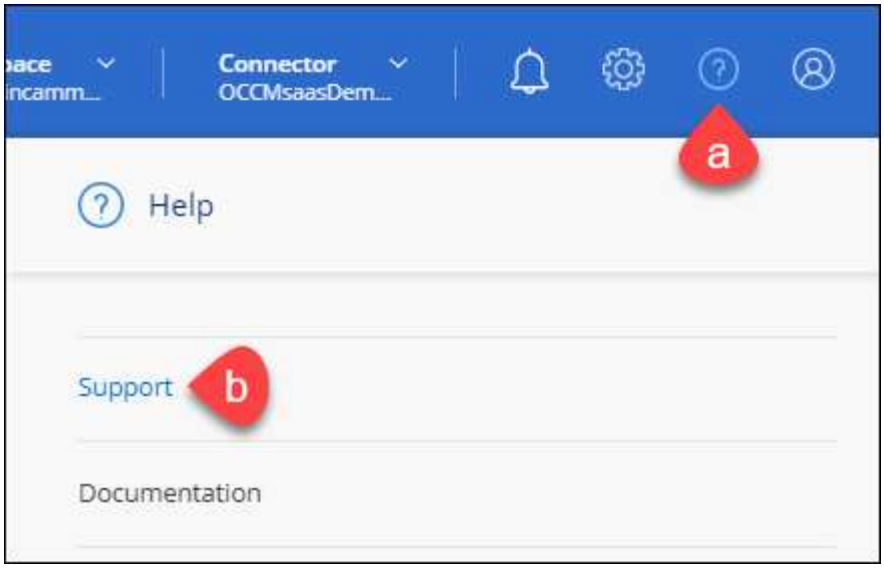
1. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die Seriennummer des BlueXP -Kontos (960xxxx) zu kopieren, die oben für das Feld „Seriennummer“ verwendet wurde. Dies beschleunigt die Kontobearbeitung.
2. Verknüpfen Sie Ihr neues NSS-Konto mit Ihrem BlueXP -Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

Ganz neu bei NetApp

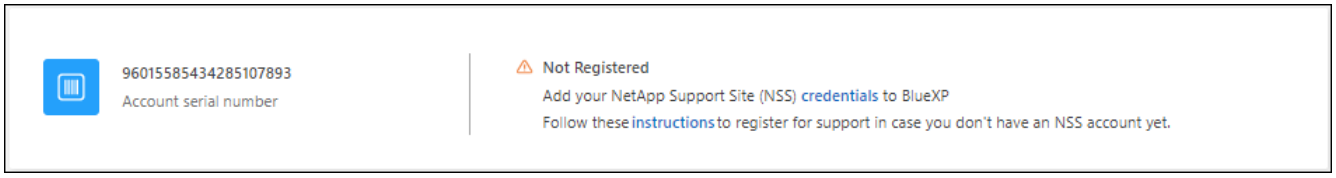
Wenn Sie NetApp noch nicht kennen und kein NSS-Konto haben, befolgen Sie die nachstehenden Schritte.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol und dann **Support** aus.



2. Suchen Sie auf der Support-Registrierungsseite nach der Seriennummer Ihrer Konto-ID.



3. Navigieren Sie zu "Support-Registrierungssite von NetApp" und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder (mit roten Sternchen gekennzeichnet) aus.
5. Wählen Sie im Feld **Produktlinie Cloud Manager** und dann Ihren entsprechenden Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer Ihres Kontos aus Schritt 2 oben, schließen Sie die Sicherheitsüberprüfung ab und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

   Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an das angegebene Postfach gesendet. Überprüfen Sie unbedingt Ihren Spam-Ordner, wenn die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Bestätigen Sie die Aktion in der E-Mail.

   Durch die Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, dass Sie ein NetApp Support Site-Konto erstellen.

8. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die oben für das Seriennummernfeld verwendete Kontoseriennummer (960xxxx) zu kopieren. Dadurch wird die Bearbeitung beschleunigt.

