Utilizzare la resilienza del ransomware

NetApp Ransomware Resilience

NetApp
February 27, 2026

Sommario

Utilizzare la resilienza del ransomware . . . 1
- Accedi NetApp Ransomware Resilience . . . 1
- Monitora lo stato del carico di lavoro in NetApp Ransomware Resilience . . . 2
  - Esaminare lo stato di salute del carico di lavoro utilizzando la dashboard . . . 2
  - Esaminare le raccomandazioni di protezione sulla dashboard . . . 4
  - Esporta i dati di protezione in file CSV . . . 5
  - Accedi alla documentazione tecnica . . . 6
- Proteggi e rileva . . . 6
  - Esamina lo stato di protezione in NetApp Ransomware Resilience . . . 6
  - Aggiungi una destinazione di backup in NetApp Ransomware Resilience . . . 8
  - Proteggi i carichi di lavoro con le strategie di protezione NetApp Ransomware Resilience . . . 14
  - Configura il rilevamento dell'attività dell'utente . . . 23
  - Gestire i gruppi di protezione in NetApp Ransomware Resilience . . . 34
  - Scansiona le informazioni di identificazione personale con NetApp Data Classification in Ransomware Resilience . . . 38
- Rispondere e recuperare . . . 42
  - Gestisci gli avvisi in NetApp Ransomware Resilience . . . 42
  - Recupera da un attacco ransomware (dopo che gli incidenti sono stati neutralizzati) con NetApp Ransomware Resilience . . . 50
- Esegui un'esercitazione di preparazione agli attacchi ransomware in NetApp Ransomware Resilience . . . 59
  - Configurare un'esercitazione di preparazione all'attacco ransomware . . . 59
  - Avviare un'esercitazione di preparazione . . . 61
  - Rispondere a un avviso di esercitazione di prontezza . . . 62
  - Ripristinare il carico di lavoro del test . . . 63
  - Modificare lo stato degli avvisi dopo l'esercitazione di preparazione . . . 64
  - Rivedere i rapporti sull'esercitazione di preparazione . . . 64
- Collega NetApp Ransomware Resilience al sistema di gestione della sicurezza e degli eventi (SIEM) per l'analisi e il rilevamento delle minacce . . . 65
  - Dati evento inviati a un SIEM . . . 65
  - Configurare AWS Security Hub per il rilevamento delle minacce . . . 66
  - Configurare Microsoft Sentinel per il rilevamento delle minacce . . . 67
  - Configurare Splunk Cloud per il rilevamento delle minacce . . . 69
  - Connetti SIEM alla resilienza del ransomware . . . 69
- Scarica i report in NetApp Ransomware Resilience . . . 70

Utilizzare la resilienza del ransomware

Accedi NetApp Ransomware Resilience

Per accedere a NetApp Ransomware Resilience, è necessario effettuare l'accesso tramite la NetApp Console.

Per accedere alla Console, puoi utilizzare le credenziali del sito di supporto NetApp oppure registrarti per un accesso cloud NetApp utilizzando il tuo indirizzo email e una password. "Scopri di più sull'accesso" .

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

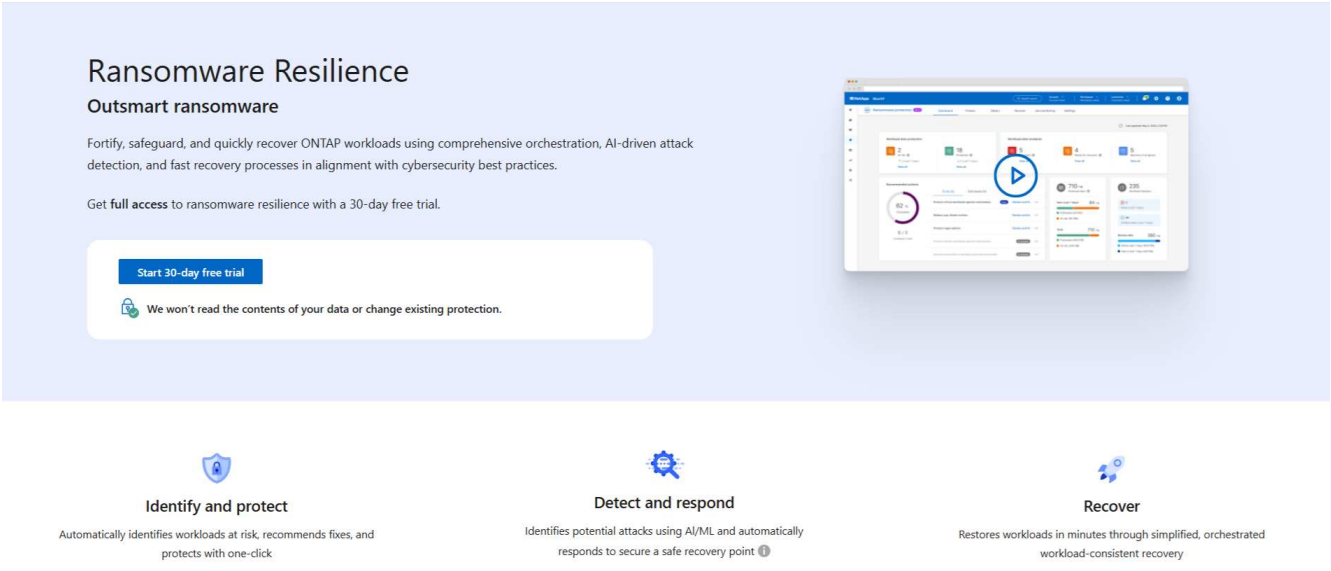
1. Apri un browser web e vai su"la console" .

   Viene visualizzata la pagina di accesso alla console.

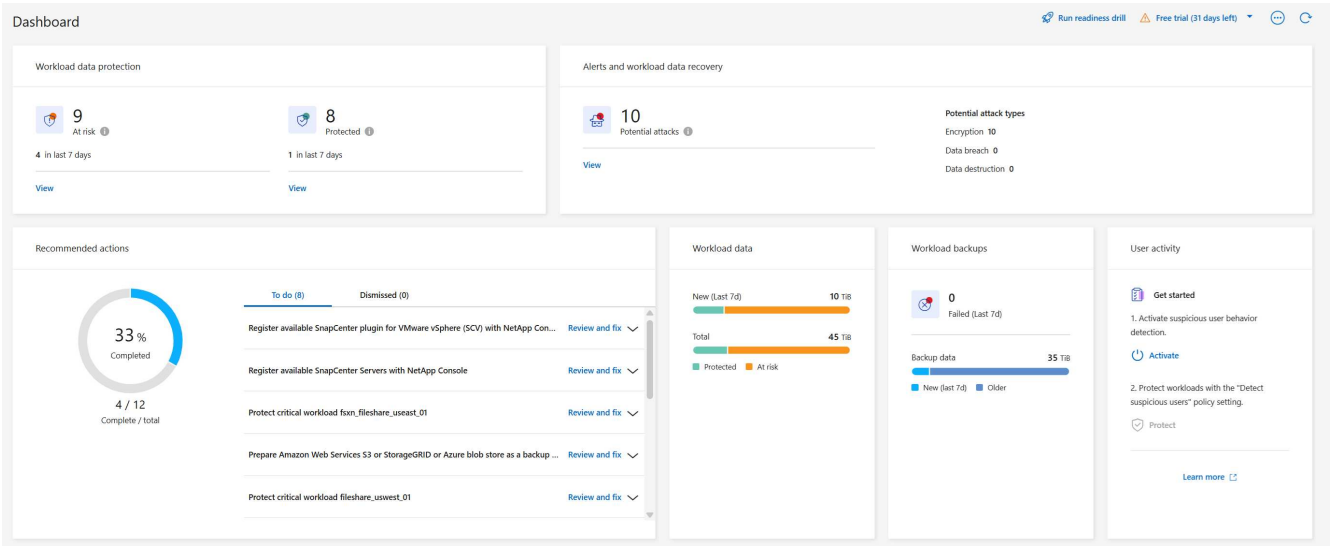
2. Accedi alla Console.
3. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.

   Se è la prima volta che accedi a questo servizio, verrà visualizzata la pagina di destinazione.

   Se non si dispone di un agente Console o non è quello adatto a questo servizio, è necessario distribuirne uno. "Scopri come configurare un agente Console" .



In caso contrario, viene visualizzata la dashboard Ransomware Resilience.



4. Se non lo hai ancora fatto, seleziona l'opzione **Scopri carichi di lavoro**.

   Fare riferimento a "Scopri i carichi di lavoro" .

Monitora lo stato del carico di lavoro in NetApp Ransomware Resilience

La dashboard NetApp Ransomware Resilience fornisce informazioni immediate sullo stato di protezione dei carichi di lavoro. È possibile individuare rapidamente i carichi di lavoro a rischio o protetti, identificare i carichi di lavoro interessati da un incidente o in fase di ripristino e valutare l'entità della protezione analizzando la quantità di storage protetto o a rischio.

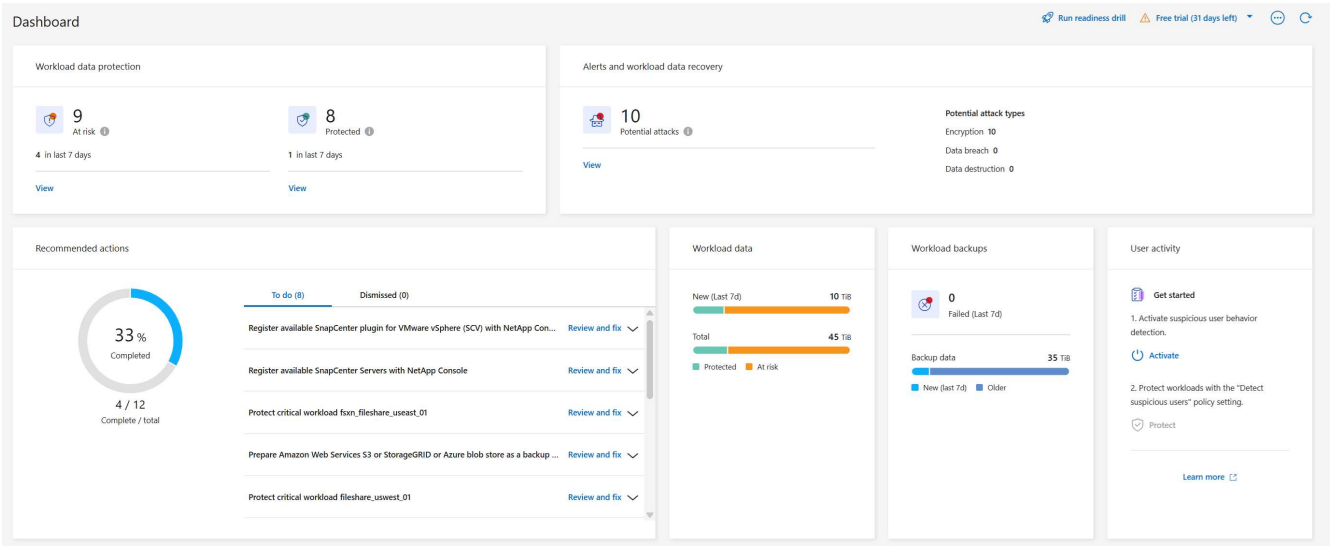
Utilizza la dashboard per rivedere i suggerimenti di protezione, modificare le impostazioni e scaricare i report.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Esaminare lo stato di salute del carico di lavoro utilizzando la dashboard

Passi

1. Dopo che la Console rileva i carichi di lavoro, la dashboard Ransomware Resilience visualizza lo stato di protezione dei dati del carico di lavoro.



2. Dalla dashboard, puoi eseguire le seguenti azioni in ciascuno dei riquadri:

   - **Protezione dei dati del carico di lavoro**: seleziona **Visualizza tutto** per visualizzare tutti i carichi di lavoro a rischio o protetti nella pagina Protezione. I carichi di lavoro sono a rischio quando i livelli di protezione non corrispondono a una policy di protezione. Fare riferimento a "Proteggere i carichi di lavoro" .

     Selezionare il suggerimento "i" per visualizzare suggerimenti su questi dati. Per aumentare il limite del carico di lavoro, seleziona **Aumenta limite del carico di lavoro** all'interno di questa nota. Selezionando questa opzione verrai indirizzato alla pagina di supporto della console, dove potrai creare un ticket di assistenza.

   - **Avvisi e ripristino dei dati del carico di lavoro**: seleziona **Visualizza tutto** per visualizzare gli incidenti attivi che hanno avuto un impatto sul tuo carico di lavoro, sono pronti per il ripristino dopo la neutralizzazione degli incidenti o sono in fase di ripristino. Fare riferimento a "Rispondere a un avviso rilevato" .
     - Un incidente è classificato in uno dei seguenti stati:
       - Nuovo
       - Licenziato
       - Licenziamento
       - Risolto
     - Un avviso può avere uno dei seguenti stati:
       - Nuovo
       - Inattivo
     - Un carico di lavoro può avere uno dei seguenti stati di ripristino:
       - Ripristino necessario
       - In corso
       - Restaurato
       - Fallito
   - **Azioni consigliate**: per aumentare la protezione, rivedi ogni raccomandazione, quindi seleziona **Rivedi e correggi**.

Vedi "Rivedi i suggerimenti di protezione sulla dashboard" o "Proteggere i carichi di lavoro".

Ransomware Resilience visualizza nuovi suggerimenti dall'ultima visita alla dashboard con il tag "Nuovo" per 24 ore. Le azioni vengono visualizzate in ordine di priorità, con la più importante in alto. Rivedi, intervieni o ignora ogni suggerimento.

Il numero totale di azioni non include le azioni che hai ignorato.

- **Dati sul carico di lavoro**: monitora le modifiche nella copertura di protezione negli ultimi 7 giorni.
- **Backup del carico di lavoro**: monitora le modifiche nei backup del carico di lavoro creati da Ransomware Resilience che non sono riusciti o sono stati completati correttamente negli ultimi 7 giorni.

Esaminare le raccomandazioni di protezione sulla dashboard

Ransomware Resilience valuta la protezione dei tuoi carichi di lavoro e consiglia azioni per migliorarla.

È possibile rivedere una raccomandazione e agire di conseguenza, modificando lo stato della raccomandazione in Completata. Oppure, se vuoi agire in seguito, puoi ignorarlo. Quando si ignora un'azione, la raccomandazione viene spostata in un elenco di azioni ignorate, che è possibile rivedere in seguito.

Ecco alcuni esempi di consigli offerti da Ransomware Resilience.

Raccomandazione	Descrizione	Come risolvere
Aggiungere una policy di protezione dal ransomware.	Al momento il carico di lavoro non è protetto.	Assegnare una policy al carico di lavoro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Connettiti al SIEM per la segnalazione delle minacce.	Inviare dati a un sistema di gestione della sicurezza e degli eventi (SIEM) per l'analisi e il rilevamento delle minacce.	Inserire i dettagli del server SIEM/XDR per abilitare il rilevamento delle minacce. Fare riferimento a "Connettersi a un SIEM".
Migliorare la sicurezza del sistema	NetApp Digital Advisor ha identificato almeno un rischio per la sicurezza elevato o critico.	Esamina tutti i rischi per la sicurezza in NetApp Digital Advisor. Fare riferimento a "Documentazione Digital Advisor" .
Rendere più forte una politica.	Alcuni carichi di lavoro potrebbero non avere una protezione sufficiente. Rafforza la protezione dei carichi di lavoro con una policy.	Aumenta la conservazione, aggiungi backup, applica backup immutabili, blocca estensioni di file sospette, abilita il rilevamento su storage secondario e molto altro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Preparare <provider di backup> come destinazione di backup per eseguire il backup dei dati del carico di lavoro.	Al momento il carico di lavoro non ha destinazioni di backup.	Aggiungi destinazioni di backup a questo workload per proteggerlo. Consulta "Aggiungi una destinazione di backup".

Raccomandazione	Descrizione	Come risolvere
Proteggi i carichi di lavoro delle applicazioni critiche o molto importanti dal ransomware.	La pagina Proteggi visualizza i carichi di lavoro delle applicazioni critici o molto importanti (in base al livello di priorità assegnato) che non sono protetti.	Assegnare una policy a questi carichi di lavoro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Proteggi i carichi di lavoro di condivisione file critici o molto importanti dal ransomware.	La pagina Protezione visualizza i carichi di lavoro critici o molto importanti di tipo Condivisione file o Datastore che non sono protetti.	Assegna una policy a ciascun workload. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware". Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware". Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware".
Esamina i nuovi avvisi.	Sono presenti nuovi avvisi.	Esamina i nuovi avvisi. Fare riferimento a "Rispondere a un avviso di ransomware rilevato" .

Passi

1. Dal riquadro Azioni consigliate in Ransomware Resilience, seleziona una raccomandazione, quindi **Esamina e correggi**.
2. Per ignorare l'azione e rimandarla a dopo, seleziona **Ignora**.

   La raccomandazione viene eliminata dall'elenco delle cose da fare e visualizzata nell'elenco delle cose ignorate.

   In seguito potrai trasformare un elemento ignorato in un elemento da fare. Quando si contrassegna un elemento come completato o si trasforma un elemento ignorato in un'azione Da fare, il totale delle azioni aumenta di 1.

3. Per rivedere le informazioni su come agire in base alle raccomandazioni, selezionare l'icona **informazioni**.

Esporta i dati di protezione in file CSV

È possibile esportare dati e scaricare file CSV che mostrano dettagli su protezione, avvisi e ripristino.

È possibile scaricare i file CSV da una qualsiasi delle opzioni del menu principale:

- **Protezione**: contiene lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale di carichi di lavoro che Ransomware Resilience contrassegna come protetti o a rischio.
- **Avvisi**: include lo stato e i dettagli di tutti gli avvisi, tra cui il numero totale di avvisi e snapshot automatici.
- **Ripristino**: include lo stato e i dettagli di tutti i carichi di lavoro che devono essere ripristinati, incluso il numero totale di carichi di lavoro che Ransomware Resilience contrassegna come "Ripristino necessario", "In corso", "Ripristino non riuscito" e "Ripristino riuscito".

Scaricando un file CSV da una pagina vengono inclusi solo i dati di quella pagina.

I file CSV includono dati per tutti i carichi di lavoro su tutti i sistemi Console.

Passi

1. Dalla dashboard Ransomware Resilience, seleziona **Aggiorna** opzione in alto a destra per aggiornare i dati che appariranno nei file.
2. Eseguire una delle seguenti operazioni:
   - Dalla pagina, seleziona **Download** opzione.
   - Dal menu Ransomware Resilience, seleziona **Report**.
3. Se hai selezionato l'opzione **Report**, seleziona uno dei file preconfigurati con nome, quindi seleziona **Scarica (CSV)** o **Scarica (JSON)**.

Accedi alla documentazione tecnica

È possibile accedere alla documentazione tecnica di Ransomware Resilience da"docs.netapp.com" o dall'interno di Ransomware Resilience.

Passi

1. Dalla dashboard Ransomware Resilience, seleziona la verticale *Azioni* opzione.
2. Seleziona una di queste opzioni:
   - **Novità** per visualizzare informazioni sulle funzionalità delle versioni attuali o precedenti nelle Note di rilascio.
   - **Documentazione** per visualizzare la documentazione di Ransomware Resilience nella home page e questa documentazione.

Proteggi e rileva

Esamina lo stato di protezione in NetApp Ransomware Resilience

La dashboard di protezione di NetApp Ransomware Resilience fornisce una panoramica dello stato di protezione e della preparazione dei tuoi carichi di lavoro. Utilizza la dashboard di protezione per ottenere informazioni su cosa è protetto, cosa necessita di protezione e qual è l'ambito della protezione.

Una volta compresa la portata della tua attuale protezione, "puoi creare e applicare strategie di protezione ransomware ai tuoi workload".

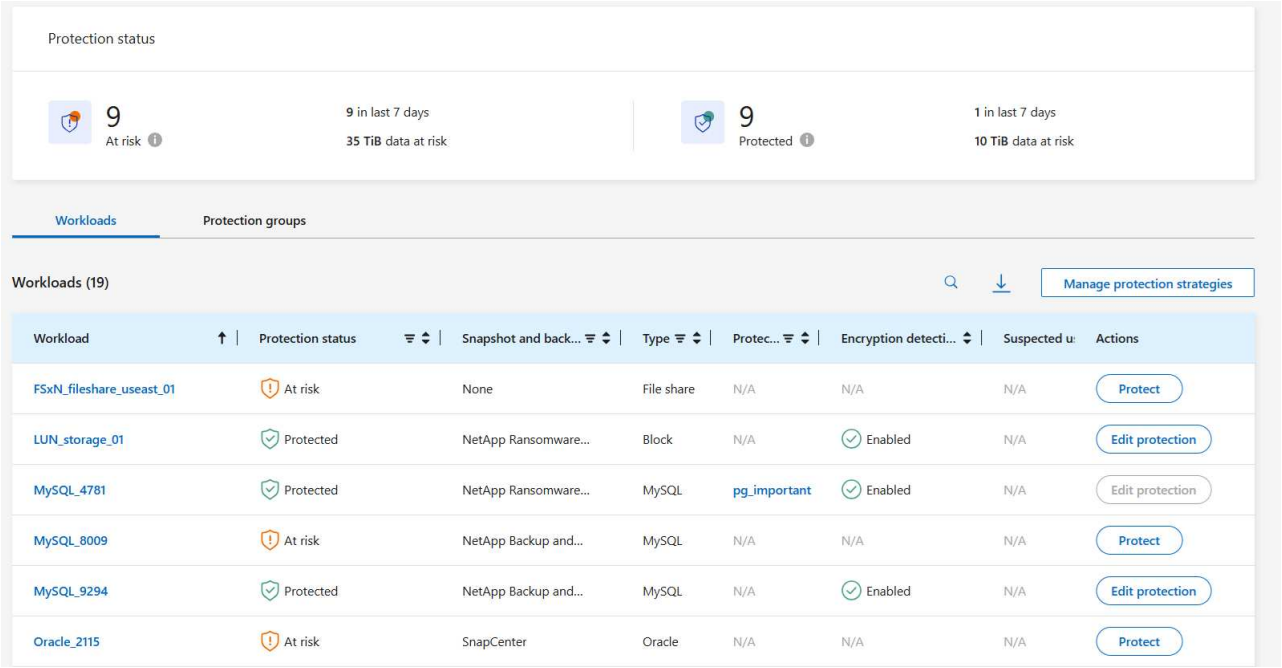
Visualizza la protezione su un workload

Uno dei primi passi per proteggere i carichi di lavoro è visualizzare i carichi di lavoro correnti e il loro stato di protezione. È possibile visualizzare i seguenti tipi di carichi di lavoro:

- Carichi di lavoro applicativi
- Carichi di lavoro a blocchi
- Carichi di lavoro di condivisione file
- Carichi di lavoro VM

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.
2. Eseguire una delle seguenti operazioni:
   - Dal riquadro Data Protection nella dashboard, seleziona **View all**.
   - Dal menu, seleziona **Protezione**.



3. Da questa pagina è possibile visualizzare e modificare i dettagli di protezione per il carico di lavoro.

Vedere "Aggiungi una strategia di protezione dal ransomware" per saperne di più sull'utilizzo di Ransomware Resilience quando è presente una policy di protezione con Backup and Recovery.

Comprendere la dashboard di protezione

La dashboard di protezione in Ransomware Resilience mostra informazioni dettagliate sui carichi di lavoro (ad esempio, nome e tipo di carico di lavoro, Console agent, sistema e storage VM), oltre a informazioni sullo stato della protezione. Utilizza la dashboard di protezione per esaminare e gestire la preparazione al ransomware per i carichi di lavoro. Le seguenti colonne sono particolarmente utili per comprendere il tuo stato di protezione:

Stato di protezione: un carico di lavoro può mostrare uno dei seguenti stati di protezione per indicare se una policy è applicata o meno:

- **Protetto**: è stata applicata una policy. ARP (o ARP/AI a seconda della versione ONTAP) è abilitato su tutti i volumi correlati al carico di lavoro.
- **A rischio**: non viene applicata alcuna politica. Se un carico di lavoro non ha un criterio di rilevamento primario abilitato, è "a rischio" anche se ha un criterio di snapshot e backup abilitato.
- **In corso**: una policy è in fase di applicazione ma non è ancora stata completata.
- **Non riuscito**: un criterio è stato applicato ma non funziona.

Stato di rilevamento:

+ Ransomware Resilience fornisce informazioni sull'ambito delle policy di rilevamento ransomware che hai

configurato sui tuoi carichi di lavoro. Esamina l'ambito di rilevamento con i seguenti campi.

- **Stato di rilevamento della crittografia**
- **Stato di rilevamento del comportamento utente sospetto**
- **Blocca le estensioni di file sospette**

Snapshot, policy di replica e di backup: questa colonna mostra il prodotto o il servizio che gestisce la policy. Se non è presente alcuna policy, il campo visualizza N/A.

Importanza

Ransomware Resilience assegna un'importanza o una priorità a ciascun carico di lavoro durante la fase di individuazione, basandosi su un'analisi di ciascun carico di lavoro. L'importanza del carico di lavoro è determinata dalle seguenti frequenze di snapshot:

- **Critico**: vengono eseguite più copie snapshot all'ora (programma di protezione molto aggressivo)
- **Importante**: le copie degli snapshot vengono create meno frequentemente di ogni ora ma più frequentemente di ogni giorno
- **Standard**: le copie snapshot vengono eseguite più di una volta al giorno

Esposizione alla privacy: Seleziona questa opzione per "eseguire la scansione delle informazioni di identificazione personale con NetApp Data Classification".

Replication destination: se hai configurato la replica Snapshot, vengono elencati i nomi delle VM e dei sistemi di storage di destinazione. Se non è presente alcuna replica, questo campo visualizza "N/A".

Backup destination: se hai configurato una strategia di protezione ransomware con backup, qui viene elencato il nome del sistema di destinazione del backup.

Prossimi passi

- "Proteggi i carichi di lavoro con strategie di protezione dal ransomware"
- "Gestisci i gruppi di protezione"
- "Scansione per dati personali identificabili"

Aggiungi una destinazione di backup in NetApp Ransomware Resilience

Quando NetApp Ransomware Resilience rileva i carichi di lavoro, se i backup sono configurati, Ransomware Resilience riconosce le destinazioni di backup. Se si prevede di utilizzare i backup come parte del "strategia di protezione dal ransomware" ma non sono state configurate destinazioni di backup sul carico di lavoro, è necessario aggiungere una destinazione di backup in NetApp Ransomware Resilience per migliorare la resilienza informatica.

Puoi scegliere una delle seguenti destinazioni di backup:

- NetApp StorageGRID
- Servizi Web Amazon (AWS)
- Piattaforma Google Cloud

- Microsoft Azure

Le destinazioni di backup non sono disponibili per i carichi di lavoro in Amazon FSx for NetApp ONTAP e Azure NetApp Files. Eseguire le operazioni di backup utilizzando soluzioni di backup native: FSx for ONTAP backup service o Azure NetApp Files backups.

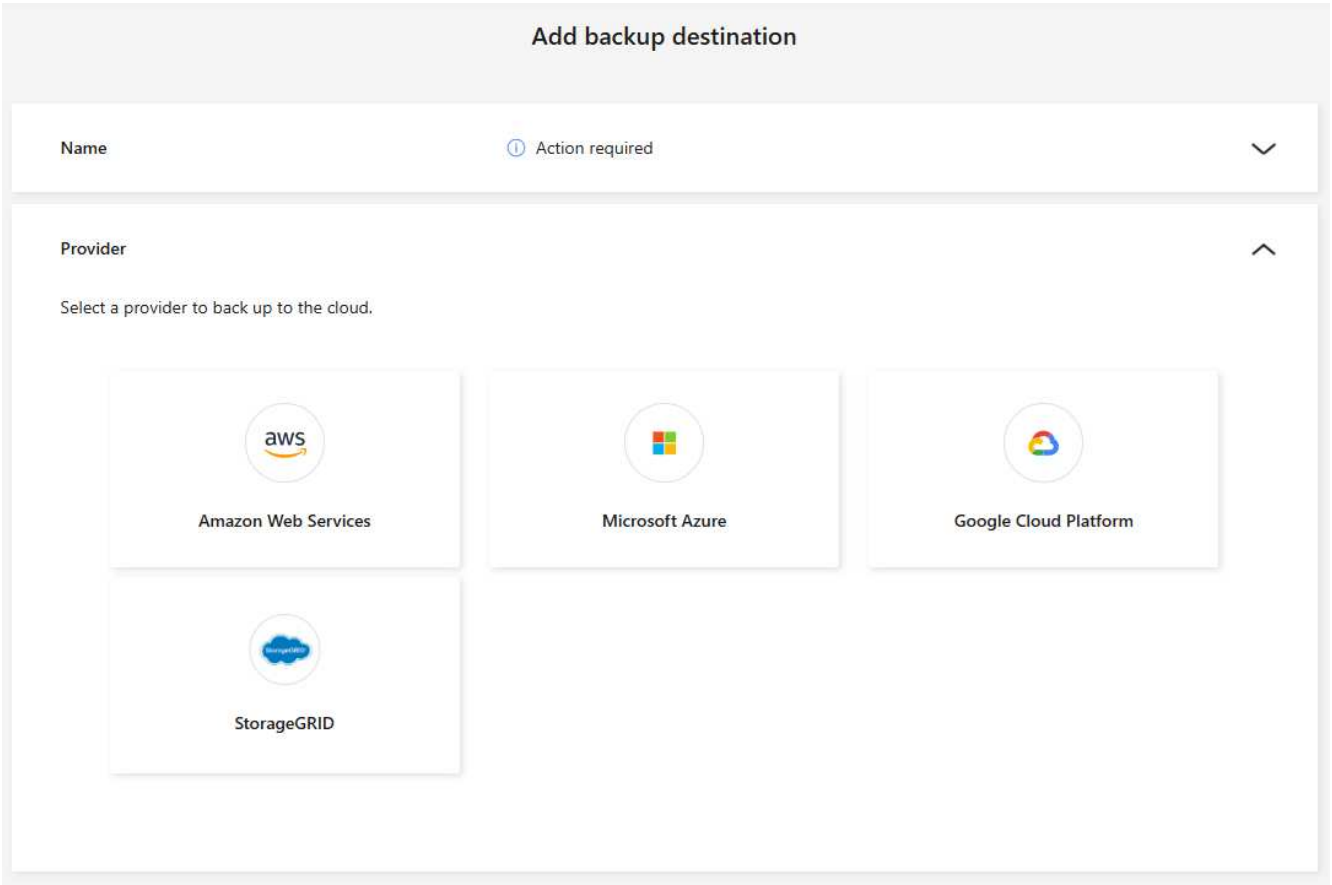
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Aggiungi StorageGRID come destinazione di backup

Per impostare NetApp StorageGRID come destinazione di backup, immettere le seguenti informazioni.

Passi

1. In Ransomware Resilience, seleziona **Impostazioni**.
2. Nel riquadro **Backup Destinations**, seleziona **Visualizza**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per la destinazione del backup.



5. Selezionare * StorageGRID*.
6. Seleziona la freccia rivolta verso il basso accanto a ciascuna impostazione per esaminare i campi obbligatori:
   - **Impostazioni del provider**:

- Scegli se **creare un nuovo bucket** o **utilizzare il tuo bucket**.
- Fornire il **fully qualified domain name (FQDN) del nodo Gateway** e la **porta**.
- Fornire le credenziali StorageGRID: **Chiave di accesso** e **Chiave segreta**.

◦ **Networking**: Seleziona lo spazio IP.

- Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.

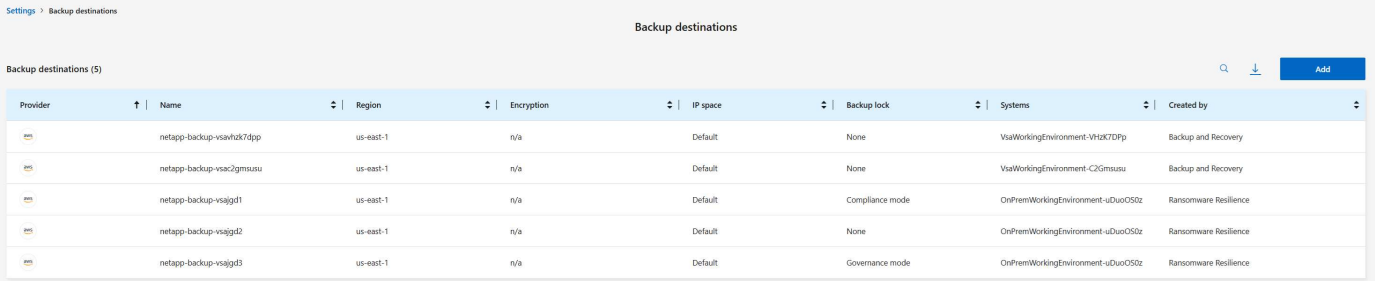
◦ **Backup Lock**

Scegli se desideri configurare il blocco del backup. Con il blocco del backup, le copie sono protette da modifiche o eliminazioni e sottoposte a scansione per rilevare minacce ransomware. Non puoi modificare questa impostazione dopo aver configurato la destinazione di backup. **Se non desideri il blocco del backup, seleziona** None**.** Seleziona **Governance mode** per consentire agli utenti con autorizzazioni specifiche di sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione. **Seleziona** Compliance mode** per impedire agli utenti di sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.

7. Selezionare **Aggiungi**.

Risultato

La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.



Aggiungi Amazon Web Services come destinazione di backup

Per impostare AWS come destinazione di backup, immettere le seguenti informazioni.

Per dettagli sulla gestione dello storage AWS nella Console, vedere "Gestisci i tuoi bucket Amazon S3".

Passi

1. In Ransomware Resilience, seleziona **Impostazioni**.
2. Nel riquadro **Backup Destinations**, seleziona **Visualizza**.
3. Selezionare **Aggiungi**.
4. Seleziona **Amazon Web Services**.
5. Selezionare la freccia giù accanto a ciascuna impostazione e immettere o selezionare i valori:

◦ **Impostazioni del provider**:

- Crea un nuovo bucket, seleziona un bucket esistente se ne esiste già uno nella Console oppure utilizza il tuo bucket in cui archiviare i backup.
- Account AWS, regione, chiave di accesso e chiave segreta per le credenziali AWS

"Se vuoi portare il tuo bucket, fai riferimento ad Aggiungi bucket S3" .

- **Crittografia**: se stai creando un nuovo bucket S3, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Se hai scelto un bucket esistente, le informazioni sulla crittografia sono già disponibili.

  Per impostazione predefinita, i dati nel bucket vengono crittografati con chiavi gestite da AWS. Puoi continuare a utilizzare le chiavi gestite da AWS oppure puoi gestire la crittografia dei tuoi dati utilizzando le tue chiavi.

- **Networking**: seleziona lo spazio IP e se utilizzerai un endpoint privato.
  - Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  - Facoltativamente, scegli se utilizzerai un endpoint privato AWS (PrivateLink) configurato in precedenza.

    Se si desidera utilizzare AWS PrivateLink, fare riferimento a "AWS PrivateLink per Amazon S3" .

- **Blocco backup**: scegli se vuoi che Ransomware Resilience protegga i backup da modifiche o eliminazioni. Questa opzione utilizza la tecnologia NetApp DataLock. Ogni backup verrà bloccato durante il periodo di conservazione, o per un minimo di 30 giorni, più un periodo di buffer fino a 14 giorni.

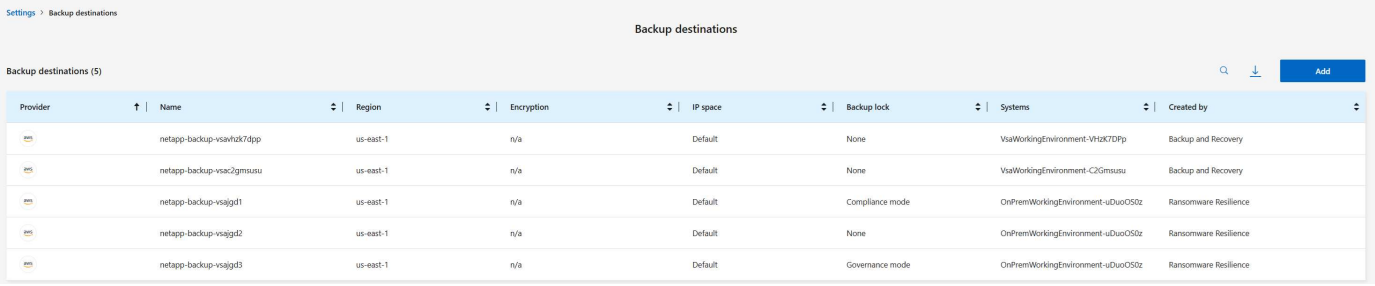
  Se si configura ora l'impostazione di blocco del backup, non sarà possibile modificarla dopo aver configurato la destinazione del backup.

  - **Modalità di governance**: utenti specifici (con autorizzazione s3:BypassGovernanceRetention) possono sovrascrivere o eliminare i file protetti durante il periodo di conservazione.
  - **Modalità di conformità**: gli utenti non possono sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.

6. Selezionare **Aggiungi**.

Risultato

La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.



Aggiungi Google Cloud Platform come destinazione di backup

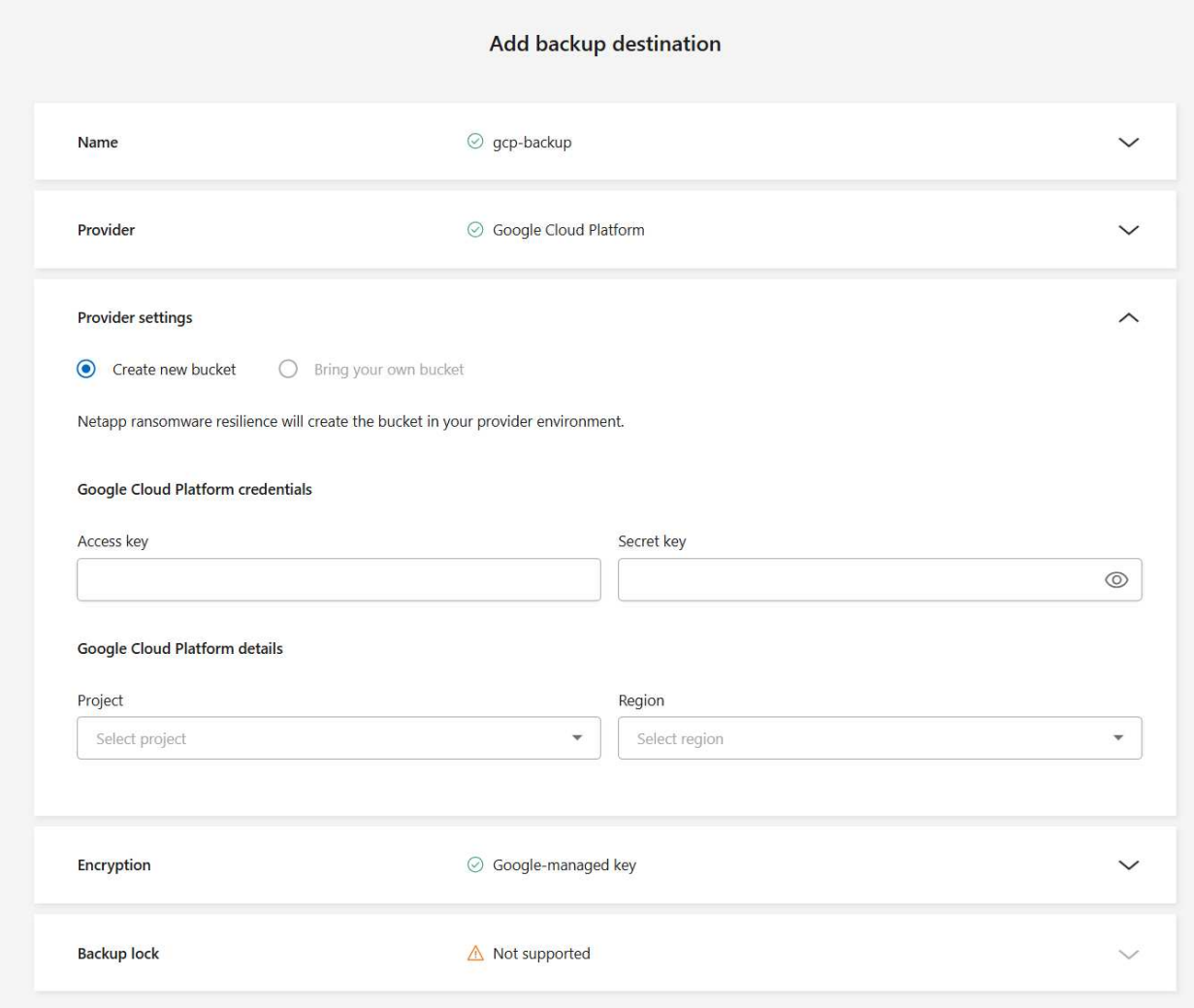
Per impostare Google Cloud Platform (GCP) come destinazione di backup, immettere le seguenti informazioni.

Per dettagli sulla gestione dello storage GCP nella Console, fare riferimento a "Opzioni di installazione dell'agente della console in Google Cloud".

Passi

1. In Ransomware Resilience, seleziona **Impostazioni**.

2. Nel riquadro **Backup Destinations**, seleziona **Visualizza**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per la destinazione del backup.
5. Seleziona **Google Cloud Platform**.
6. Selezionare la freccia giù accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni del provider**:
     - Scegli se **creare un nuovo bucket** o **utilizzare il tuo bucket**.
     - Fornire le credenziali di Google Cloud Platform: **Access key** e **Secret key**.
     - Seleziona il tuo **Project** e la **Region** in cui si trova.



   - **Crittografia**: se stai creando un nuovo bucket, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Se hai scelto un bucket esistente, le informazioni sulla crittografia sono già disponibili.

     Per impostazione predefinita, i dati nel bucket vengono crittografati con chiavi gestite da Google. Puoi continuare con l'impostazione predefinita selezionando **Google-managed keys** oppure utilizzare **Customer-managed keys**.

7. Selezionare **Aggiungi**.

Risultato

La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.

Aggiungi Microsoft Azure come destinazione di backup

Per impostare Azure come destinazione di backup, immettere le seguenti informazioni.

Per informazioni dettagliate sulla gestione delle credenziali di Azure e degli abbonamenti al marketplace nella console, fare riferimento a "Gestisci le tue credenziali di Azure e gli abbonamenti al marketplace" .

Passi

1. In Ransomware Resilience, seleziona **Impostazioni**.
2. Nel riquadro **Backup Destinations**, seleziona **Visualizza**.
3. Selezionare **Aggiungi**.
4. Selezionare **Azure**.
5. Selezionare la freccia giù accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni del provider**:
     - Crea un nuovo account di archiviazione, selezionane uno esistente se ne esiste già uno nella Console oppure utilizza il tuo account di archiviazione che memorizzerà i backup.
     - Fornire l'ID dell'applicazione (client), il client secret e l'ID della directory (tenant). Selezionare **Authenticate**.
     - Seleziona la Azure subscription, la regione e il gruppo di risorse per la tua Azure subscription.

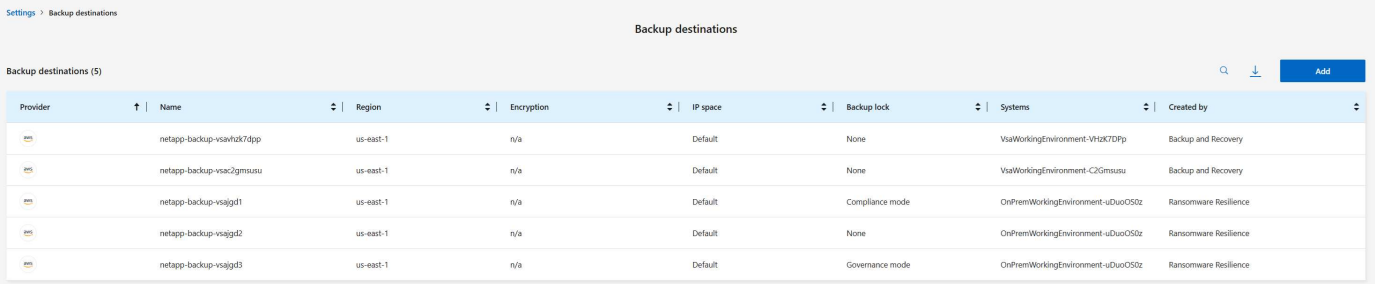
       "Se si desidera utilizzare il proprio account di archiviazione, fare riferimento ad Aggiungere account di archiviazione BLOB di Azure" .
   - **Crittografia**: per impostazione predefinita, i dati vengono crittografati con una chiave gestita da Microsoft. Seleziona **Microsoft-managed key** per mantenere questa opzione; in alternativa, scegli **Customer managed key** per utilizzare le tue chiavi per la crittografia.
   - **Networking**: seleziona lo spazio IP e se utilizzerai un endpoint privato.
     - Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
     - Facoltativamente, scegli se utilizzerai un endpoint privato di Azure configurato in precedenza.