Nach Abschluss

NetApp sollte sich während dieses Vorgangs mit Ihnen in Verbindung setzen. Dies ist eine einmalige

Onboarding-Übung für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, verknüpfen Sie das Konto mit Ihrem BlueXP -Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen

Die Verknüpfung der Anmeldeinformationen der NetApp Support Site mit Ihrer BlueXP -Organisation ist erforderlich, um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu aktivieren:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für den Support

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugriff auf die technischen Supportressourcen von NetApp zu erhalten.

- Bereitstellen von Cloud Volumes ONTAP mit eigener Lizenz (BYOL)

  Die Angabe Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Hierzu gehören automatische Updates bei Laufzeitverlängerungen.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

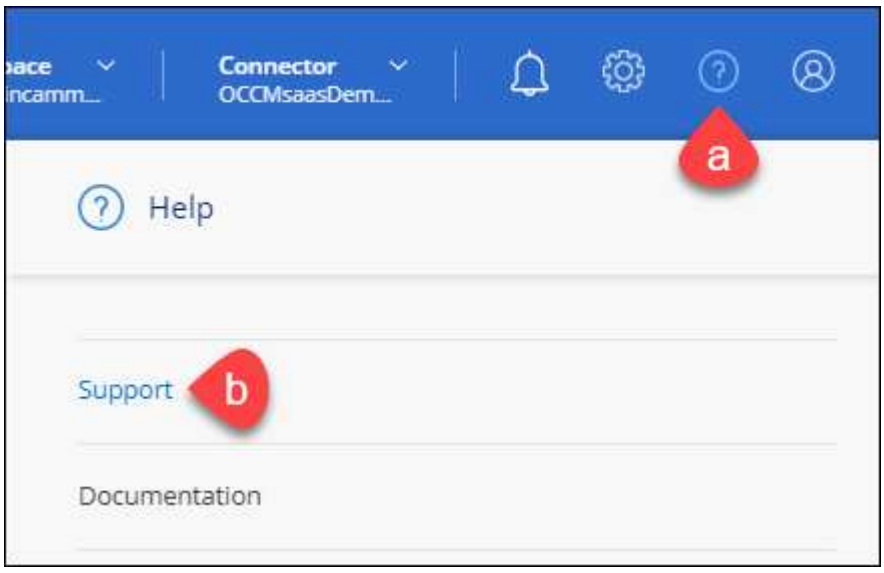
Das Verknüpfen von NSS-Anmeldeinformationen mit Ihrer BlueXP Organisation unterscheidet sich vom Verknüpfen des NSS-Kontos mit einer BlueXP Benutzeranmeldung.

Diese NSS-Anmeldeinformationen sind mit Ihrer spezifischen BlueXP -Organisations-ID verknüpft. Benutzer, die zur BlueXP -Organisation gehören, können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie über ein Partner- oder Reseller-Konto verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen, diese können jedoch nicht zusammen mit Konten auf Kundenebene hinzugefügt werden.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol und dann **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste speziell für Support und Lizenzierung.

4. Geben Sie auf der Anmeldeseite Ihre bei der NetApp Support Site registrierte E-Mail-Adresse und Ihr Kennwort ein, um den Authentifizierungsprozess durchzuführen.

   Diese Aktionen ermöglichen BlueXP , Ihr NSS-Konto für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder temporäres Konto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto geben, wenn es sich bei diesem Konto um ein Konto auf Partnerebene handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

   Dasselbe gilt, wenn Sie bereits über NSS-Konten auf Kundenebene verfügen und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS-Verwaltung** können Sie Ihre E-Mail-Adresse aus dem ••• Speisekarte.

   - Wenn Sie Ihre Anmeldeinformationen aktualisieren müssen, gibt es auch die Option **Anmeldeinformationen aktualisieren** im ••• Speisekarte.

     Bei Verwendung dieser Option werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Sie werden durch eine entsprechende Benachrichtigung darauf aufmerksam gemacht.

Hilfe erhalten

NetApp bietet Support für BlueXP und seine Cloud-Services auf vielfältige Weise. Umfangreiche kostenlose Self-Support-Optionen stehen Ihnen rund um die Uhr zur Verfügung, darunter Knowledgebase-Artikel und ein Community-Forum. Ihre Support-Registrierung beinhaltet technischen Remote-Support per Web-Ticketing.

Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters

Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der BlueXP -Dokumentation für das jeweilige Produkt.

- "Amazon FSx für ONTAP"

- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Um technischen Support speziell für BlueXP und seine Speicherlösungen und -dienste zu erhalten, verwenden Sie die unten beschriebenen Supportoptionen.

Nutzen Sie Möglichkeiten zur Selbsthilfe

Diese Optionen stehen Ihnen 24 Stunden am Tag, 7 Tage die Woche kostenlos zur Verfügung:

- Dokumentation

  Die BlueXP -Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Durchsuchen Sie die BlueXP Wissensdatenbank nach hilfreichen Artikeln zur Problembehebung.

- "Gemeinschaften"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu starten.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie nach der Aktivierung des Supports mit einem NetApp -Support-Spezialisten zusammenarbeiten, um alle Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** zu verwenden, müssen Sie zunächst Ihre Anmeldeinformationen für die NetApp -Support-Site mit Ihrem BlueXP Login verknüpfen. "Erfahren Sie, wie Sie die mit Ihrem BlueXP Login verknüpften Anmeldeinformationen verwalten" .
- Wenn Sie einen Fall für ein ONTAP -System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer für dieses System verknüpft sein.

Schritte

1. Wählen Sie in BlueXP*Hilfe > Support*.
2. Wählen Sie auf der Seite **Ressourcen** unter „Technischer Support“ eine der verfügbaren Optionen aus:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem telefonieren möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket bei einem NetApp -Support-Spezialisten zu öffnen:

      - **Dienst**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispielsweise BlueXP , wenn es sich um ein spezielles technisches Supportproblem mit Arbeitsabläufen oder Funktionen innerhalb des Dienstes handelt.
      - **Arbeitsumgebung**: Wählen Sie, falls für den Speicher zutreffend, * Cloud Volumes ONTAP* oder **On-Prem** und dann die zugehörige Arbeitsumgebung aus.

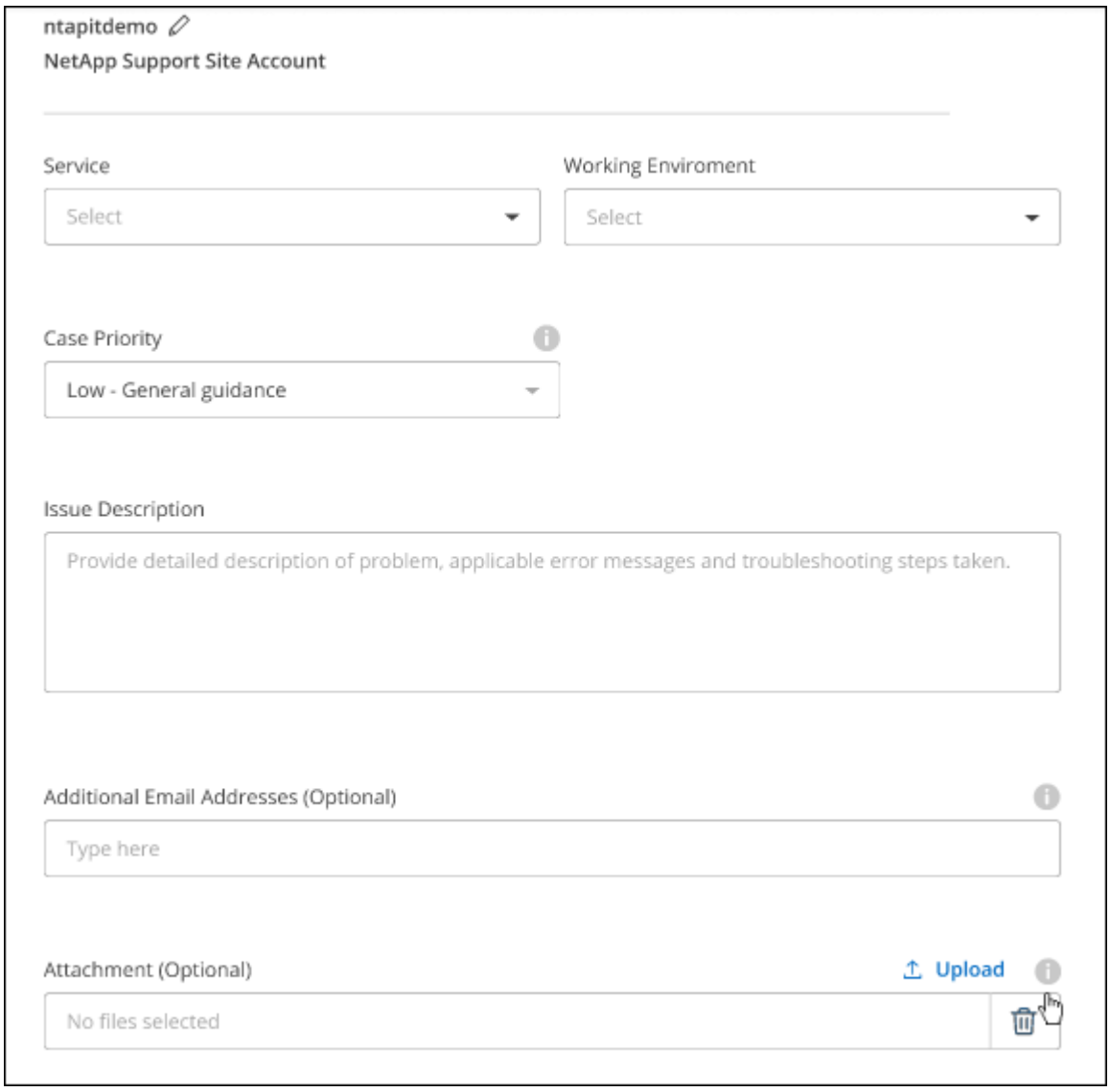
        Die Liste der Arbeitsumgebungen liegt im Rahmen der BlueXP -Organisation (oder des Kontos), des Projekts (oder Arbeitsbereichs) und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Fallpriorität**: Wählen Sie die Priorität für den Fall. Sie kann „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“ sein.