       Se si desidera utilizzare Azure PrivateLink, fare riferimento a "Azure PrivateLink" .
   - **Backup Lock**

     Scegli se desideri configurare il blocco del backup. Con il blocco del backup, le copie sono protette da modifiche o eliminazioni e sottoposte a scansione per rilevare minacce ransomware. Non puoi modificare questa impostazione dopo aver configurato la destinazione di backup. **Se non desideri il blocco del backup, seleziona** None**.** Seleziona **Governance mode** per consentire agli utenti con autorizzazioni specifiche di sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione. **Seleziona** Compliance mode** per impedire agli utenti di sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.
6. Selezionare **Aggiungi**.

Risultato

La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.



Proteggi i carichi di lavoro con le strategie di protezione NetApp Ransomware Resilience

Le strategie di protezione dal ransomware sono una caratteristica fondamentale di NetApp Ransomware Resilience: supportano il rilevamento, la protezione e la replicazione. Le strategie di protezione sono un elemento essenziale della tua strategia di sicurezza informatica.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Comprendere le strategie di protezione dal ransomware

Le strategie di protezione dal ransomware comprendono *rilevamento*, *protezione* e *replica*.

- **Le policy di rilevamento** identificano le minacce ransomware
- **Le policy di protezione** includono policy di snapshot e backup. In una strategia di protezione sono necessarie policy di rilevamento e snapshot. Le policy di backup sono facoltative.

  Se utilizzi altri prodotti NetApp per proteggere il tuo carico di lavoro, Ransomware Resilience li rileva e ti offre la possibilità di:

  - utilizzare una policy di rilevamento ransomware e continuare a utilizzare le policy di snapshot e backup create da altri strumenti NetApp , oppure
  - utilizzare Ransomware Resilience per gestire rilevamento, snapshot e backup.
- **I criteri di replica** consentono di replicare gli snapshot da Ransomware Resilience a un sito secondario. Le pianificazioni di replicazione possono essere impostate su frequenze orarie, giornaliere, settimanali o mensili.

  Attualmente è possibile replicare gli snapshot solo nell'archiviazione ONTAP locale.

Se stai configurando strategie di protezione per Amazon FSxN per ONTAP e Azure NetApp Files, consulta "le limitazioni per ogni servizio".

Per una migliore gestione e protezione del tuo patrimonio di dati, puoi creare "carichi di lavoro di gruppo" per proteggere collettivamente i volumi con un'unica strategia.

Politiche di protezione con altri servizi gestiti NetApp

Oltre a Ransomware Resilience, puoi utilizzare NetApp Backup and Recovery per gestire la protezione delle condivisioni di file e delle condivisioni di file delle VM.

Le informazioni sulla protezione dai servizi di Backup & Recovery vengono visualizzate in Ransomware Resilience. Puoi aggiungere policy di rilevamento a questi servizi con Ransomware Resilience. L'aggiunta di una policy di protezione con Ransomware Resilience sostituisce le policy di protezione esistenti.

Ransomware Resilience rileva anche le policy di protezione da SnapCenter per VMware per i datastore delle VM e da SnapCenter per Oracle. Non è possibile utilizzare questi servizi per il ripristino con Ransomware Resilience.

Se una policy di rilevamento ransomware è gestita da Autonomous Ransomware Protection (ARP o ARP/AI, a seconda della versione ONTAP) e FPolicy in ONTAP, tali carichi di lavoro sono protetti e continueranno a essere gestiti da ARP e FPolicy.

> Le destinazioni di backup non sono disponibili per i carichi di lavoro in Amazon FSx for NetApp ONTAP o Azure NetApp Files. Esegui le operazioni di backup utilizzando il servizio di backup FSx for ONTAP. Imposti le policy di backup per i carichi di lavoro in FSx for ONTAP in AWS, non in Ransomware Resilience. Le policy di backup vengono visualizzate in Ransomware Resilience e rimangono invariate rispetto ad AWS.

Criteri di protezione per carichi di lavoro non protetti dalle applicazioni NetApp

Se il carico di lavoro non è gestito da Backup and Recovery o Ransomware Resilience, potrebbero essere presenti snapshot creati come parte di ONTAP o di altri prodotti. Se la protezione FPolicy di ONTAP è attiva, puoi modificarla utilizzando ONTAP.

Criteri di rilevamento predefiniti

È possibile scegliere una delle seguenti policy predefinite di Ransomware Resilience, in base all'importanza del carico di lavoro.

> Il criterio **Estensione utente crittografia** è l'unico criterio predefinito che supporta il rilevamento di comportamenti sospetti degli utenti.

+ La **Criterio di replica critica** è l'unica politica predefinita che supporta la replica degli snapshot su ONTAP.

Livello di politica	Istantanea	Frequenza	Conservazione (giorni)	Numero di copie snapshot	Numero massimo di copie snapshot
Politica sui carichi di lavoro critici	Ogni quarto d'ora	Ogni 15 minuti	3	288	309
	Quotidiano	Ogni 1 giorno	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni	60	2	309

Livello di politica	Istantanea	Frequenza	Conservazione (giorni)	Numero di copie snapshot	Numero massimo di copie snapshot
Important e politica sul carico di lavoro	Ogni quarto d'ora	Ogni 30 minuti	3	144	165
	Quotidiano	Ogni 1 giorno	14	14	165
	Settimanale	Ogni 1 settimana	35	5	165
	Mensile	Ogni 30 giorni	60	2	165
Politica standard del carico di lavoro	Ogni quarto d'ora	Ogni 30 minuti	3	72	93
	Quotidiano	Ogni 1 giorno	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93
Estension e utente crittografi a	Ogni quarto d'ora	Ogni 30 minuti	3	72	93
	Quotidiano	Ogni 1 giorno	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93
Politica di replicazio ne critica	Ogni quarto d'ora	Ogni 15 minuti	3	288	309
	Quotidiano	Ogni 1 giorno	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni	60	2	309

Aggiungi una strategia di protezione dal ransomware

Esistono tre approcci per aggiungere una strategia di protezione dal ransomware:

- **Creare una strategia di protezione dal ransomware se non si dispone di policy di snapshot o backup.**

  La strategia di protezione dal ransomware include:

    - Politica di snapshot
    - Criterio di rilevamento del ransomware
    - Politica di backup
- **Sostituisci le policy di snapshot o backup esistenti da Backup and Recovery protection con strategie di protezione gestite da Ransomware Resilience.**

  La strategia di protezione dal ransomware include:

    - Politica di snapshot
    - Criterio di rilevamento del ransomware
    - Politica di backup
- **Creare una policy di rilevamento per i carichi di lavoro con policy di snapshot e backup esistenti gestite in altri prodotti o servizi NetApp .**

  La policy di rilevamento non modifica le policy gestite in altri prodotti.

  La policy di rilevamento abilita la protezione autonoma contro i ransomware e la protezione FPolicy se sono già attivate in altri servizi. Scopri di più su"Protezione autonoma dal ransomware" ,"Backup e ripristino" , E"Politica ONTAP" .

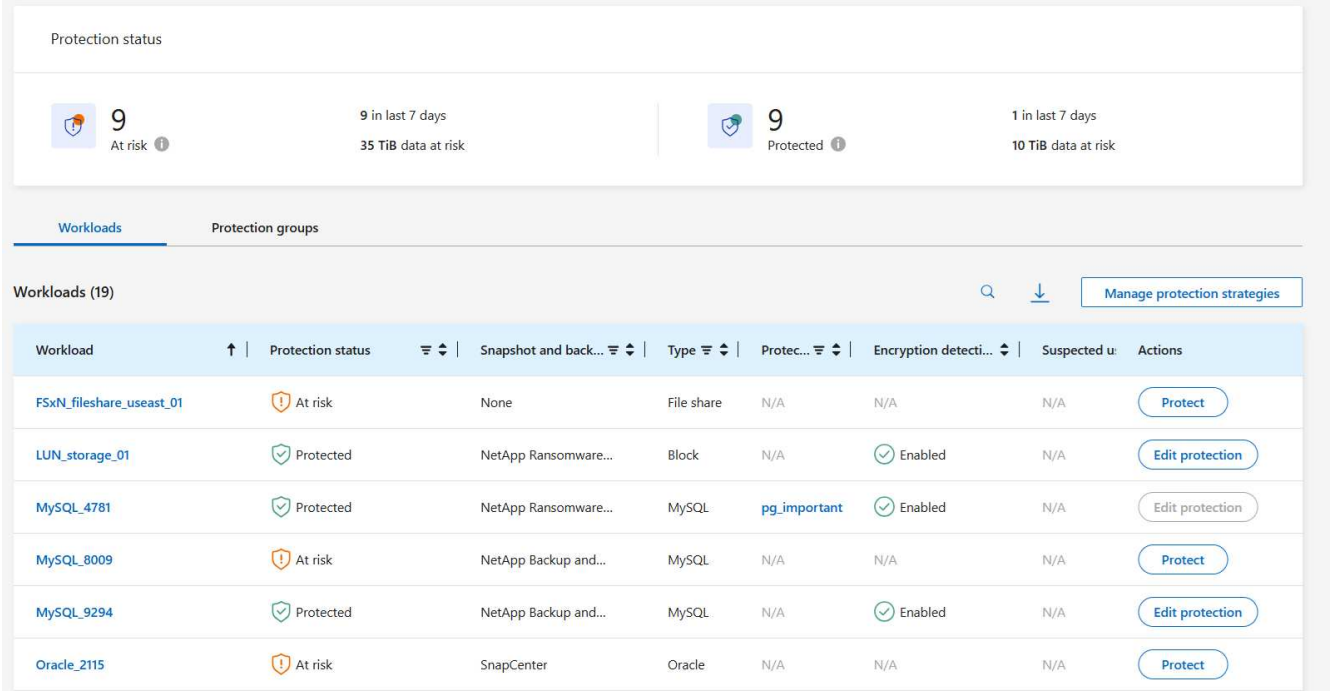
Creare una strategia di protezione dal ransomware (se non si dispone di snapshot o policy di backup)

Se nel carico di lavoro non sono presenti policy di snapshot o backup, è possibile creare una strategia di protezione dal ransomware, che può includere le seguenti policy create in Ransomware Resilience:

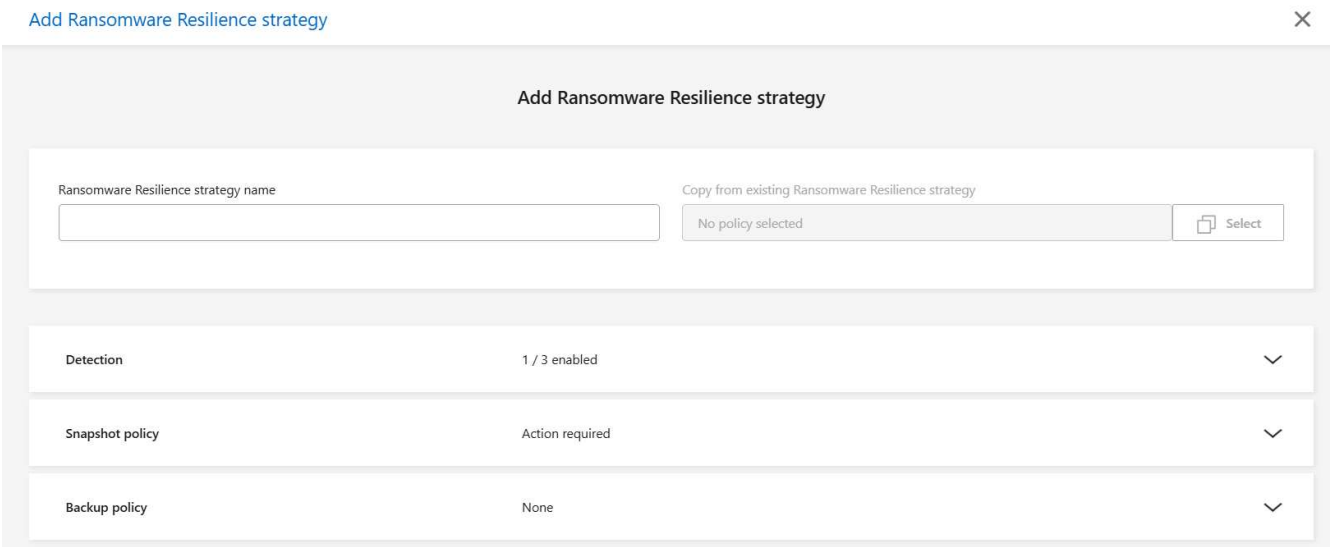
- Politica di snapshot
- Politica di backup
- Criterio di rilevamento del ransomware
- Replicazione secondaria a ONTAP

Passaggi per creare una strategia di protezione dal ransomware

1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona un carico di lavoro, quindi **Proteggi**.
3. Nella pagina Strategie di protezione dal ransomware, seleziona **Aggiungi**.



4. Inserisci un nuovo nome per la strategia oppure inserisci un nome esistente per copiarlo. Se inserisci un nome esistente, scegli quale copiare e seleziona **Copia**.

> Se si sceglie di copiare e modificare una strategia esistente, Ransomware Resilience aggiunge "_copy" al nome originale. Dovresti modificare il nome e almeno un'impostazione per renderlo univoco.

5. Per ogni elemento, seleziona la **freccia giù**.
   - **Politica di rilevamento**:
     - **Criterio**: scegliere uno dei criteri di rilevamento predefiniti.

        - **Rilevamento primario**: abilita Ransomware Resilience per rilevare potenziali attacchi ransomware.
        - **Rilevamento del comportamento sospetto dell'utente**: abilita il rilevamento del comportamento dell'utente per trasmettere gli eventi delle attività dell'utente a Ransomware Resilience e rilevare eventi sospetti, come violazioni dei dati.
        - **Blocca estensioni file**: abilita Ransomware Resilience per bloccare le estensioni di file sospette note. Ransomware Resilience esegue automaticamente copie snapshot quando il rilevamento primario è abilitato.

          Se si desidera modificare le estensioni dei file bloccati, modificarle in Gestione sistema.

    - **Politica di snapshot**:
        - **Nome base policy snapshot**: seleziona una policy oppure seleziona **Crea** e inserisci un nome per la policy snapshot.
        - **Blocco snapshot**: abilita questa opzione per bloccare le copie snapshot sull'archiviazione primaria in modo che non possano essere modificate o eliminate per un determinato periodo di tempo, anche se un attacco ransomware riesce a raggiungere la destinazione dell'archiviazione di backup. Questo è anche chiamato *archiviazione immutabile*. Ciò consente tempi di ripristino più rapidi.

          Quando uno snapshot è bloccato, la data di scadenza del volume viene impostata sulla data di scadenza della copia dello snapshot.

    Il blocco della copia snapshot è disponibile con ONTAP 9.12.1 e versioni successive. Per saperne di più su SnapLock, fare riferimento a "SnapLock in ONTAP" .

    - **Pianificazioni snapshot**: scegli le opzioni di pianificazione, il numero di copie snapshot da conservare e seleziona per abilitare la pianificazione.
        - **Politica di replicazione**:
    - **Nome base della policy di replicazione**: immettere un nuovo nome o sceglierne uno esistente. Il nome base è il prefisso aggiunto a tutti gli snapshot.
    - **Pianificazioni di replicazione**: attiva/disattiva le frequenze che desideri abilitare (oraria, giornaliera, settimanale o mensile) e imposta il valore di conservazione (il numero di snapshot replicati da conservare) per ogni pianificazione abilitata.
        - **Politica di backup**:
    - **Nome base della policy di backup**: inserisci un nuovo nome o scegline uno esistente.
    - **Pianificazioni di backup**: scegli le opzioni di pianificazione per l'archiviazione secondaria e abilita la pianificazione.

    > Per abilitare il blocco del backup su storage secondario, configura le destinazioni di backup utilizzando l'opzione **Impostazioni**. Per i dettagli, vedere "Configurare le impostazioni".

6. Selezionare **Aggiungi**.

Aggiungi una policy di rilevamento ai carichi di lavoro con policy di Snapshot e backup esistenti gestite da NetApp Backup and Recovery

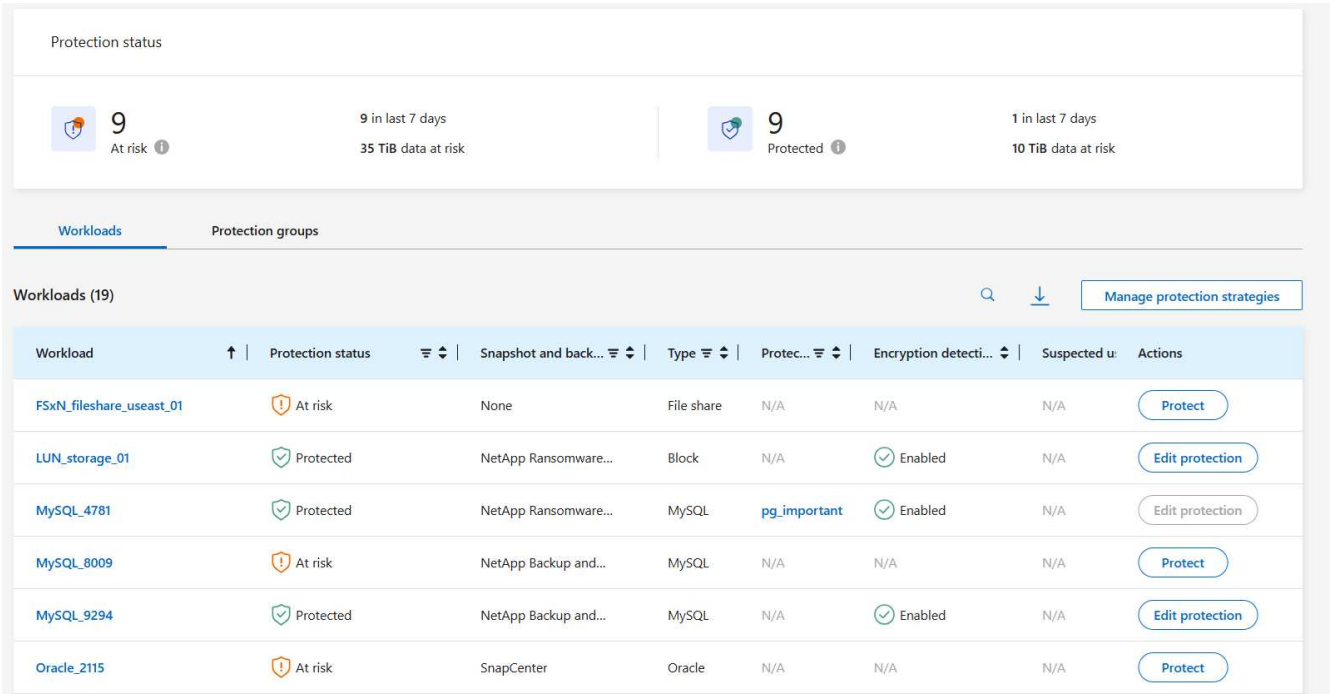
Ransomware Resilience consente di assegnare una policy di rilevamento o una policy di protezione ai carichi di lavoro con protezione snapshot e backup esistente gestita in altri NetApp prodotti o servizi. Backup and Recovery utilizza policy che regolano snapshot, replica su storage secondario o backup su storage a oggetti.

Aggiungere una policy di rilevamento ai carichi di lavoro con policy di backup o snapshot esistenti

Se disponi di policy di snapshot o backup esistenti con Backup and Recovery, puoi aggiungere una policy per rilevare gli attacchi ransomware. Per gestire la protezione e il rilevamento con Ransomware Resilience, consulta Proteggiti con la resilienza del ransomware.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona un carico di lavoro, quindi seleziona **Proteggi**.
3. Ransomware Resilience rileva se sono presenti policy di Backup and Recovery attive.
4. Per lasciare invariato il tuo Backup and Recovery esistente e applicare solo una policy di *detection*, lascia la casella **Replace existing policies** non selezionata.
5. Seleziona le impostazioni di rilevamento che desideri:
   - **Rilevamento della crittografia**
   - **Rilevamento di comportamenti utente sospetti**
   - **Blocca le estensioni di file sospette**
6. Selezionare **Avanti**.
7. Se hai selezionato **Rilevamento comportamento utente sospetto** come impostazione di rilevamento, seleziona l'agente Attività utente o "o crearne uno".

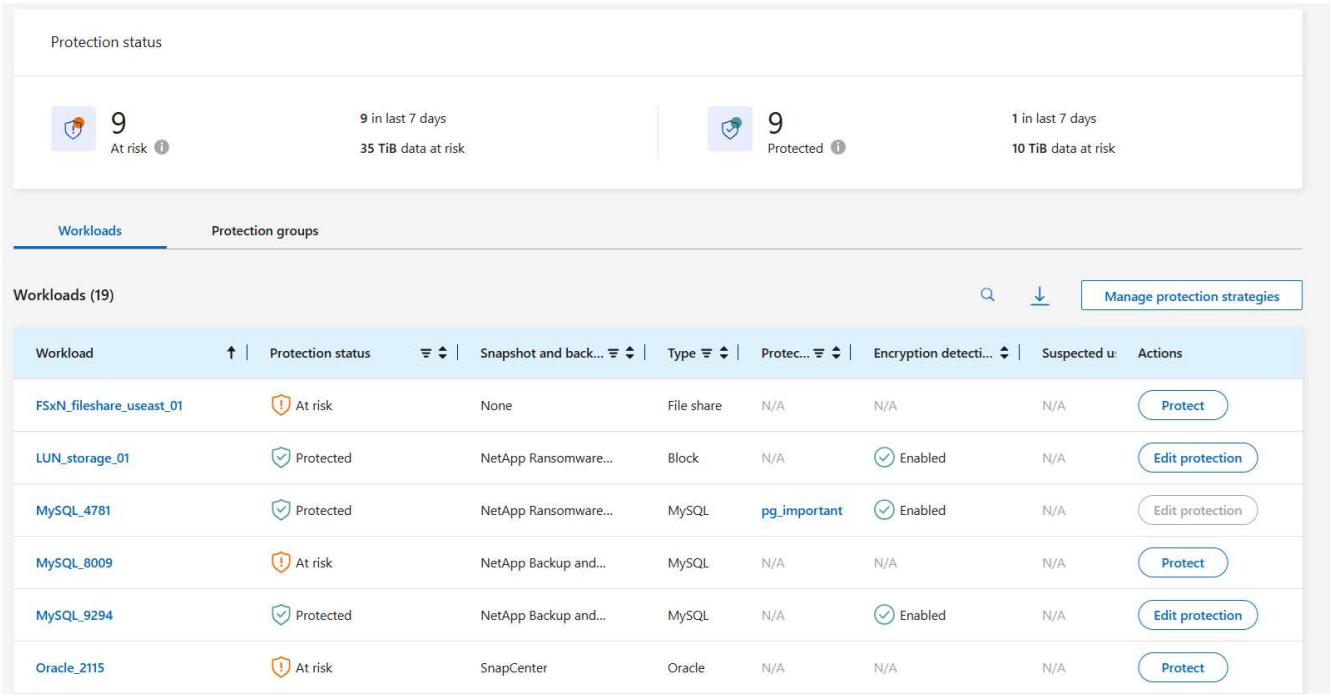
   L'agente di attività utente ospita i nuovi collettori di dati. Ransomware Resilience crea automaticamente il raccoglitore dati per trasmettere gli eventi di attività dell'utente a Ransomware Resilience per rilevare comportamenti anomali dell'utente.
8. Selezionare **Avanti**.
9. Rivedi le tue scelte. Selezionare **Crea** per attivare il rilevamento.
10. Nella pagina Protezione, controlla lo **Stato di rilevamento** per confermare che il rilevamento sia Attivo.

Sostituisci le policy di backup o snapshot esistenti con una strategia di protezione dal ransomware

È possibile sostituire le policy di backup o snapshot esistenti con una strategia di protezione dal ransomware. Questo approccio rimuove la protezione gestita esternamente e configura il rilevamento e la protezione in Ransomware Resilience.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona un carico di lavoro, quindi seleziona **Proteggi**.
3. Ransomware Resilience rileva se sono presenti policy di Backup and Recovery attive. Per sostituire le policy esistenti, seleziona la casella **Replace existing policies**. Quando selezioni la casella, Ransomware Resilience sostituisce l'elenco delle policy di rilevamento con le policy di rilevamento.
4. Scegli una polizza di protezione. Se non esiste alcuna policy di protezione, seleziona **Aggiungi** per crearne una nuova. Per informazioni sulla creazione di una policy, vedereCreare una politica di protezione . Selezionare **Avanti**.
5. Se la strategia prevede la replica, selezionare **Sistema di destinazione** e **VM di archiviazione di destinazione**. Selezionare **Avanti**.
6. Seleziona una destinazione di backup o creane una nuova. Selezionare **Avanti**.
   a. Se la strategia di protezione prevede il rilevamento del comportamento dell'utente, selezionare un agente di attività utente nel proprio ambiente per ospitare i nuovi raccoglitori di dati. Ransomware Resilience crea automaticamente il raccoglitore dati per trasmettere gli eventi di attività dell'utente a Ransomware Resilience per rilevare comportamenti anomali dell'utente.
7. Esaminare la nuova strategia di protezione, quindi selezionare **Proteggi** per applicarla.
8. Nella pagina Protezione, controlla lo **Stato di rilevamento** per confermare che il rilevamento sia Attivo.

Assegna una politica diversa

È possibile sostituire la policy esistente con una diversa.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, nella riga del carico di lavoro, seleziona **Modifica protezione**.
3. Se il carico di lavoro ha una policy di Backup and Recovery esistente che si desidera mantenere, deselezionare **Replace existing policies**. Per sostituire le policy esistenti, selezionare **Replace existing policies**.
4. Nella pagina Criteri, seleziona la freccia rivolta verso il basso per il criterio che desideri assegnare per esaminarne i dettagli.
5. Seleziona la policy che vuoi assegnare.
6. Selezionare **Proteggi** per completare la modifica.

Gestire le strategie di protezione dal ransomware

È possibile eliminare una strategia ransomware.

Visualizza i carichi di lavoro protetti da una strategia di protezione ransomware

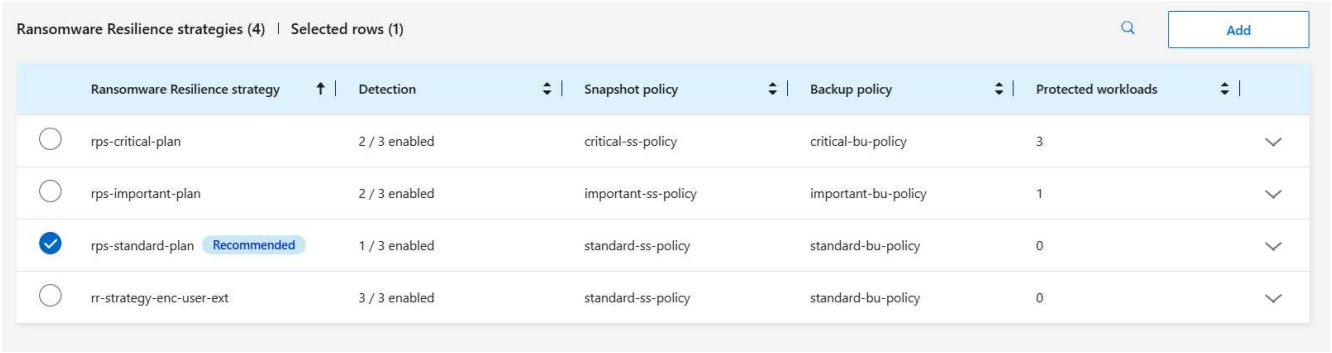
Prima di eliminare una strategia di protezione ransomware, potrebbe essere opportuno verificare quali carichi di lavoro sono protetti da tale strategia.

È possibile visualizzare i carichi di lavoro dall'elenco delle strategie o quando si modifica una strategia specifica.

Passaggi per visualizzare le strategie

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, seleziona **Gestisci strategie di protezione**.

   La pagina Strategie di protezione dal ransomware mostra un elenco di strategie.



3. Nella pagina Strategie di protezione ransomware, nella colonna Carichi di lavoro protetti, seleziona la freccia rivolta verso il basso alla fine della riga.

Eliminare una strategia di protezione ransomware

È possibile eliminare una strategia di protezione che al momento non è associata ad alcun carico di lavoro.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, seleziona **Gestisci strategie di protezione**.

3. Nella pagina Gestisci strategie, seleziona *Azioni* opzione per la strategia che vuoi eliminare.
4. Dal menu Azioni, seleziona **Elimina criterio**.

Configura il rilevamento dell'attività dell'utente

Scopri il rilevamento delle attività degli utenti in NetApp Ransomware Resilience

Grazie al rilevamento dell'attività dell'utente, NetApp Ransomware Resilience consente di affrontare gli eventi ransomware a livello di utente, bloccando eventi quali violazioni dei dati ed eliminazioni su larga scala.

NetApp Ransomware Resilience offre un rilevamento delle violazioni dei dati basato sull'intelligenza artificiale monitorando le attività sospette degli utenti. Forti aumenti dell'attività di lettura e dei modelli di accesso all'attività di lettura vengono utilizzati per determinare l'intento malevolo. Una volta rilevato, Ransomware Resilience genera automaticamente avvisi nella NetApp Console, via e-mail e in qualsiasi ecosistema di sicurezza configurato (ad esempio, SIEM).

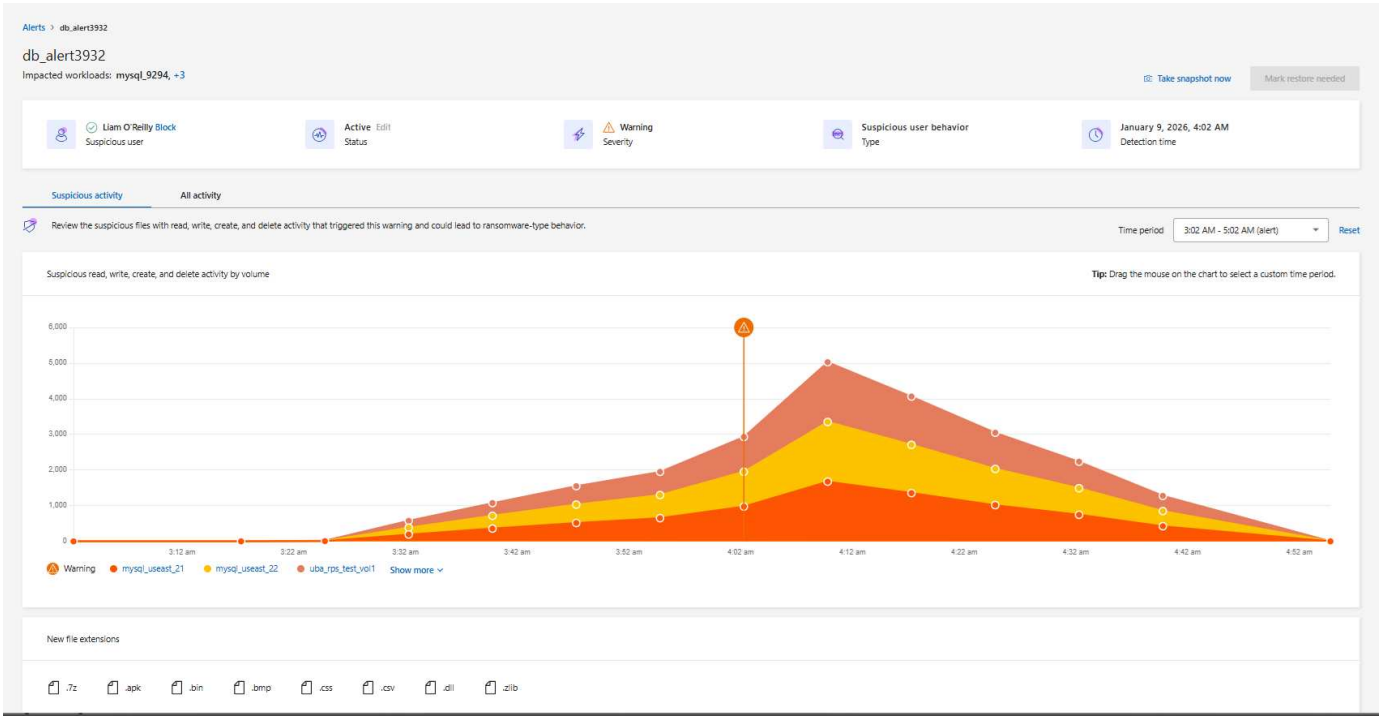
Grazie al rilevamento e all'invio di avvisi in caso di comportamenti sospetti degli utenti, Ransomware Resilience ti avvisa di tentativi e modelli di violazione e distruzione dei dati che sembrano sospetti. In ogni avviso, Ransomware Resilience identifica un utente che puoi bloccare.

Ransomware Resilience rileva le attività sospette degli utenti analizzando gli eventi di attività degli utenti generati da FPolicy in ONTAP. Per raccogliere dati sull'attività dell'utente, è necessario distribuire uno o più agenti di attività dell'utente. L'agente è un server Linux o una macchina virtuale con connettività ai dispositivi del tuo tenant.

> Il rilevamento delle attività utente non è attualmente supportato per i carichi di lavoro SAN. È possibile utilizzare il rilevamento delle attività utente con i carichi di lavoro NAS in Amazon FSxN per ONTAP, Cloud Volumes ONTAP e ONTAP.

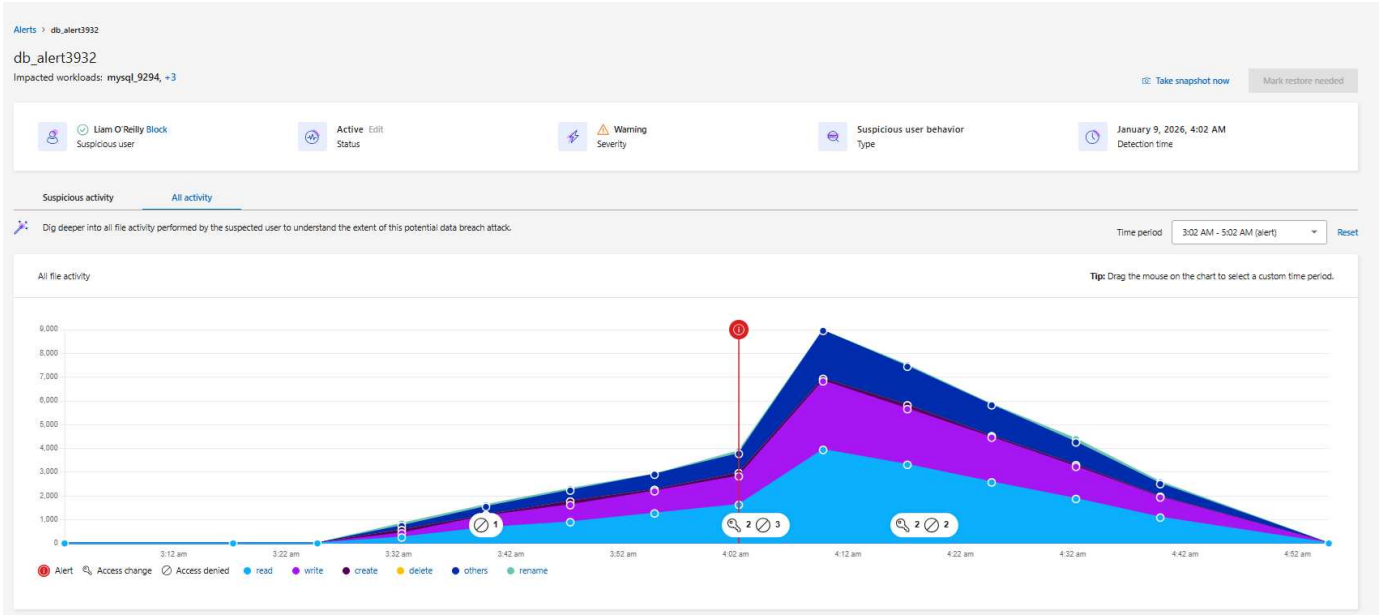
Analisi forense delle attività sospette degli utenti

Ransomware Resilience offre forensics per i comportamenti degli utenti: elenchi e grafici che mostrano quando si sono verificate attività sospette e quando sono state inviate notifiche. Questi dettagliano la frequenza delle attività sospette su file, directory, volumi e carichi di lavoro nel tempo per aiutare a tracciare gli eventi. Puoi anche osservare la comparsa di nuove estensioni di file.



.

È possibile confrontare le attività sospette con una visualizzazione di tutte le attività. Nella visualizzazione di tutte le attività, è possibile osservare eventi di lettura, scrittura, ridenominazione, spostamento, creazione ed eliminazione, oltre a eventi di modifica dell'accesso e di accesso negato.



.

Componenti

Ci sono tre componenti chiave nel rilevamento dell'attività sospetta degli utenti in Ransomware Resilience.

- L'**agente di attività utente** è un ambiente eseguibile per i raccoglitori di dati. È necessario configurare l'agente di attività utente.
- Il **collettore dati** condivide gli eventi di attività dell'utente con Ransomware Resilience. Il collettore dati

viene creato automaticamente quando "abilita una strategia di protezione dal ransomware con rilevamento delle attività sospette degli utenti".

- Il **connettore directory utente** consente la mappatura tra nomi utente e ID utente, garantendo maggiore chiarezza nella risposta a comportamenti sospetti degli utenti. È necessario configurare il connettore directory utente.

NetApp Ransomware Resilience e Data Infrastructure Insights

Il rilevamento del comportamento sospetto degli utenti di Ransomware Resilience è un'integrazione con Data Infrastructure Insights (DII) Workload Security e utilizza "Endpoint DII". Non è necessaria alcuna configurazione DII per abilitare il rilevamento del comportamento degli utenti in Ransomware Resilience. Per abilitare il rilevamento del comportamento degli utenti, "crea l'agente e i collettori richiesti e abilita la strategia di protezione ransomware appropriata".

Se stai già utilizzando NetApp Data Infrastructure Insights (DII) Workload Security, è consigliato utilizzare gli stessi agenti Workload Security per Ransomware Resilience. Non è necessario distribuire agenti Workload Security separati per Ransomware Resilience, tuttavia, l'utilizzo degli stessi agenti Workload Security richiede una relazione di associazione tra l'organizzazione Ransomware Resilience Console e il tenant DII Storage Workload Security. Contatta il tuo rappresentante di account per abilitare questa associazione.

Prossimi passi

- "Requisiti per il rilevamento dell'attività comportamentale dell'utente"
- "Configura gli agenti e i rilevatori di attività comportamentale degli utenti"

Requisiti per il rilevamento del comportamento dell'utente in NetApp Ransomware Resilience

NetApp Ransomware Resilience il rilevamento del comportamento utente consente di rispondere agli eventi ransomware a livello utente. È necessario creare un set di agenti per abilitare il rilevamento del comportamento utente. Prima di abilitare il rilevamento, è necessario assicurarsi di soddisfare i requisiti di sistema operativo, server e rete indicati, in modo che Ransomware Resilience possa rilevare e segnalare correttamente gli eventi.

Supporto del cloud provider

I dati sulle attività sospette degli utenti possono essere archiviati in AWS e Azure nelle seguenti regioni:

Fornitore di cloud	Regione
AWS	• Asia Pacifico (Sydney) (ap-southeast-2) • Europa (Francoforte) (eu-central-1) • Stati Uniti orientali (Virginia settentrionale) (us-east-1)
Azzurro	Stati Uniti orientali

Requisiti del sistema operativo

Il rilevamento di comportamenti sospetti degli utenti è supportato con i seguenti sistemi operativi:

Sistema operativo	Versioni supportate
AlmaLinux	Da 9.4 (64 bit) a 9.5 (64 bit) e 10 (64 bit), incluso SELinux
CentOS	CentOS Stream 9 (64 bit)
Debian	11 (64 bit), 12 (64 bit), incluso SELinux
OpenSUSE Leap	Da 15.3 (64 bit) a 15.6 (64 bit)
Oracle Linux	8.10 (64 bit) e 9.1 (64 bit) fino a 9.6 (64 bit), incluso SELinux
Cappello rosso	8.10 (64 bit), 9.1 (64 bit) fino a 9.6 (64 bit) e 10 (64 bit), incluso SELinux
Roccioso	Rocky 9.4 (64 bit) fino a 9.6 (64 bit), incluso SELinux
SUSE Enterprise Linux	15 SP4 (64 bit) fino a 15 SP6 (64 bit), incluso SELinux
Ubuntu	20.04 LTS (64 bit), 22.04 LTS (64 bit) e 24.04 LTS (64 bit)

L'ordinateur que vous utilisez pour l'agent d'activité de l'utilisateur ne doit pas exécuter d'autres logiciels au niveau de l'application. Si consiglia un server dedicato.

IL `unzip` il comando è necessario per l'installazione. IL `sudo su -` Il comando è necessario per l'installazione, l'esecuzione degli script e la disinstallazione.

Requisiti del server

Il server deve soddisfare i seguenti requisiti minimi:

- **CPU**: 4 core
- **RAM**: 16 GB di RAM
- **Spazio su disco**: 36 GB di spazio libero su disco

Raccomandazioni per il server

- Assegnare spazio extra sul disco per consentire la creazione del file system. Assicurarsi che ci siano almeno 35 GB di spazio libero nel file system. + Se `/opt` è una cartella montata da un archivio NAS, gli utenti locali devono avere accesso a questa cartella. La creazione dell'agente di attività utente può fallire se gli utenti locali non dispongono delle autorizzazioni necessarie.
- Si consiglia di installare l'agente di attività utente su un sistema separato dall'ambiente Ransomware Resilience. Se si installano entrambi sulla stessa macchina, è necessario prevedere da 50 a 55 GB di spazio su disco. Per Linux, allocare 25-30 GB di spazio a `/opt/netapp` e 25 GB a `var/log/netapp`.
- Si consiglia di sincronizzare l'ora sia sul sistema ONTAP sia sulla macchina dell'agente di attività utente utilizzando il protocollo NTP (Network Time Protocol) o il protocollo SNTP (Simple Network Time Protocol).

Regole di accesso alla rete cloud

Esamina le regole di accesso alla rete cloud per la tua area geografica di riferimento (Asia Pacifico, Europa o Stati Uniti).

Durante l'installazione iniziale, sostituire l' `<site_name>` con un'autorizzazione con carattere jolly (`*`). Dopo che l'agente è attivato e completamente operativo, è possibile sostituire l'autorizzazione con il nome del sito. Contattare il proprio rappresentante NetApp per il nome del sito.

L'agente di attività utente utilizza NetApp Data Insights Infrastructure technology, da cui l'utilizzo di `cloudinsights` endpoints. Per ulteriori informazioni, vedere

Distribuzioni di agenti di attività utente con sede in APAC

Protocollo	Porta	Fonte	Destinazione	Descrizione
HTTPS (TCP)	443	Agente di attività dell'utente	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	Accesso alla resilienza del ransomware

Distribuzioni di agenti di attività utente con sede in Europa

Protocollo	Porta	Fonte	Destinazione	Descrizione
HTTPS (TCP)	443	Agente di attività dell'utente	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accesso alla resilienza del ransomware

Distribuzioni di agenti di attività utente con sede negli Stati Uniti

Protocollo	Porta	Fonte	Destinazione	Descrizione
HTTPS (TCP)	443	Agente di attività dell'utente	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	Accesso alla resilienza del ransomware

Regole in-network

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agente di attività dell'utente	URL del server LDAP	Connettiti a LDAP
HTTPS (TCP)	443	Agente di attività dell'utente	Indirizzo IP di gestione del cluster o SVM (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP
TCP	35000 - 55000	Indirizzi IP LIF dei dati SVM	Agente di attività dell'utente	Comunicazione da ONTAP all'agente di attività dell'utente per gli eventi Fpolicy. Queste porte devono essere aperte verso l'agente di attività utente affinché ONTAP possa inviargli eventi, incluso qualsiasi firewall sull'agente di attività utente stesso (se presente). + **NOTA:** Non è necessario riservare **tutte** queste porte, ma le porte riservate a questo scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando 100 porte e di aumentarle se necessario.