  Um weitere Einzelheiten zu diesen Prioritäten zu erfahren, bewegen Sie die Maus über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller zutreffenden Fehlermeldungen oder Schritte zur Fehlerbehebung, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderen auf dieses Problem aufmerksam machen möchten.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge hoch, einen nach dem anderen.

  Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nach Abschluss

Ein Popup mit Ihrer Support-Fallnummer wird angezeigt. Ein NetApp -Support-Spezialist wird Ihren Fall prüfen und sich in Kürze bei Ihnen melden.

Um einen Verlauf Ihrer Supportfälle anzuzeigen, können Sie **Einstellungen > Zeitleiste** auswählen und nach Aktionen mit der Bezeichnung „Supportfall erstellen“ suchen. Über eine Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Beim Versuch, einen Fall zu erstellen, kann es sein, dass die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Dienst zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das damit verknüpfte Unternehmen nicht dasselbe Unternehmen sind, für das die Seriennummer des BlueXP Kontos gilt (d. h. 960xxxx) oder die Seriennummer der Arbeitsumgebung. Sie können auf eine der folgenden Arten Hilfe anfordern:

- Verwenden Sie den Chat im Produkt
- Senden Sie einen nicht-technischen Fall an https://mysupport.netapp.com/site/help

Verwalten Sie Ihre Supportfälle (Vorschau)

Sie können aktive und gelöste Supportfälle direkt von BlueXP aus anzeigen und verwalten. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle verwalten.

Das Fallmanagement ist als Vorschau verfügbar. Wir planen, dieses Erlebnis zu verfeinern und in kommenden Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Feedback über den Chat im Produkt.

Beachten Sie Folgendes:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht links zeigt die Gesamtzahl der Fälle, die in den letzten drei Monaten von dem von Ihnen angegebenen NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht rechts zeigt die Gesamtzahl der in den letzten drei Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die mit der von Ihnen ausgewählten Ansicht in Zusammenhang stehen.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie „Priorität“ und „Status“ filtern. Andere Spalten bieten lediglich Sortierfunktionen.