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000-55000	IP di gestione del cluster	Agente di attività dell'utente	Comunicazione dall'IP di gestione del cluster ONTAP all'agente di attività dell'utente per **eventi EMS**. Queste porte devono essere aperte verso l'agente di attività utente affinché ONTAP possa inviargli eventi EMS, incluso qualsiasi firewall sull'agente di attività utente stesso. + **NOTA:** Non è necessario riservare **tutte** queste porte, ma le porte riservate a questo scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando 100 porte e di aumentarle se necessario.
SSH	22	Agente di attività dell'utente	Gestione dei cluster	Necessario per il blocco degli utenti CIFS/SMB.

Passaggio successivo

- "Configura gli agenti e i raccoglitori di attività utente"

Configurare agenti e collettori per il rilevamento delle attività degli utenti in NetApp Ransomware Resilience

NetApp Ransomware Resilience rilevamento dell'attività utente aiuta a prevenire eventi ransomware a livello utente. Per abilitare il rilevamento di comportamenti sospetti degli utenti in Ransomware Resilience, è necessario installare almeno un agente di attività utente, che crea un ambiente di raccolta di dati per monitorare il comportamento degli utenti alla ricerca di modelli anomali che assomigliano a eventi ransomware.

Un agente di attività utente ospita un raccoglitore di dati e un connettore di directory utente, che inviano entrambi i dati a una posizione SaaS per l'analisi.

- Il **collettore dati** raccoglie i dati sull'attività degli utenti da ONTAP. Il collettore dati viene creato automaticamente quando si crea una strategia di protezione con rilevamento del comportamento degli utenti.

- Il **connettore directory utente** si connette alla tua directory per mappare gli ID utente ai nomi utente. Devi configurare il connettore directory utente.

L'agente di attività utente, il data collector e il connettore della user directory possono essere tutti gestiti dalla dashboard delle impostazioni di Ransomware Resilience.

> Se stai già utilizzando NetApp Data Infrastructure Insights (DII) Workload Security, è consigliato utilizzare gli stessi agenti Workload Security per Ransomware Resilience. Non è necessario distribuire agenti Workload Security separati per Ransomware Resilience, tuttavia, l'utilizzo degli stessi agenti Workload Security richiede una relazione di associazione tra l'organizzazione Ransomware Resilience Console e il tenant DII Storage Workload Security. Contatta il tuo rappresentante di account per abilitare questa associazione.

+ Se *non* stai utilizzando DII, procedi con le istruzioni di configurazione qui.

Prima di iniziare

- Assicurati di soddisfare i "requisiti del sistema operativo, del server e della rete".

Ruolo Console obbligatorio Per attivare il rilevamento di attività utente sospette, è necessario il ruolo **Organization admin role**. Per le successive configurazioni di attività utente sospette, è necessario il ruolo **Ransomware Resilience user behavior admin role**. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console".

Assicurarsi che ogni ruolo venga applicato a livello di organizzazione.

Creare un agente di attività utente

Gli agenti di attività utente sono ambienti eseguibili per "raccoglitori di dati"; i raccoglitori di dati condividono gli eventi di attività utente con Ransomware Resilience. È necessario creare almeno un agente di attività utente per abilitare il rilevamento di attività utente sospette.

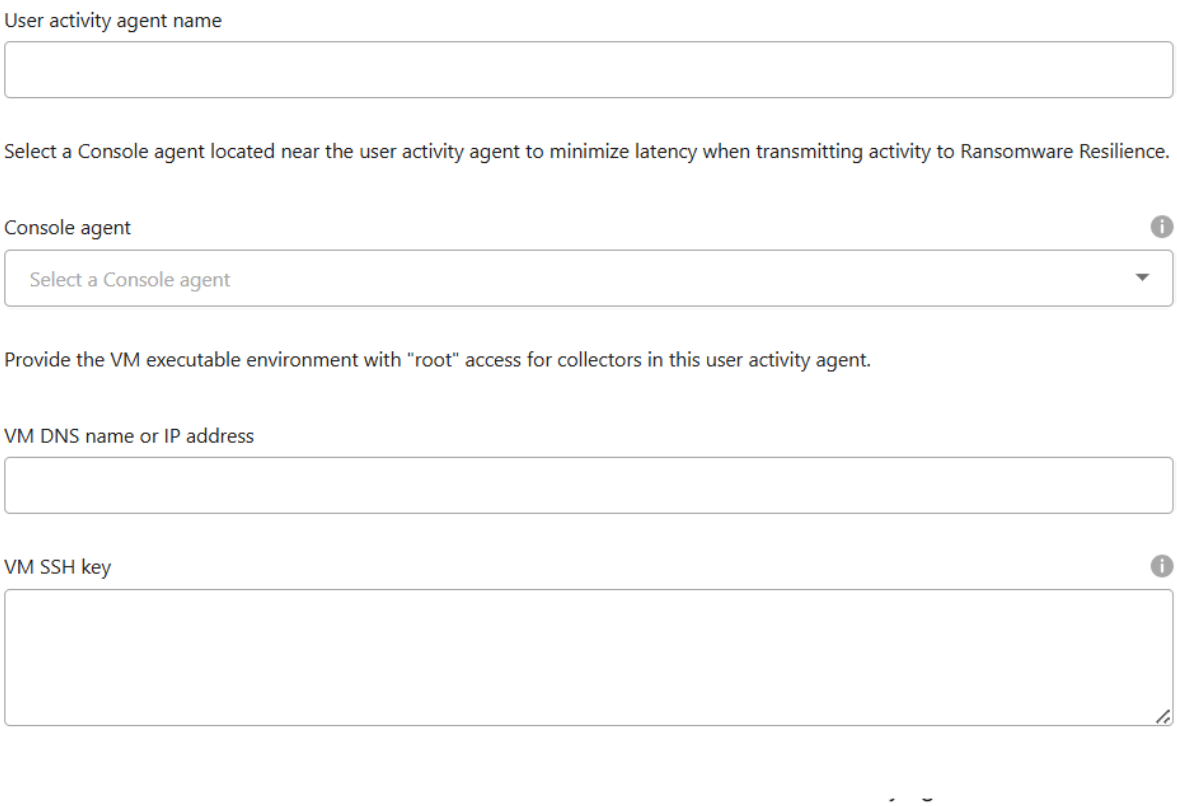
Passi

1. Se è la prima volta che crei un agente di attività utente, vai alla **Dashboard**. Nel riquadro **Attività utente**, seleziona **Attiva**.

   Se vuoi aggiungere un ulteriore agente di attività utente, vai su **Impostazioni**, individua il riquadro **Attività utente**, quindi seleziona **Gestisci**. Nella schermata Attività utente, seleziona la scheda **Agenti attività utente**, quindi **Aggiungi**.

2. Seleziona un **fornitore cloud**, quindi una **regione**. Selezionare **Avanti**.
3. Fornire i dettagli dell'agente di attività dell'utente:
   - **Nome dell'agente di attività dell'utente**
   - **Agente console** - L'agente console deve trovarsi nella stessa rete dell'agente di attività utente e disporre di connettività SSH all'indirizzo IP dell'agente di attività utente.
   - **Nome DNS o indirizzo IP della VM**
   - **Chiave SSH VM** - Inserisci la chiave SSH utilizzando questo formato:

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



4. Selezionare **Avanti**.
5. Rivedi le tue impostazioni. Selezionare **Attiva** per completare l'aggiunta dell'agente di attività utente.
6. Conferma che l'agente di attività utente è stato creato correttamente. Nel riquadro Attività utente, una distribuzione riuscita viene visualizzata come **Running**.

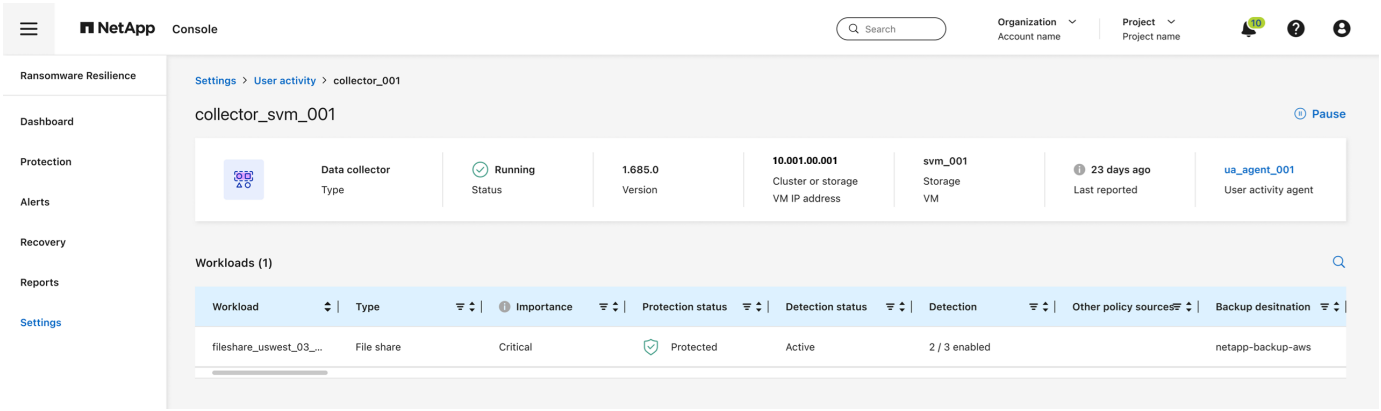
Risultato

Dopo che l'agente di attività utente è stato creato correttamente, torna al menu **Impostazioni** e seleziona **Gestisci** nel riquadro Attività utente. Seleziona la scheda **Agenti di attività utente** e poi seleziona l'agente di attività utente per visualizzare i dettagli relativi, inclusi i collettori di dati e i connettori della directory utente.

Aggiungi un raccoglitore di dati

I collettori di dati vengono creati automaticamente quando si attiva una strategia di protezione dal ransomware con rilevamento di attività sospette degli utenti. Per ulteriori informazioni, vedere "aggiungere una politica di rilevamento".

È possibile visualizzare i dettagli del raccoglitore dati. Da Impostazioni, seleziona **Gestisci** nel riquadro Attività utente. Selezionare la scheda **Raccolta dati**, quindi selezionare la raccolta dati per visualizzarne i dettagli o metterla in pausa.



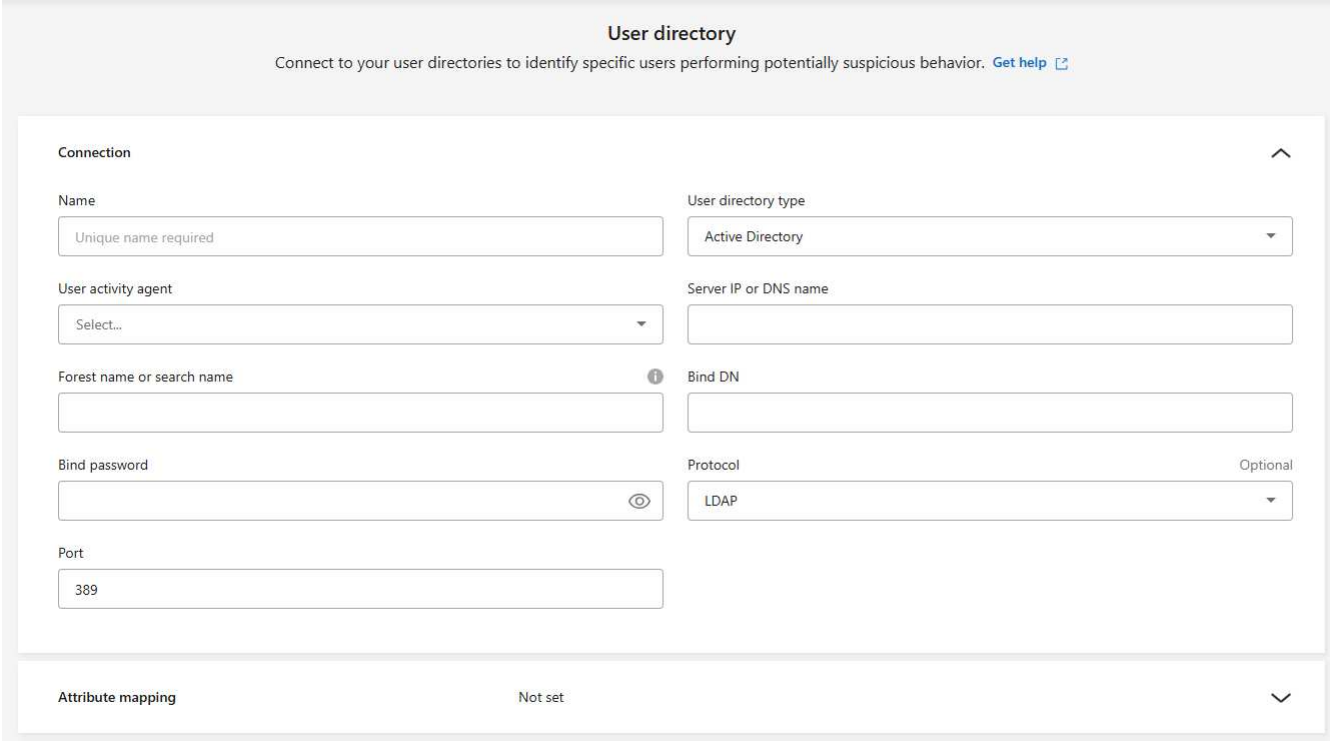
Crea un connettore di directory utente

Per mappare gli ID utente ai nomi utente, è necessario creare un connettore di directory utente.

Passi

1. In Ransomware Resilience, vai su **Impostazioni**.
2. Nel riquadro Attività utente, seleziona **Gestisci**.
3. Selezionare la scheda **Connettori directory utente**, quindi **Aggiungi**.
4. Configurare la connessione. Inserisci le informazioni richieste per ogni campo.

Campo	Descrizione
Nome	Inserisci un nome univoco per il connettore della directory utente
Tipo di directory utente	Il tipo di directory
Indirizzo IP del server o nome di dominio	L'indirizzo IP o il nome di dominio completo (FQDN) del server che ospita la connessione
Nome della foresta o nome della ricerca	È possibile specificare il livello di foresta della struttura della directory come nome di dominio diretto (ad esempio `unit.company.com`) o un insieme di nomi distinti relativi (ad esempio: `DC=unit,DC=company,DC=com`). Puoi anche inserire un `OU` per filtrare per unità organizzativa o per `CN` per limitare a un utente specifico (ad esempio: `CN=user,OU=engineering,DC=unit,DC=company,DC=com`).
LEGA DN	Il BIND DN è un account utente autorizzato a effettuare ricerche nella directory, ad esempio utente@dominio.com. L'utente necessita dell'autorizzazione di sola lettura del dominio.
Password BIND	La password per l'utente fornita in BIND DN
Protocollo	Il campo protocollo è facoltativo. È possibile utilizzare LDAP, LDAPS o LDAP su StartTLS.
Porta	Inserisci il numero di porta scelto



Fornire i dettagli della mappatura degli attributi:

- **Nome da visualizzare**
- **SID** (se si utilizza LDAP)
- **Nome utente**
- **ID Unix** (se stai utilizzando NFS)
- Se selezioni **Includi attributi facoltativi**, puoi anche aggiungere un indirizzo email, un numero di telefono, un ruolo, uno stato, un paese, un reparto, una foto, il nome del responsabile o dei gruppi. Selezionare **Avanzate** per aggiungere una query di ricerca facoltativa.

5. Selezionare **Aggiungi**.
6. Torna alla scheda dei connettori della directory utente per controllare lo stato del connettore della directory utente. Se la creazione avviene correttamente, lo stato del connettore della directory utente viene visualizzato come **In esecuzione**.

Elimina un connettore di directory utente

Passi

1. In Ransomware Resilience, vai su **Impostazioni**.
2. Individua il riquadro Attività utente e seleziona **Gestisci**.
3. Selezionare la scheda **Connettore directory utente**.
4. Identifica il connettore della directory utente che desideri eliminare. Nel menu azioni alla fine della riga, seleziona i tre punti … quindi **Elimina**.
5. Nella finestra di dialogo pop-up, seleziona **Delete** per confermare.

Escludi gli utenti dagli avvisi

Se ci sono determinati utenti attendibili il cui comportamento potrebbe attivare avvisi sul comportamento degli utenti, puoi escluderli dagli avvisi.

Passi

1. In Ransomware Resilience, seleziona **Impostazioni**.
2. Nella dashboard Impostazioni, individua la scheda User activity, quindi seleziona **Manage**.
3. Seleziona la scheda **Utenti esclusi**.
4. Per rivedere i singoli utenti nell'interfaccia utente, seleziona **Seleziona manualmente**. Per caricare un elenco di utenti esclusi, seleziona **Carica**.
   a. Se hai selezionato **Seleziona manualmente**, seleziona la casella di controllo accanto ai nomi degli utenti specifici che desideri escludere.
   b. Se selezioni **Carica**, devi prima scaricare un file CSV che include l'elenco di tutti gli utenti. Seleziona **Scarica** per accedere all'elenco.

      Esamina il file CSV. Rimuovi i nomi di tutti gli utenti per cui desideri mantenere il rilevamento. Quando l'elenco include solo i nomi degli utenti che desideri escludere dal rilevamento, salvalo. Seleziona **Upload** per individuare il file, quindi selezionalo.
5. Seleziona **Aggiungi** per completare l'aggiunta degli utenti all'elenco delle esclusioni.
6. Nella scheda **Utenti esclusi**, i nomi degli utenti rimossi dagli avvisi di rilevamento del comportamento utente ora vengono visualizzati nella dashboard.

È anche possibile escludere un utente direttamente da un avviso. Per ulteriori informazioni, vedere "Rispondere agli avvisi di ransomware".

Rimuovi gli utenti dall'elenco degli utenti esclusi

È possibile aggiungere nuovamente un utente al rilevamento in seguito.

Passi

1. Nella dashboard Impostazioni, individua la scheda User activity, quindi seleziona **Manage**.
2. Seleziona la scheda **Utenti esclusi**.
3. Individua il nome dell'utente che desideri rimuovere dalla selezione degli utenti esclusi. Seleziona il menu Azione (... sulla riga con il nome dell'utente, quindi **Rimuovi**.
4. Nella finestra di dialogo, seleziona **Remove** per confermare che desideri rimuovere gli utenti selezionati.

Rispondere agli avvisi di attività sospette degli utenti

Dopo aver configurato il rilevamento delle attività sospette degli utenti, è possibile monitorare gli eventi nella pagina degli avvisi. Per ulteriori informazioni, vedere "Rileva attività dannose e comportamenti sospetti degli utenti".

Gestire i gruppi di protezione in NetApp Ransomware Resilience

NetApp Ransomware Resilience offre gruppi di protezione per semplificare la gestione del patrimonio dati. I gruppi di protezione sono raggruppamenti logici di carichi di lavoro. Ransomware Resilience può proteggere tutti i volumi di un gruppo di protezione

contemporaneamente con una singola strategia di protezione, evitandoti di dover applicare una strategia a ciascun carico di lavoro.

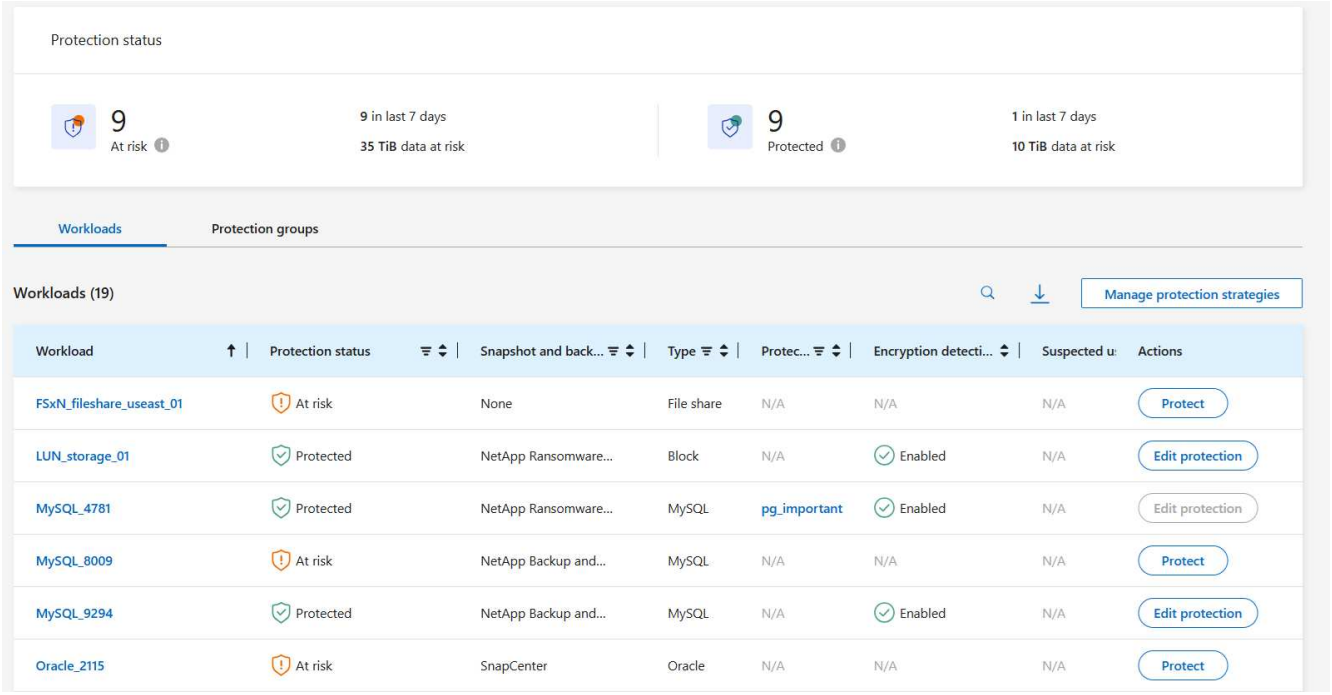
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Crea un gruppo di protezione

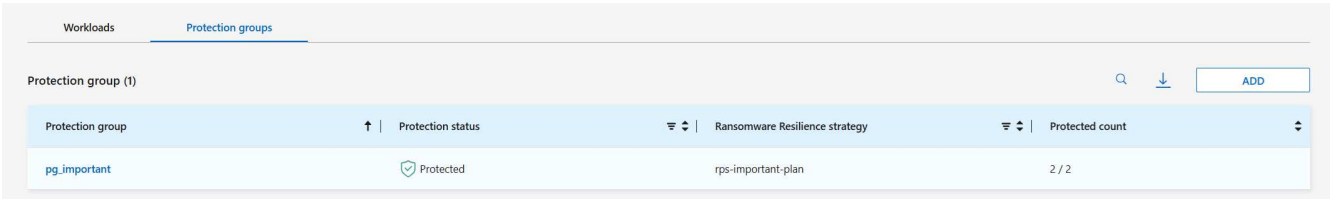
È possibile creare gruppi indipendentemente dal loro stato di protezione (ovvero, gruppi non protetti e gruppi protetti). Quando si aggiunge una policy di protezione a un gruppo di protezione, la nuova policy di protezione sostituisce qualsiasi policy esistente, incluse le policy gestite da NetApp Backup and Recovery.

Passi

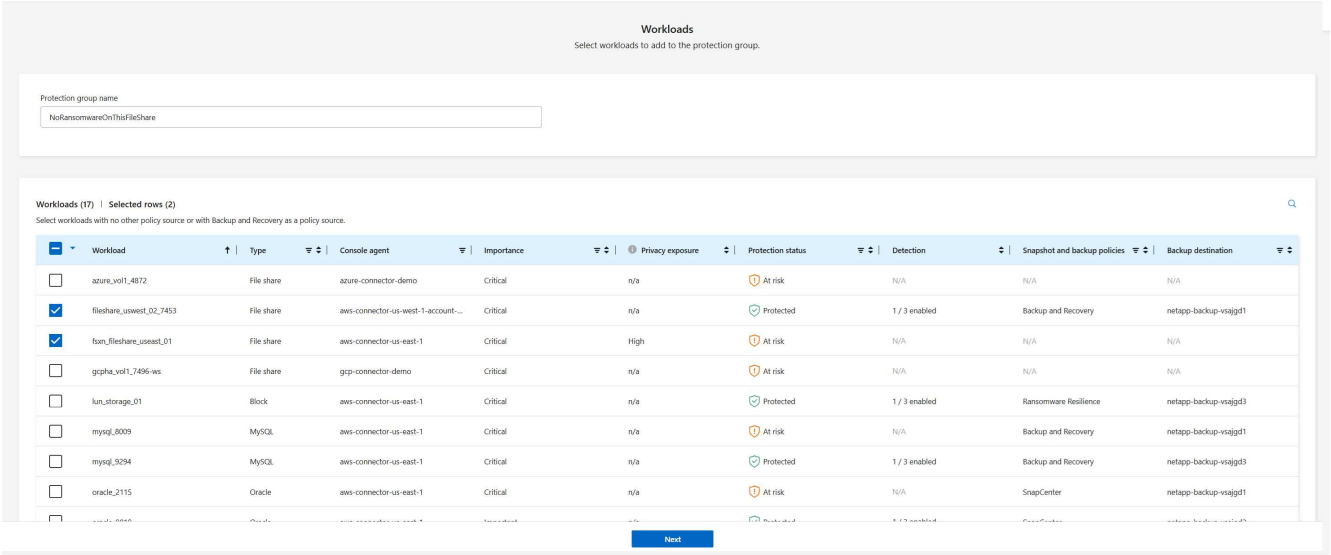
1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla dashboard Protection, seleziona la scheda **Protection groups**.



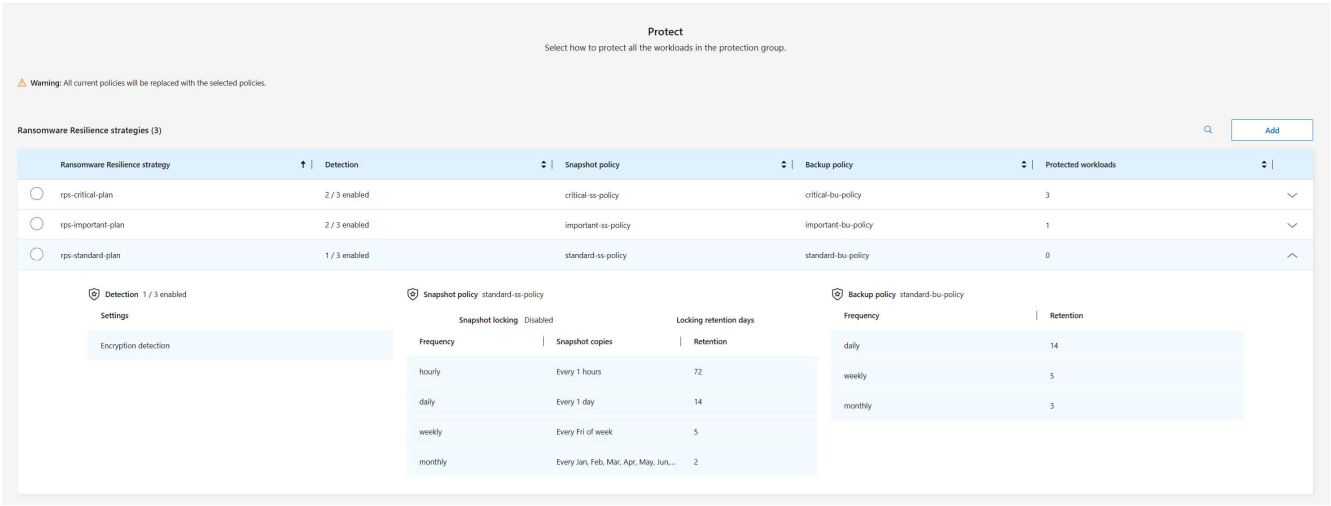
3. Selezionare **Aggiungi**.



4. Immettere un nome per il gruppo di protezione.
5. Seleziona i carichi di lavoro da aggiungere al gruppo.

   Per visualizzare maggiori dettagli sui carichi di lavoro, scorrere verso destra.

6. Selezionare **Avanti**.



7. Seleziona una strategia di protezione per il gruppo.
8. Se la strategia di protezione include la replica, rivedere le impostazioni di replica.
   a. Per replicare tutti gli snapshot nella stessa destinazione, seleziona **Usa la stessa destinazione per ogni carico di lavoro**. Selezionare un **Sistema di destinazione** e una **VM di archiviazione di destinazione** per i carichi di lavoro nella sezione Agente console. + Per utilizzare destinazioni diverse, deselezionare la casella. Esaminare ciascun carico di lavoro in ciascun agente della console e assegnare un **Sistema di destinazione** e una **VM di archiviazione di destinazione** per ciascun carico di lavoro. Selezionare **Avanti**.
9. Per configurare un criterio di backup, selezionarne uno, quindi selezionare **Avanti**.
10. Se la policy di rilevamento include il rilevamento del comportamento dell'utente, seleziona il raccoglitore dati che desideri utilizzare, quindi **Avanti**.

11. Rivedere le selezioni per il gruppo di protezione.
12. Per finalizzare il gruppo di protezione, seleziona **Add**.

Quando si esamina la dashboard di protezione in Ransomware Resilience, è possibile ordinare i carichi di lavoro per gruppo di protezione.

Modifica protezione gruppo

È possibile modificare i criteri di rilevamento per un gruppo esistente.

Passi

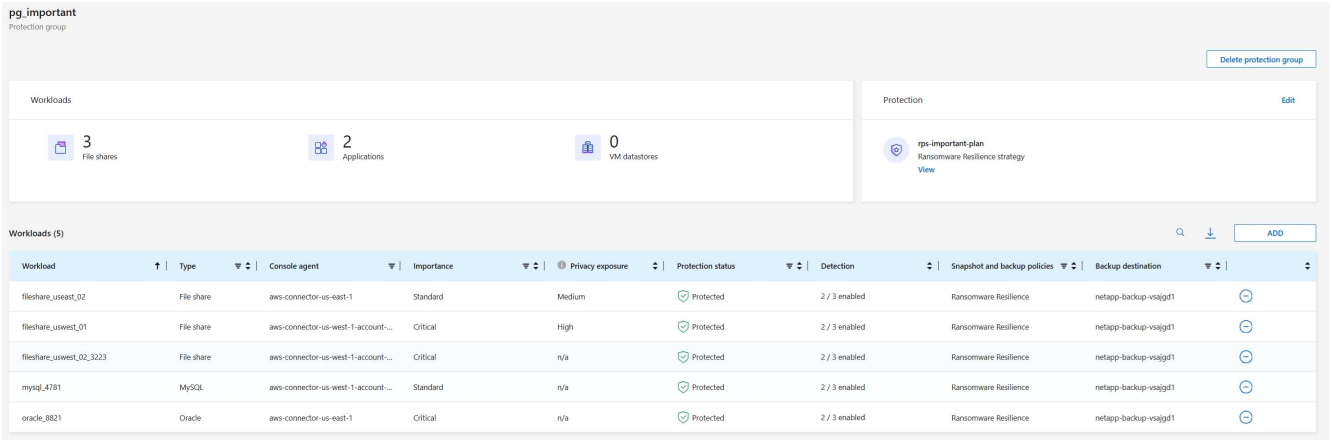
1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**, quindi seleziona il gruppo di cui desideri modificare la policy.
3. Dalla pagina di panoramica del gruppo di protezione, seleziona **Modifica protezione**.
4. Seleziona una policy di protezione esistente da applicare oppure seleziona **Aggiungi** per creare una nuova policy di protezione. Per ulteriori informazioni sull'aggiunta di una policy di protezione, consulta "Creare una politica di protezione". Quindi seleziona **Salva**.
5. Nella panoramica della destinazione di backup, seleziona una destinazione di backup esistente oppure **Aggiungi una nuova destinazione di backup**.
6. Seleziona **Avanti** per rivedere le modifiche.

Rimuovi i carichi di lavoro da un gruppo di protezione

Potresti in seguito dover rimuovere i carichi di lavoro da un gruppo di protezione esistente.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**.
3. Seleziona il gruppo da cui desideri rimuovere uno o più carichi di lavoro.



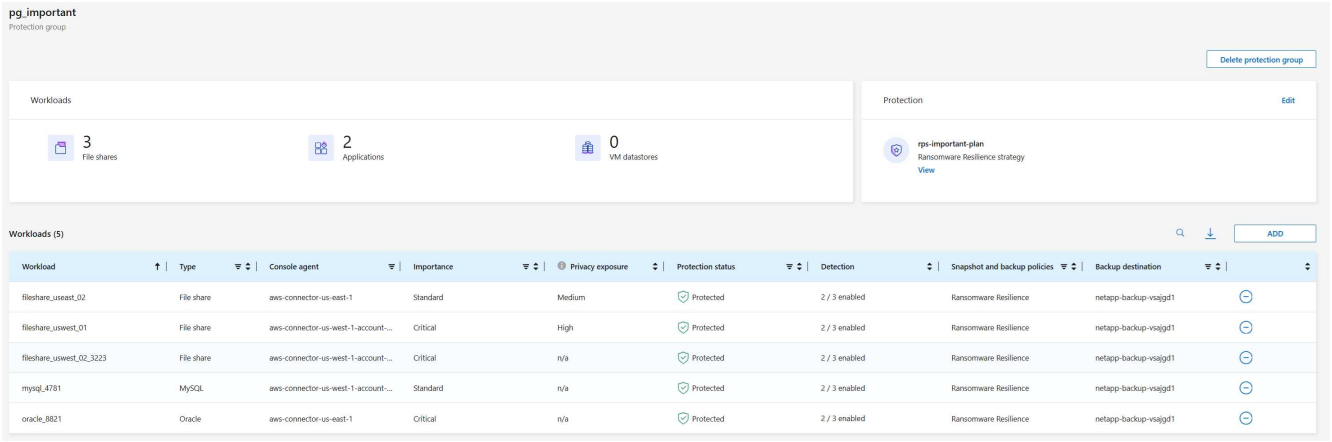
4. Dalla pagina del gruppo di protezione, seleziona il carico di lavoro che desideri rimuovere dal gruppo e seleziona l'opzione **Azioni** ⋯.
5. Dal menu Azioni, seleziona **Rimuovi carico di lavoro**.
6. Conferma di voler rimuovere il carico di lavoro e seleziona **Rimuovi**.

Elimina un gruppo di protezione

Quando si elimina un gruppo di protezione, Ransomware Resilience rimuove il gruppo e la strategia di protezione sui carichi di lavoro. Non elimina i singoli carichi di lavoro.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**.
3. Seleziona il gruppo da cui desideri rimuovere uno o più carichi di lavoro.



4. Nella pagina del gruppo di protezione selezionato, in alto a destra, seleziona **Elimina gruppo di protezione**.
5. Conferma di voler eliminare il gruppo e seleziona **Elimina**.

Scansiona le informazioni di identificazione personale con NetApp Data Classification in Ransomware Resilience

All'interno di NetApp Ransomware Resilience, puoi utilizzare NetApp Data Classification per analizzare e classificare i dati in un carico di lavoro di condivisione file. La classificazione dei dati aiuta a determinare se il set di dati include informazioni di identificazione personale (PII), che possono aumentare i rischi per la sicurezza. Data Classification è un componente fondamentale della NetApp Console ed è disponibile senza costi aggiuntivi.

"Classificazione dei dati"utilizza l'elaborazione del linguaggio naturale basata sull'intelligenza artificiale per l'analisi e la categorizzazione dei dati contestuali, fornendo informazioni fruibili sui dati per soddisfare i requisiti di conformità, rilevare vulnerabilità di sicurezza, ottimizzare i costi e accelerare la migrazione.

Questo processo può influire sull'importanza del carico di lavoro per garantire la protezione adeguata.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Identificare l'esposizione alla privacy con la classificazione dei dati

Prima di utilizzare la classificazione dei dati all'interno di Ransomware Resilience, è necessario"per abilitare la classificazione dei dati per analizzare i tuoi dati" .

È possibile implementare la classificazione dei dati nella pagina Protezione di Ransomware Resilience. Seguire la procedura per identificare l'esposizione alla privacy. Quando selezioni **Identifica esposizione**, se non hai ancora implementato la classificazione dei dati, una finestra di dialogo ti consente di abilitarla.

Per ulteriori informazioni sulla classificazione dei dati, vedere:

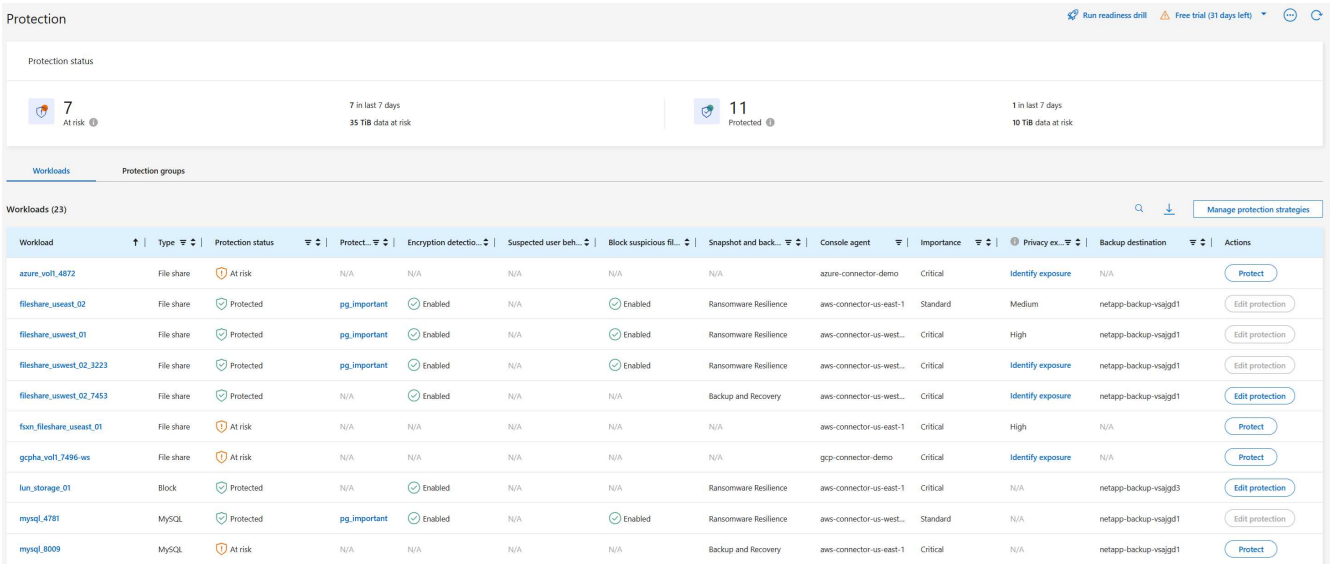
- "Scopri di più sulla classificazione dei dati"
- "Categorie di dati privati"
- "Esamina i dati archiviati nella tua organizzazione"

Prima di iniziare

La scansione dei dati PII in Ransomware Resilience è disponibile se hai"Classificazione dei dati distribuita" . La classificazione dei dati è disponibile come parte della Console senza costi aggiuntivi e può essere distribuita in locale o nel cloud del cliente.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, individua un carico di lavoro di condivisione file nella colonna Carico di lavoro.



3. Per consentire alla Classificazione dei dati di analizzare i dati alla ricerca di informazioni personali identificabili (PII), nella colonna **Esposizione alla privacy**, selezionare **Identifica esposizione**.

> Se non hai distribuito Data CCasification, selezionando **Identifica esposizione** si apre una finestra di dialogo per distribuire Data Classification. Selezionare **Distribuisci**. Dopo aver implementato la classificazione dei dati, puoi tornare alla pagina Protezione e selezionare **Identifica esposizione**.

Risultato

La scansione può richiedere diversi minuti, a seconda delle dimensioni e del numero dei file. Durante la scansione, la pagina Protezione indica che sta identificando i file e ne fornisce il conteggio. Una volta

completata la scansione, la colonna Esposizione privacy classifica il livello di esposizione come Basso, Medio o Alto.

Esaminare l'esposizione alla privacy

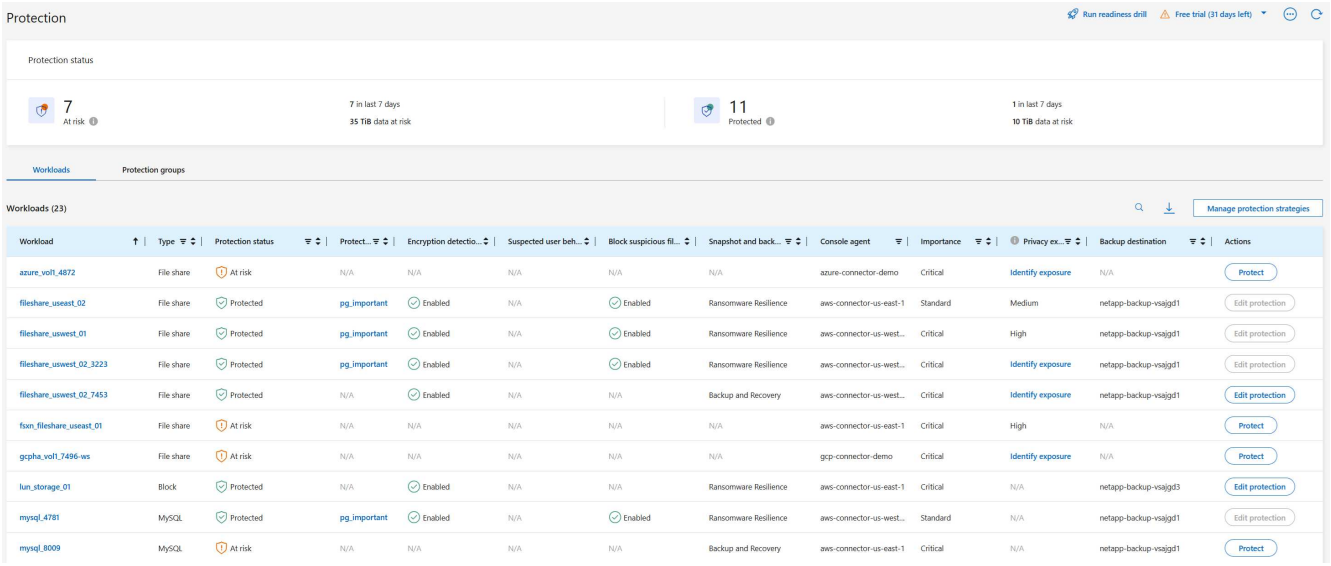
Dopo aver eseguito le scansioni di classificazione dei dati per individuare le informazioni personali identificabili, valutare il rischio.

I dati PII sono classificati in una delle tre designazioni:

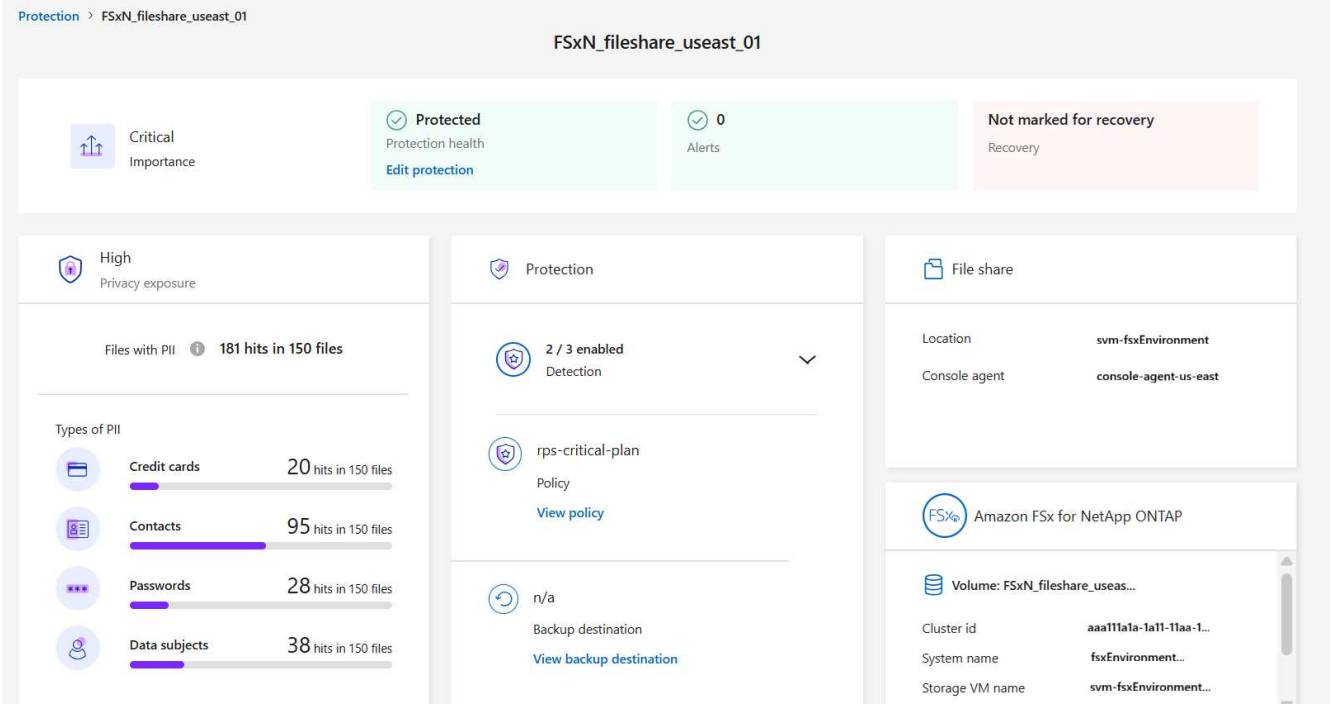
- **Alto**: oltre il 70% dei file contiene PII
- **Medio**: più del 30% e meno del 70% dei file contengono PII
- **Basso**: maggiore dello 0% e inferiore al 30% dei file contiene PII

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, individua il carico di lavoro di condivisione file nella colonna Carico di lavoro che mostra uno stato nella colonna Esposizione alla privacy.