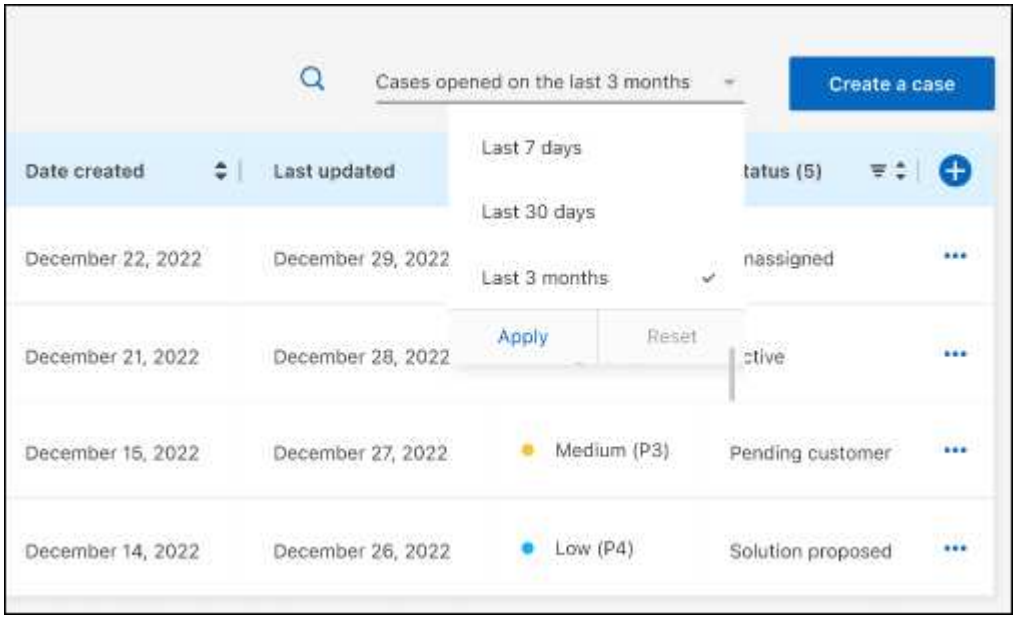
  Weitere Einzelheiten finden Sie in den folgenden Schritten.
- Auf Einzelfallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Ausstehend abgeschlossen“ befindet.

Schritte

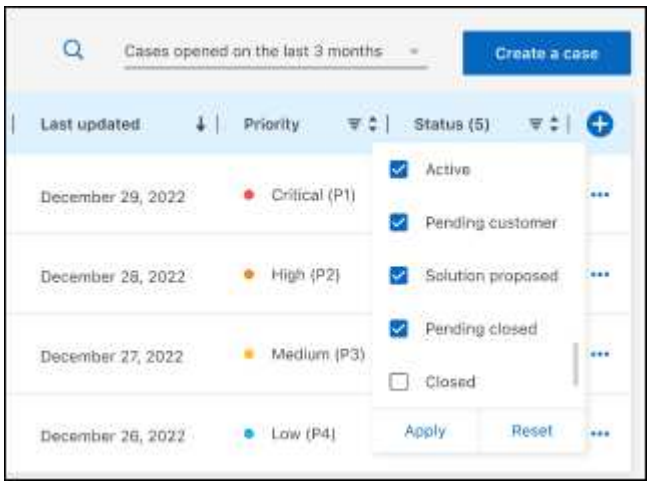
1. Wählen Sie in BlueXP*Hilfe > Support*.
2. Wählen Sie **Fallmanagement** und fügen Sie Ihr NSS-Konto zu BlueXP hinzu, wenn Sie dazu aufgefordert werden.