3. Selezionare il collegamento al carico di lavoro nella colonna Carico di lavoro per visualizzarne i dettagli.



4. Nella pagina Dettagli carico di lavoro, esamina i dettagli nel riquadro Esposizione alla privacy.

Impatto dell'esposizione alla privacy sull'importanza del carico di lavoro

Le modifiche all'esposizione alla privacy possono influire sull'importanza del carico di lavoro.

Quando l'esposizione alla privacy:	Da questa esposizione alla privacy:	A questa esposizione della privacy:	Quindi, l'importanza del carico di lavoro fa questo: .
Diminuisce	Alto, medio o basso	Medio, Basso o Nessuno	Rimane lo stesso
Aumenta	Nessuno	Basso	Rimane allo standard
	Basso	Medio	Modifiche da Standard a Importante
	Basso o medio	Alto	Modifiche da Standard o Importante a Critico

Per maggiori informazioni

Per maggiori dettagli sulla classificazione dei dati, fare riferimento alla documentazione sulla classificazione dei dati:

- "Scopri di più sulla classificazione dei dati"
- "Categorie di dati privati"
- "Esamina i dati archiviati nella tua organizzazione"

Rispondere e recuperare

Gestisci gli avvisi in NetApp Ransomware Resilience

Quando NetApp Ransomware Resilience rileva un possibile attacco, visualizza un avviso sulla dashboard e nel menu Notifiche. Ransomware Resilience acquisisce immediatamente uno snapshot. Quando ricevi un avviso, esamina il potenziale rischio nella scheda **Alerts** di Ransomware Resilience per valutare l'impatto sui tuoi dati e prevenire un potenziale attacco ransomware.

Se Ransomware Resilience rileva un possibile attacco, viene visualizzata una notifica nelle impostazioni di notifica della Console e viene inviata un'email agli indirizzi configurati. L'email include informazioni sulla gravità, sul workload interessato e un collegamento all'alert nella scheda **Alerts** di Ransomware Resilience.

Puoi ignorare i falsi positivi o decidere di recuperare immediatamente i tuoi dati.

Se si ignora l'avviso, Ransomware Resilience apprende questo comportamento, lo associa alle normali operazioni e non avvia più un avviso.

Per iniziare a recuperare i dati, contrassegna l'avviso come pronto per il recupero, in modo che l'amministratore dell'archiviazione possa avviare il processo di recupero.

Ogni avviso potrebbe includere più incidenti su volumi e stati diversi. Esaminare tutti gli incidenti.

Come vengono generati gli avvisi

Ransomware Resilience si basa su prove relative a modelli di entropia dei dati, tipi di estensione dei file e crittografia per generare avvisi. Gli avvisi si basano sui seguenti eventi:

- Violazione dei dati
- Distruzione dei dati
- Le estensioni dei file sono state create o modificate
- Creazione di file con un confronto tra i tassi rilevati e quelli previsti
- Eliminazione dei file con un confronto tra i tassi rilevati e quelli previsti
- Comportamento sospetto dell'utente
- Quando la crittografia è elevata, senza modifiche all'estensione del file

Per avvisi di violazione dei dati, distruzione dei dati e comportamento sospetto degli utenti, è necessario configurare "rilevamento dell'attività dell'utente".

Tipi e stati di avviso

Gli avvisi hanno uno dei due stati: **Nuovo** o **Inattivo**.

Un avviso è classificato come uno dei seguenti tipi:

- **Potenziale attacco**: Un avviso viene classificato come potenziale attacco quando:
  - Autonomous Ransomware Protection rileva una nuova estensione e l'occorrenza si ripete più di 20 volte nelle ultime 24 ore (comportamento predefinito).

    - Vengono rilevate violazioni dei dati.
    - È stata rilevata la distruzione dei dati.
- **Avviso**: un avviso si verifica in base ai seguenti comportamenti:
    - Non è mai stata identificata prima una nuova estensione e lo stesso comportamento non si ripete abbastanza volte da poter essere considerato un attacco.
    - Si osserva un'elevata entropia.
    - L'attività di lettura, scrittura, ridenominazione o eliminazione dei file è raddoppiata rispetto ai livelli normali.

Per gli ambienti SAN, gli avvisi si basano solo sull'entropia elevata.

Le prove si basano sulle informazioni di Autonomous Ransomware Protection in ONTAP. Per i dettagli, fare riferimento a "Panoramica sulla protezione autonoma dal ransomware" .

Stati di allerta

Un incidente di allerta può avere i seguenti stati:

Stato	Descrizione
Nuovo	Tutti gli incidenti sono contrassegnati come "nuovi" quando vengono identificati per la prima volta.
In revisione	È possibile contrassegnare manualmente un incidente di allerta come "in review" mentre lo si valuta.
Respinto	Se sospetti che l'attività non sia un attacco ransomware, puoi modificare lo stato in "dismissed". + ATTENZIONE: dopo aver ignorato un attacco, non puoi ripristinarne lo stato. Se ignori un workload, tutte le copie snapshot eseguite automaticamente in risposta al potenziale attacco ransomware verranno eliminate definitivamente.
Risolto	L'incidente è stato risolto.
Risolto automaticamente	Per gli avvisi di bassa priorità, l'incidente viene risolto automaticamente se non è stata intrapresa alcuna azione su di esso entro cinque giorni.

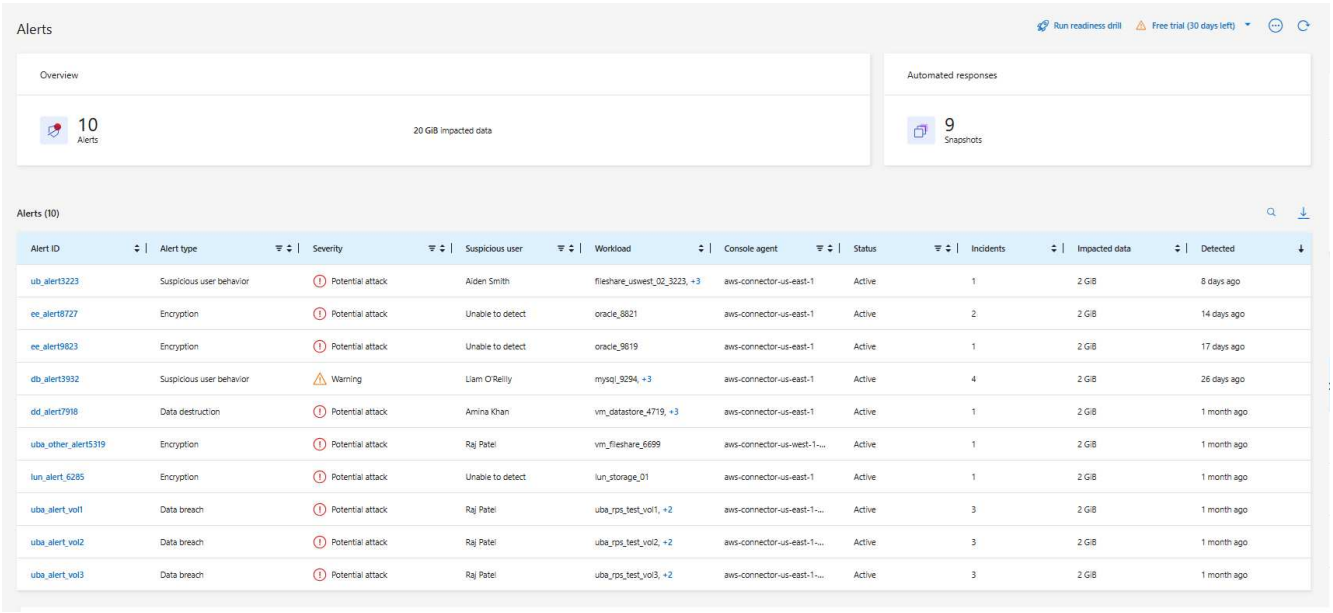
Visualizza avvisi

È possibile accedere agli avvisi dalla dashboard di NetApp Ransomware Resilience o dalla scheda **Alerts**.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Nella dashboard NetApp Ransomware Resilience, esamina il riquadro Avvisi.
2. Selezionare **Visualizza tutto** sotto uno degli stati.
3. Selezionare un avviso per esaminare tutti gli incidenti su ciascun volume per ciascun avviso.
4. Per rivedere altri avvisi, seleziona **Avviso** nel breadcrumb in alto a sinistra.
5. Esaminare gli avvisi nella pagina Avvisi.



6. Continua con una delle seguenti opzioni:
   - Rileva attività dannose e comportamenti anomali degli utenti .
   - Contrassegna gli incidenti ransomware come pronti per il ripristino (dopo che gli incidenti sono stati neutralizzati) .
   - Ignorare gli incidenti che non sono potenziali attacchi .

Rispondere a un'e-mail di avviso

Quando Ransomware Resilience rileva un potenziale attacco, invia una notifica via email agli utenti iscritti, in base alle preferenze di notifica di iscrizione configurate nelle impostazioni della NetApp Console. L'email contiene informazioni sull'avviso, tra cui la gravità e le risorse interessate.

Per impostare le notifiche e-mail nella NetApp Console, vedere "Imposta le impostazioni di notifica via email".

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Visualizza l'email.
2. Nell'email, seleziona **Visualizza avviso** e accedi a Ransomware Resilience.

   Viene visualizzata la pagina Avvisi.

3. Esaminare tutti gli incidenti su ciascun volume per ciascun avviso.
4. Per rivedere altri avvisi, seleziona **Avviso** nel breadcrumb in alto a sinistra.
5. Continua con una delle seguenti opzioni:
   - Rileva attività dannose e comportamenti anomali degli utenti .
   - Contrassegna gli incidenti ransomware come pronti per il ripristino (dopo che gli incidenti sono stati neutralizzati) .

- Ignorare gli incidenti che non sono potenziali attacchi .

Rileva attività dannose e comportamenti anomali degli utenti

Nella scheda Avvisi è possibile verificare se si è verificata un'attività dannosa o un comportamento anomalo da parte dell'utente.

È necessario aver configurato un agente di attività utente e abilitato una policy di protezione con rilevamento del comportamento utente per visualizzare gli avvisi a livello utente. La colonna **Utente sospetto** viene visualizzata nella dashboard Avvisi solo quando il rilevamento del comportamento utente è abilitato. Per abilitare il rilevamento degli utenti sospetti, vedere "Attività utente sospetta".

Visualizza attività dannose

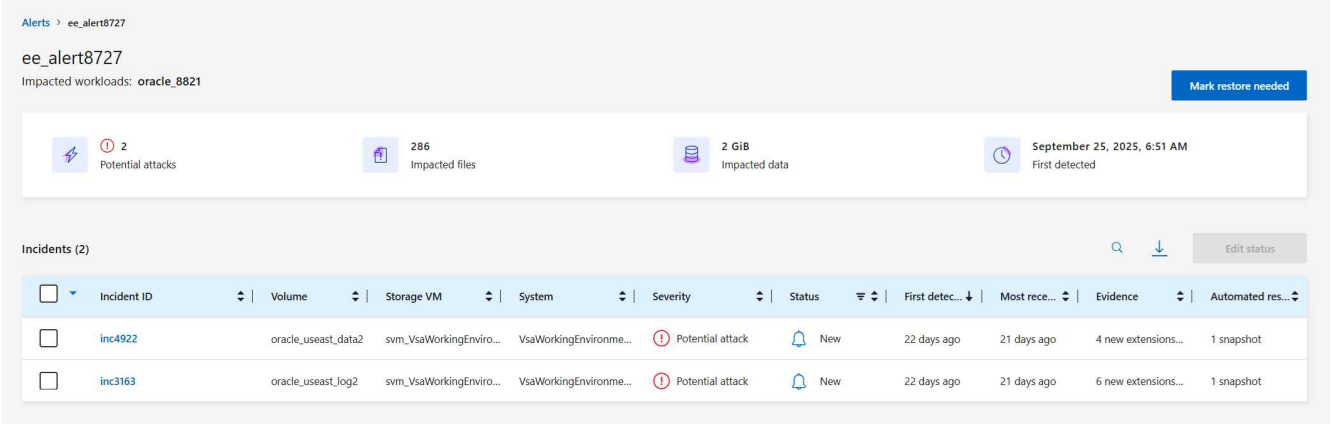
Quando Autonomous Ransomware Protection attiva un avviso in Ransomware Resilience, puoi visualizzare i seguenti dettagli:

- Quando è stato attivato l'avviso
- Quando l'accesso è stato modificato o negato
- Entropia dei dati in arrivo
- Tasso di creazione previsto di nuovi file rispetto al tasso rilevato
- Tasso di eliminazione previsto dei file rispetto al tasso rilevato
- Frequenza di ridenominazione prevista dei file rispetto alla frequenza rilevata
- Carichi di lavoro, volumi, file e directory interessati

Questi dettagli sono visualizzabili per i carichi di lavoro NAS. Per gli ambienti SAN sono disponibili solo i dati sull'entropia.

Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.
2. Seleziona un avviso.
3. Esaminare gli incidenti nell'avviso.



4. Seleziona un incidente per esaminarne i dettagli.

Visualizza il comportamento anomalo dell'utente

Se hai configurato il rilevamento degli utenti sospetti per visualizzare comportamenti anomali degli utenti, puoi visualizzare i dati a livello di utente e bloccare utenti specifici. Per abilitare le impostazioni per gli utenti sospetti, consulta "Configura agenti e collettori per il rilevamento delle attività degli utenti".

Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.
2. Seleziona un avviso.
3. Esaminare gli incidenti nell'avviso.
   a. Per bloccare un utente sospetto nel tuo ambiente, seleziona **Block** accanto al nome dell'utente.
   b. Per disattivare gli avvisi su un determinato utente che è oggetto di un avviso che sai essere falso, seleziona i tre puntini (... quindi **Escludi questo utente dal monitoraggio**. Rivedi la finestra di dialogo quindi seleziona **Escludi** per confermare.

Per riattivare gli avvisi per un utente, restituisci l'avviso. Seleziona i tre puntini e poi **Includi questo utente nel monitoraggio**. Puoi anche "Escludi utenti" dal monitoraggio.

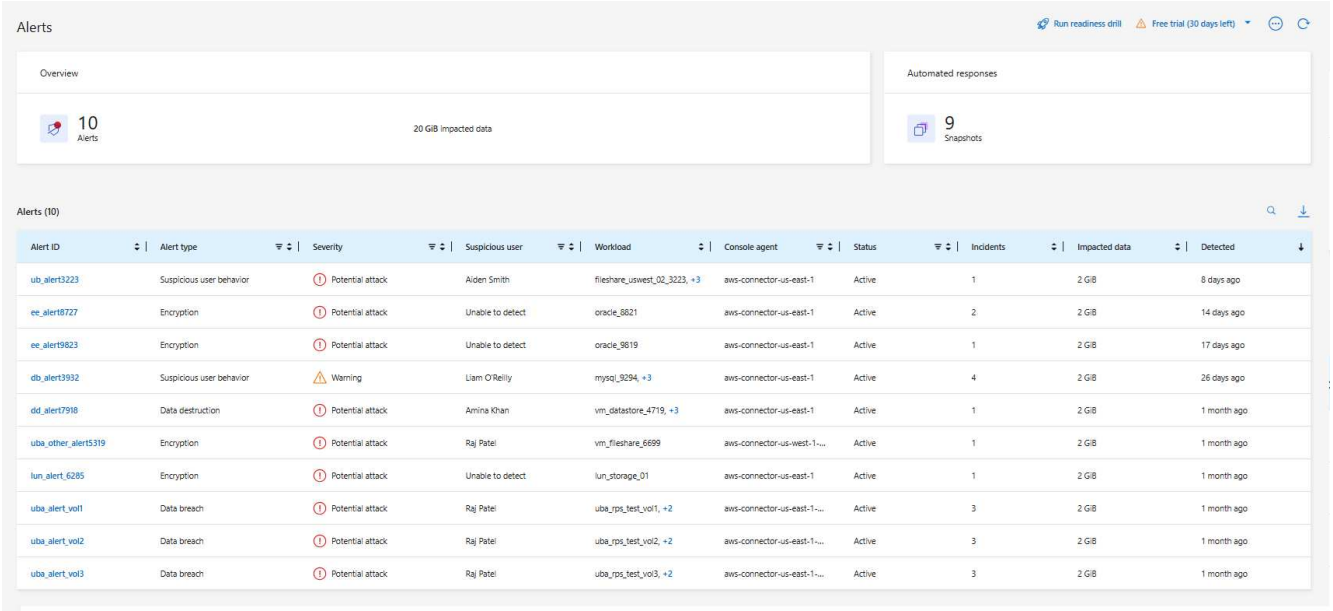
Contrassegna gli incidenti ransomware come pronti per il ripristino (dopo che gli incidenti sono stati neutralizzati)

Dopo aver fermato l'attacco, informa l'amministratore dello storage che i dati sono pronti così che possa avviare il processo di ripristino.

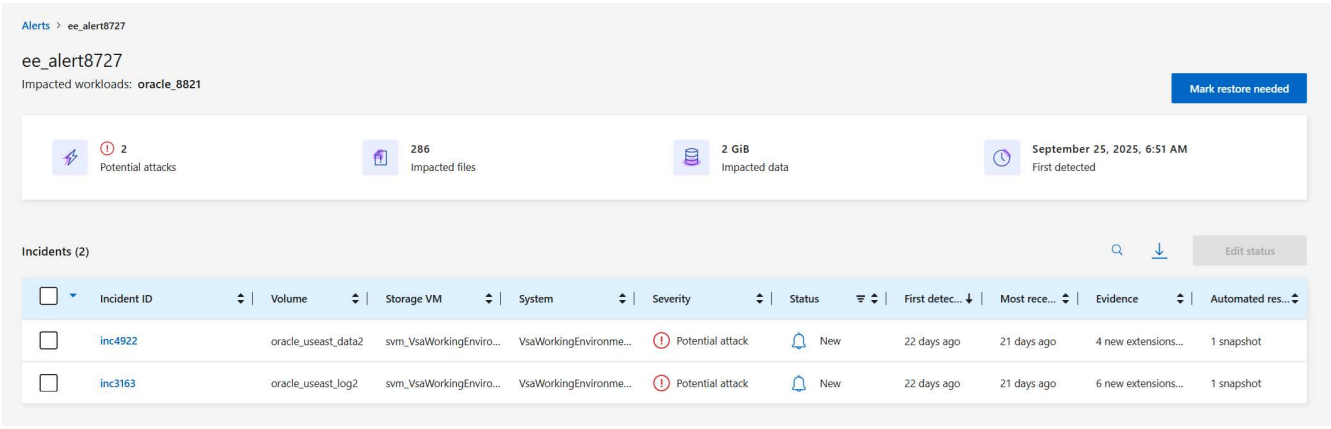
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.



2. Nella pagina Avvisi, seleziona l'avviso.
3. Esaminare gli incidenti nell'avviso.



4. Se si determina che gli incidenti sono pronti per il ripristino, selezionare **Segna come ripristino necessario**.
5. Conferma l'azione e seleziona **Segna come ripristino necessario**.
6. Per avviare il ripristino del carico di lavoro, selezionare **Recupera** carico di lavoro nel messaggio oppure selezionare la scheda **Ripristino**.

Risultato

Dopo che l'avviso è stato contrassegnato per il ripristino, l'avviso passa dalla scheda Avvisi alla scheda Ripristino.

Ignorare gli incidenti che non sono potenziali attacchi

Dopo aver esaminato gli incidenti, è necessario stabilire se si tratta di potenziali attacchi. Se non si tratta di minacce reali, possono essere ignorate.

Puoi ignorare i falsi positivi o decidere di recuperare immediatamente i tuoi dati. Se si ignora l'avviso, Ransomware Resilience apprende questo comportamento e lo associa alle normali operazioni, senza più avviare un avviso per tale comportamento.

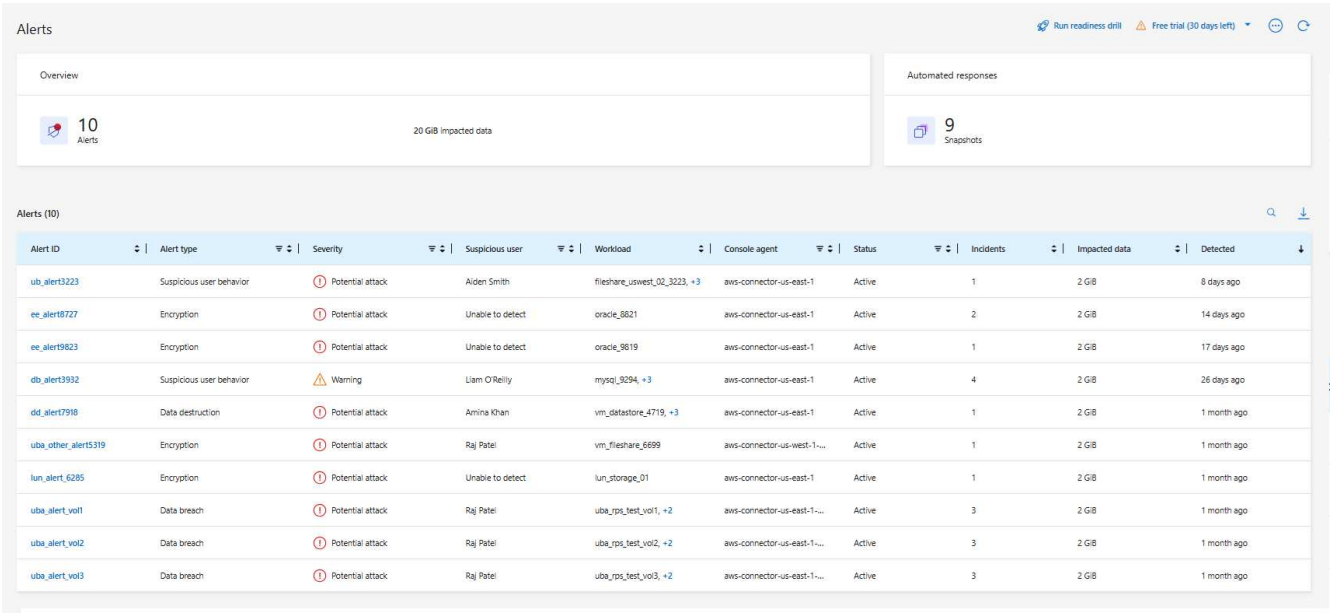
Se si elimina un carico di lavoro, tutte le copie snapshot eseguite automaticamente in risposta a un potenziale attacco ransomware vengono eliminate definitivamente.