   Auf der Seite **Fallverwaltung** werden offene Fälle angezeigt, die sich auf das NSS-Konto beziehen, das mit Ihrem BlueXP -Benutzerkonto verknüpft ist. Dies ist dasselbe NSS-Konto, das oben auf der **NSS-Verwaltungsseite** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:

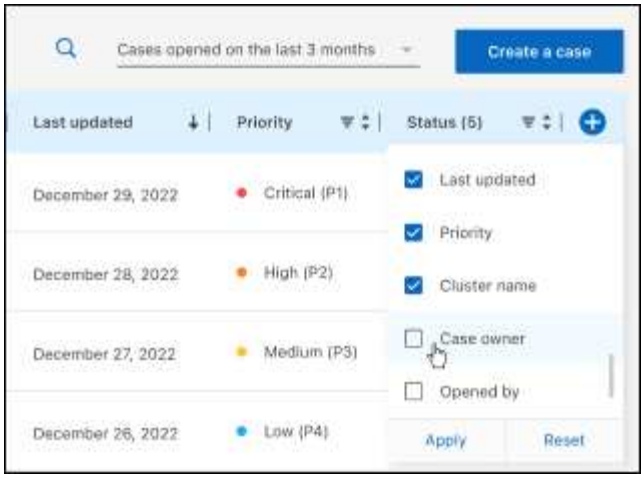
- Wählen Sie unter **Fälle der Organisation** die Option **Anzeigen** aus, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
- Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.



- Filtern Sie den Inhalt der Spalten.



- Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie und wählen Sie dann die Spalten aus, die Sie anzeigen möchten.

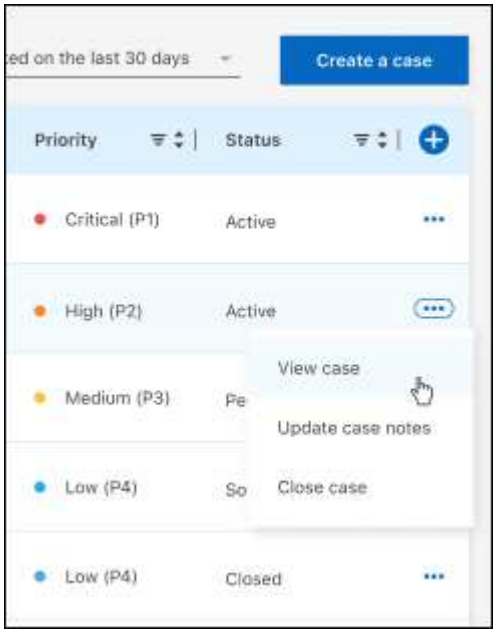


4. Verwalten Sie einen vorhandenen Fall, indem Sie ••• und wählen Sie eine der verfügbaren Optionen aus:

   - **Fall anzeigen**: Alle Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Details zum Grund für das Schließen des Falls an und wählen Sie **Fall schließen** aus.



Häufig gestellte Fragen zur NetApp Ransomware Resilience

Diese FAQ können hilfreich sein, wenn Sie nur eine schnelle Antwort auf eine Frage zu NetApp Ransomware Resilience suchen.

Einsatz

Benötigen Sie eine Lizenz zur Nutzung von Ransomware Resilience?

Sie können die folgenden Lizenztypen verwenden:

- Melden Sie sich für eine 30-tägige kostenlose Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) für NetApp Intelligent Services und Ransomware Resilience über Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace und Microsoft Azure Marketplace.
- Bringen Sie Ihre eigene Lizenz (BYOL) mit. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL im Abschnitt „Lizenzen und Abonnements“ der Konsole zu aktivieren.

Wie aktivieren Sie Ransomware-Resilienz? Für Ransomware Resilience ist keine Aktivierung erforderlich. Sie können über die NetApp -Konsole auf Ransomware Resilience zugreifen.

Um loszulegen, müssen Sie sich anmelden oder sich an Ihren NetApp Vertriebsmitarbeiter wenden, um diesen Service auszuprobieren. Wenn Sie dann den Konsolenagenten verwenden, enthält dieser die entsprechenden Funktionen für Ransomware-Resilienz.

Um mit Ransomware Resilience zu beginnen, wählen Sie auf der Zielseite „Workloads ermitteln“ aus.

Ist Ransomware Resilience im Standard-, eingeschränkten und privaten Modus verfügbar? Derzeit ist Ransomware Resilience nur im Standardmodus verfügbar. Bleiben Sie dran für mehr.

Eine Erläuterung dieser Modi für alle NetApp -Datendienste finden Sie unter "Bereitstellungsmodi der NetApp Konsole" .

Zugang

Wie lautet die Ransomware-Resilience-URL? Geben Sie in einem Browser ein "https://console.netapp.com/ransomware-resilience" um auf die Konsole zuzugreifen.

Wie werden Zugriffsberechtigungen gehandhabt? "Erfahren Sie mehr über die Konsolenzugriffsrollen für alle Dienste" .

Welche Geräteauflösung ist am besten? Die empfohlene Geräteauflösung für Ransomware Resilience beträgt 1920 x 1080 oder besser.

Welchen Browser sollte ich verwenden? Jeder moderne Browser.

Interaktion mit anderen Diensten

Ist Ransomware Resilience über die in NetApp ONTAP vorgenommenen Schutzeinstellungen informiert? Ja, Ransomware Resilience erkennt in ONTAP festgelegte Snapshot-Zeitpläne.

Wenn Sie eine Richtlinie mit Ransomware Resilience festlegen, müssen Sie zukünftige Änderungen nur in diesem Dienst vornehmen? Wir empfehlen Ihnen, Richtlinienänderungen von Ransomware Resilience vorzunehmen.

Wie interagiert Ransomware Resilience mit NetApp Backup and Recovery und SnapCenter?

Ransomware Resilience verwendet die folgenden Produkte und Dienste:

- Backup und Wiederherstellung zum Ermitteln und Festlegen von Snapshot- und Backup-Richtlinien für Dateifreigabe-Workloads
- SnapCenter oder SnapCenter für VMware zum Erkennen und Festlegen von Snapshot- und Backup-Richtlinien für Anwendungs- und VM-Workloads.

Darüber hinaus verwendet Ransomware Resilience Backup and Recovery und SnapCenter / SnapCenter für VMware, um eine datei- und workloadkonsistente Wiederherstellung durchzuführen.

Arbeitslasten

Was macht eine Arbeitsbelastung aus? Eine Workload ist eine Anwendung, eine VM oder eine Dateifreigabe. Eine Arbeitslast umfasst alle Volumes, die von einer einzelnen Anwendungsinstanz verwendet werden. Beispielsweise kann eine auf ora3.host.com bereitgestellte Oracle DB-Instance für ihre Daten bzw. Protokolle über vol1 und vol2 verfügen. Diese Volumes bilden zusammen die Arbeitslast für diese bestimmte Instanz der Oracle-DB-Instanz.

Wie priorisiert Ransomware Resilience Workload-Daten? Die Datenpriorität wird durch die erstellten Snapshot-Kopien und geplanten Backups bestimmt.

Die Workload-Priorität (kritisch, Standard, wichtig) wird durch die Snapshot-Häufigkeiten bestimmt, die bereits auf jedes mit dem Workload verknüpfte Volume angewendet werden.

"Informieren Sie sich über die Priorität oder Wichtigkeit der Arbeitslast" .

Welche Workloads unterstützt Ransomware Resilience?

Ransomware Resilience kann die folgenden Workloads identifizieren: Oracle, MySQL, Dateifreigaben, Blockspeicher, VMs und VM-Datenspeicher.

Wenn Sie SnapCenter oder SnapCenter für VMware verwenden, werden außerdem alle von diesen Produkten unterstützten Workloads in Ransomware Resilience identifiziert und Ransomware Resilience kann diese Workload-konsistent schützen und wiederherstellen.

Wie verknüpfen Sie Daten mit einer Arbeitslast?

Ransomware Resilience verknüpft Daten auf folgende Weise mit einer Arbeitslast:

- Ransomware Resilience erkennt die Volumes und Dateierweiterungen und ordnet sie der entsprechenden Arbeitslast zu.
- Wenn Sie außerdem über SnapCenter oder SnapCenter für VMware verfügen und Workloads in Backup

und Recovery konfiguriert haben, erkennt Ransomware Resilience die von SnapCenter und SnapCenter für VMware verwalteten Workloads und die zugehörigen Volumes.

Was ist eine „geschützte“ Arbeitslast? Bei Ransomware Resilience zeigt eine Arbeitslast den Status „geschützt“ an, wenn für sie eine primäre Erkennungsrichtlinie aktiviert ist. Dies bedeutet vorerst, dass ARP auf allen mit der Arbeitslast verbundenen Volumes aktiviert ist.

Was ist eine „gefährdete“ Arbeitsbelastung? Wenn für einen Workload keine primäre Erkennungsrichtlinie aktiviert ist, ist er „gefährdet“, auch wenn für ihn eine Sicherungs- und Snapshot-Richtlinie aktiviert ist.

Neues Volume hinzugefügt, wird aber noch nicht angezeigt Wenn Sie Ihrer Umgebung ein neues Volume hinzugefügt haben, starten Sie die Erkennung erneut und wenden Sie Schutzrichtlinien an, um das neue Volume zu schützen.

Schutzrichtlinien

Können Ransomware-Resilience-Richtlinien gleichzeitig mit anderen Workload-Richtlinien verwendet werden? Derzeit unterstützt Backup und Recovery (Cloud Backup) eine Backup-Richtlinie pro Volume. Daher haben Backup and Recovery und Ransomware Resilience gemeinsame Sicherungsrichtlinien.

Snapshot-Kopien sind nicht begrenzt und können von jedem Dienst separat hinzugefügt werden.

Welche Richtlinien sind in einer Ransomware-Schutzstrategie erforderlich?

Die folgenden Richtlinien sind in der Ransomware-Schutzstrategie erforderlich:

- Richtlinie zur Ransomware-Erkennung
- Snapshot-Richtlinie

Eine Backup-Richtlinie ist in der Ransomware-Resilience-Strategie nicht erforderlich.

Ist Ransomware Resilience über die in NetApp ONTAP vorgenommenen Schutzeinstellungen informiert?

Ja, Ransomware Resilience erkennt in ONTAP festgelegte Snapshot-Zeitpläne und stellt fest, ob ARP und FPolicy auf allen Volumes in einer erkannten Arbeitslast aktiviert sind. Die Informationen, die Sie zunächst im Dashboard sehen, werden aus anderen NetApp -Lösungen und -Produkten aggregiert.

Ist Ransomware Resilience mit den bereits in Backup and Recovery und SnapCenter festgelegten Richtlinien vertraut?

Ja, wenn Sie Workloads in Backup and Recovery oder SnapCenter verwalten, werden die von diesen Produkten verwalteten Richtlinien in Ransomware Resilience übernommen.

Können Sie Richtlinien ändern, die von NetApp Backup and Recovery und/oder SnapCenter übernommen wurden?

Nein, Sie können von Ransomware Resilience aus keine von Backup and Recovery oder SnapCenter verwalteten Richtlinien ändern. Sie verwalten alle Änderungen an diesen Richtlinien in Backup and Recovery oder SnapCenter.

Wenn Richtlinien von ONTAP vorhanden sind (bereits im System Manager aktiviert, z. B. ARP, FPolicy und Snapshots), werden diese in Ransomware Resilience geändert?

Nein. Ransomware Resilience ändert keine vorhandenen Erkennungsrichtlinien (ARP-, FPolicy-Einstellungen)

von ONTAP.

Was passiert, wenn Sie nach der Anmeldung für Ransomware Resilience neue Richtlinien in Backup and Recovery oder SnapCenter hinzufügen?

Ransomware Resilience erkennt alle neuen Richtlinien, die in Backup and Recovery oder SnapCenter erstellt wurden.

Können Sie Richtlinien von ONTAP ändern?

Ja, Sie können Richtlinien von ONTAP in Ransomware Resilience ändern. Sie können in Ransomware Resilience auch neue Richtlinien erstellen und auf Workloads anwenden. Diese Aktion ersetzt vorhandene ONTAP -Richtlinien durch die in Ransomware Resilience erstellten Richtlinien.

Können Sie Richtlinien deaktivieren?

Sie können ARP in Erkennungsrichtlinien über die Benutzeroberfläche, APIs oder CLI des System Managers deaktivieren.

Sie können FPolicy- und Sicherungsrichtlinien deaktivieren, indem Sie eine andere Richtlinie anwenden, die diese nicht enthält.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

- "Hinweis zur NetApp Konsole"