Se si ignora un avviso, non è possibile modificarne lo stato né annullare la modifica.

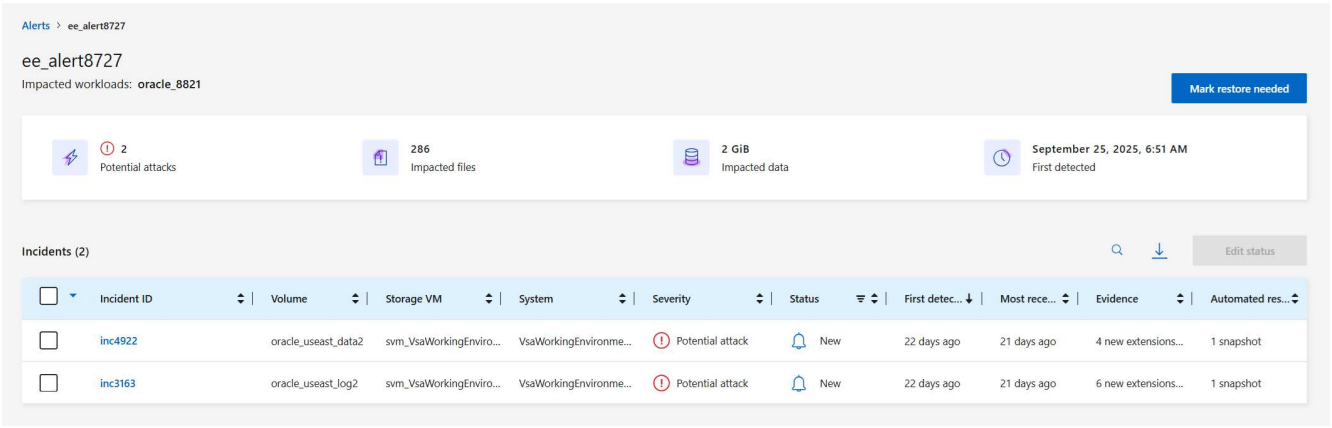
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

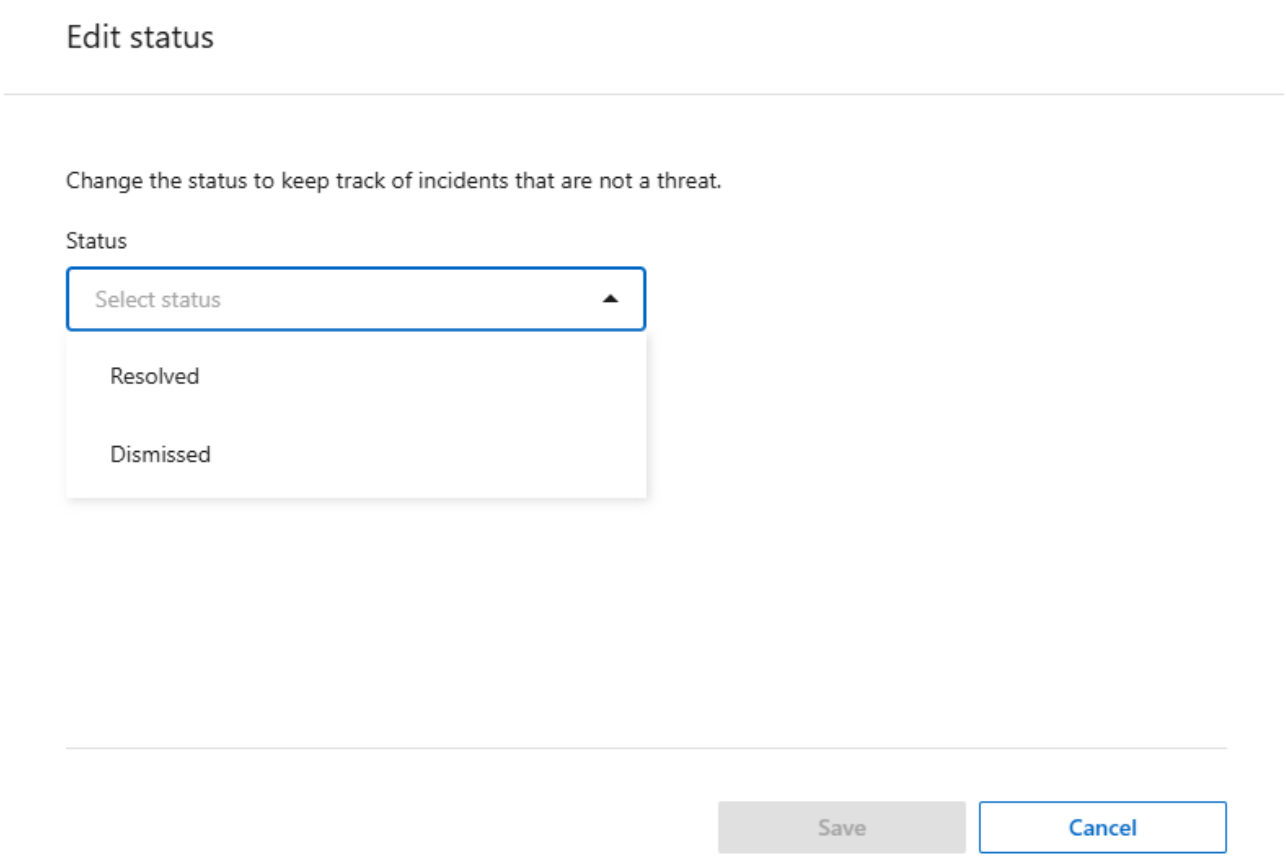
1. Dal menu Ransomware Resilience, seleziona **Avvisi**.



2. Nella pagina Avvisi, seleziona l'avviso.



3. Seleziona uno o più incidenti. In alternativa, selezionare tutti gli incidenti selezionando la casella ID incidente in alto a sinistra della tabella.
4. Se stabilisci che l'incidente non rappresenta una minaccia, scartalo come falso positivo:
   - Seleziona l'incidente.
   - Selezionare il pulsante **Modifica stato** sopra la tabella.



5. Dalla casella Modifica stato, seleziona lo stato **Ignorato**.

   Vengono visualizzate informazioni aggiuntive sul carico di lavoro e sulle copie snapshot eliminate.

6. Seleziona **Salva**.

   Lo stato dell'incidente o degli incidenti cambia in "Ignorato".

Visualizza un elenco dei file interessati

Prima di ripristinare il carico di lavoro di un'applicazione a livello di file, è possibile visualizzare un elenco dei file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco dei file interessati. Quindi utilizzare la pagina Recupero per caricare l'elenco e scegliere quali file ripristinare.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

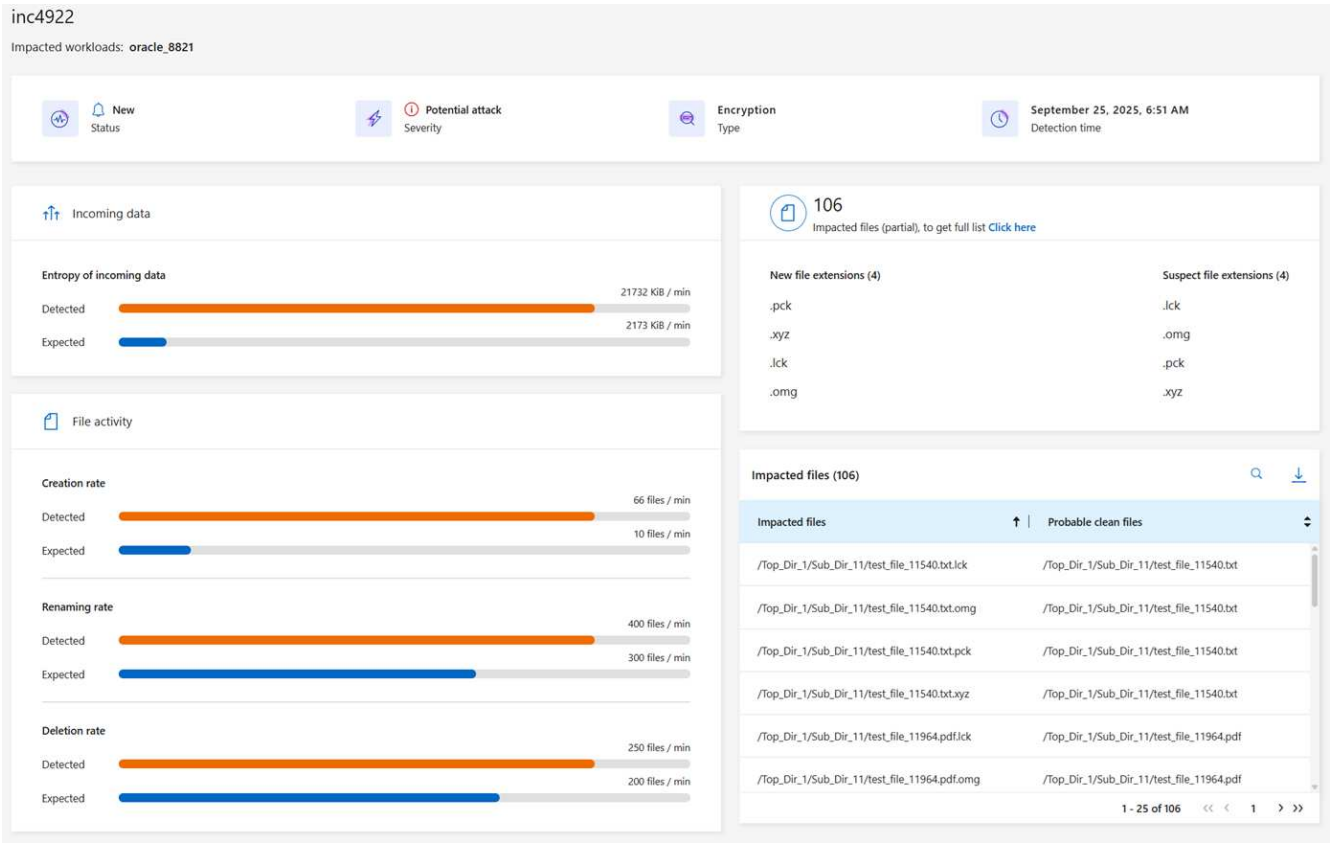
Passi

Utilizzare la pagina Avvisi per recuperare l'elenco dei file interessati.

Se un volume presenta più avvisi, potrebbe essere necessario scaricare l'elenco CSV dei file interessati per ciascun avviso.

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.

2. Nella pagina Avvisi, ordina i risultati in base al carico di lavoro per visualizzare gli avvisi per il carico di lavoro dell'applicazione che desideri ripristinare.
3. Dall'elenco degli avvisi per quel carico di lavoro, seleziona un avviso.
4. Per quell'avviso, seleziona un singolo incidente.



5. Per quell'incidente, seleziona l'icona di download per scaricare l'elenco dei file interessati in formato CSV.

Recupera da un attacco ransomware (dopo che gli incidenti sono stati neutralizzati) con NetApp Ransomware Resilience

Dopo che i carichi di lavoro sono stati contrassegnati come "Ripristino necessario", NetApp Ransomware Resilience consiglia un punto di ripristino effettivo (RPA) e orchestra il flusso di lavoro per un ripristino a prova di crash.

- Se l'applicazione o la macchina virtuale è gestita da NetApp Backup and Recovery o Ransomware Resilience, Ransomware Resilience esegue un ripristino coerente con l'arresto anomalo, in cui tutti i dati che erano presenti nel volume nello stesso momento vengono ripristinati, ad esempio, se il sistema si è arrestato in modo anomalo.

  È possibile ripristinare il carico di lavoro selezionando tutti i volumi, volumi specifici o file specifici.

Il ripristino del carico di lavoro può avere un impatto sui carichi di lavoro in esecuzione. Dovresti coordinare i processi di recupero con le parti interessate appropriate.

Un carico di lavoro può avere uno dei seguenti stati di ripristino:

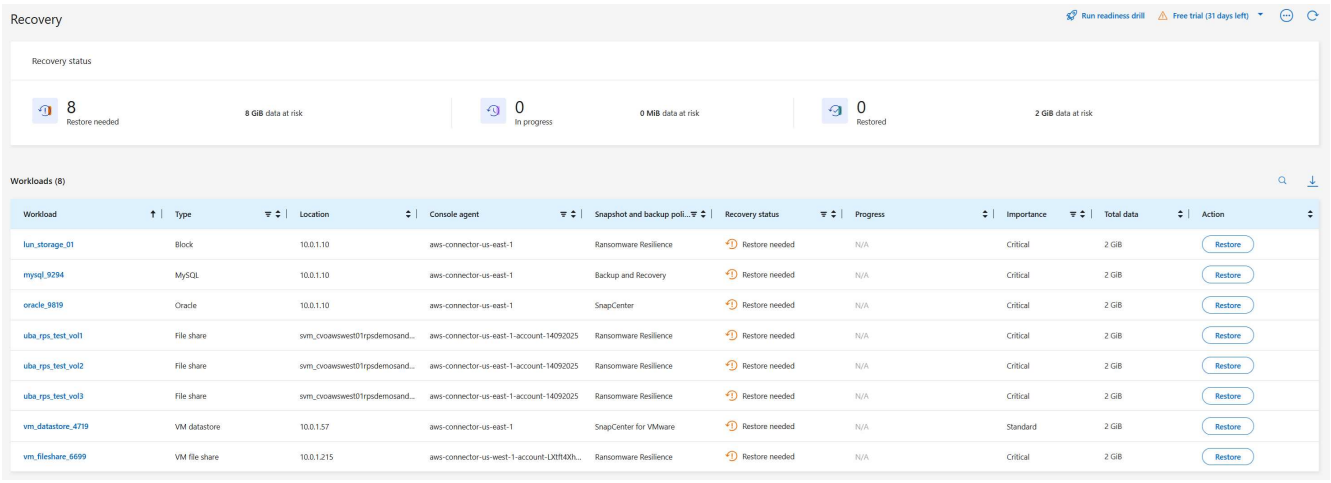
- **Ripristino necessario**: il carico di lavoro deve essere ripristinato.
- **In corso**: l'operazione di ripristino è attualmente in corso.
- **Ripristinato**: il carico di lavoro è stato ripristinato.
- **Non riuscito**: il processo di ripristino del carico di lavoro non è stato completato.

Visualizza i carichi di lavoro pronti per essere ripristinati

Esaminare i carichi di lavoro che si trovano nello stato di ripristino "Ripristino necessario".

Passi

1. Eseguire una delle seguenti operazioni:
   - Dalla dashboard, controlla i totali "Ripristino necessario" nel riquadro Avvisi e seleziona **View all**.
   - Dal menu, seleziona **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Recupero**.



Ripristina un carico di lavoro

Utilizzando Ransomware Resilience, l'amministratore dell'archiviazione può stabilire il modo migliore per ripristinare i carichi di lavoro dal punto di ripristino consigliato o da quello preferito.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

L'amministratore dell'archiviazione di sicurezza può recuperare i dati a diversi livelli:

- Recupera tutti i volumi
- Ripristina un'applicazione a livello di volume o di file e cartella.
- Ripristina una condivisione file a livello di volume, directory o file/cartella.
- Ripristina da un datastore a livello di VM.

Il processo varia a seconda del tipo di carico di lavoro.

Passi

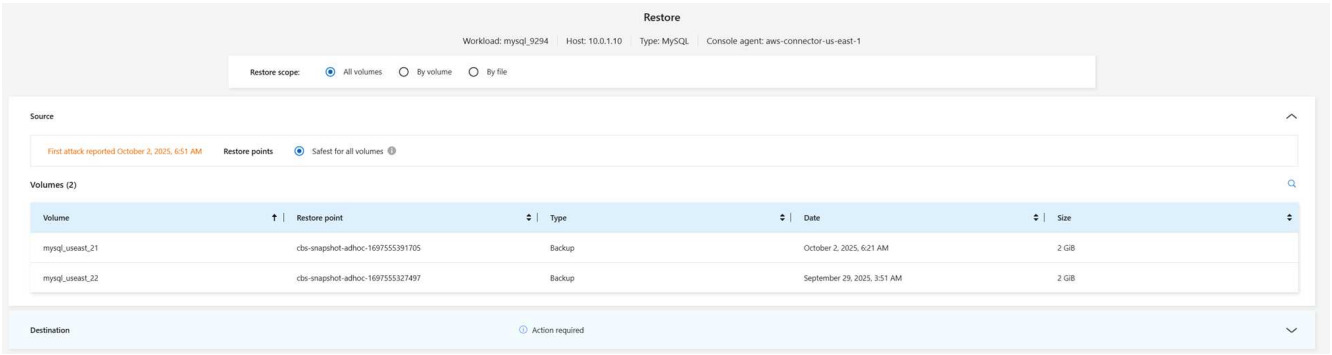
1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Recupero**.
3. Selezionare un carico di lavoro che si trovi nello stato "Ripristino necessario".
4. Per ripristinare, seleziona **Ripristina**.
5. **Ambito di ripristino**: seleziona il tipo di ripristino che desideri completare:
    - Tutti i volumi
    - Per volume
    - Per file: è possibile specificare una cartella o singoli file da ripristinare.

    Per i carichi di lavoro SAN, è possibile eseguire il ripristino solo per carico di lavoro.

    È possibile selezionare fino a 100 file o una singola cartella.
6. Procedere con una delle seguenti procedure a seconda che si sia scelto applicazione, volume o file.

Ripristina tutti i volumi

1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Selezionare un carico di lavoro che si trovi nello stato "Ripristino necessario".
3. Per ripristinare, seleziona **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, seleziona **Tutti i volumi**.



5. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli.
    a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

    Ransomware Resilience identifica come punto di ripristino migliore l'ultimo backup appena prima dell'incidente e mostra l'indicazione "Il più sicuro per tutti i volumi". Ciò significa che tutti i volumi verranno ripristinati in una copia precedente al primo attacco al primo volume rilevato.
6. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
    a. Selezionare il sistema.
    b. Selezionare la VM di archiviazione.
    c. Selezionare l'aggregato.

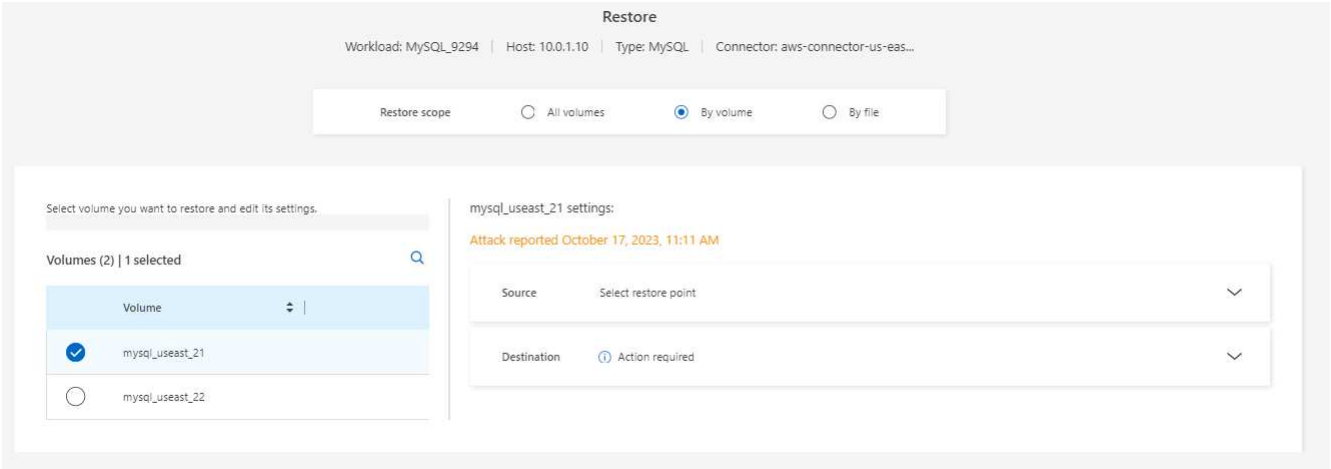
d. Modifica il prefisso del volume che verrà aggiunto a tutti i nuovi volumi.

Il nuovo nome del volume appare come prefisso + nome del volume originale + nome del backup + data del backup.

7. Seleziona **Salva**.
8. Selezionare **Avanti**.
9. Rivedi le tue selezioni.
10. Selezionare **Ripristina**.
11. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati.

Ripristinare un carico di lavoro applicativo a livello di volume

1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Selezionare un carico di lavoro applicativo che si trovi nello stato "Ripristino necessario".
3. Per ripristinare, seleziona **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, seleziona **Per volume**.



5. Nell'elenco dei volumi, seleziona il volume che desideri ripristinare.
6. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli.
   a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

Ransomware Resilience identifica come punto di ripristino migliore l'ultimo backup appena prima dell'incidente e mostra l'indicazione "Consigliato".

7. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
   a. Selezionare il sistema.
   b. Selezionare la VM di archiviazione.
   c. Selezionare l'aggregato.
   d. Controllare il nuovo nome del volume.

Il nuovo nome del volume appare come nome del volume originale + nome del backup + data del backup.

8. Seleziona **Salva**.
9. Selezionare **Avanti**.
10. Rivedi le tue selezioni.
11. Selezionare **Ripristina**.
12. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati.

Ripristinare il carico di lavoro di un'applicazione a livello di file

Prima di ripristinare il carico di lavoro di un'applicazione a livello di file, è possibile visualizzare un elenco dei file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco dei file interessati. Quindi utilizzare la pagina Recupero per caricare l'elenco e scegliere quali file ripristinare.

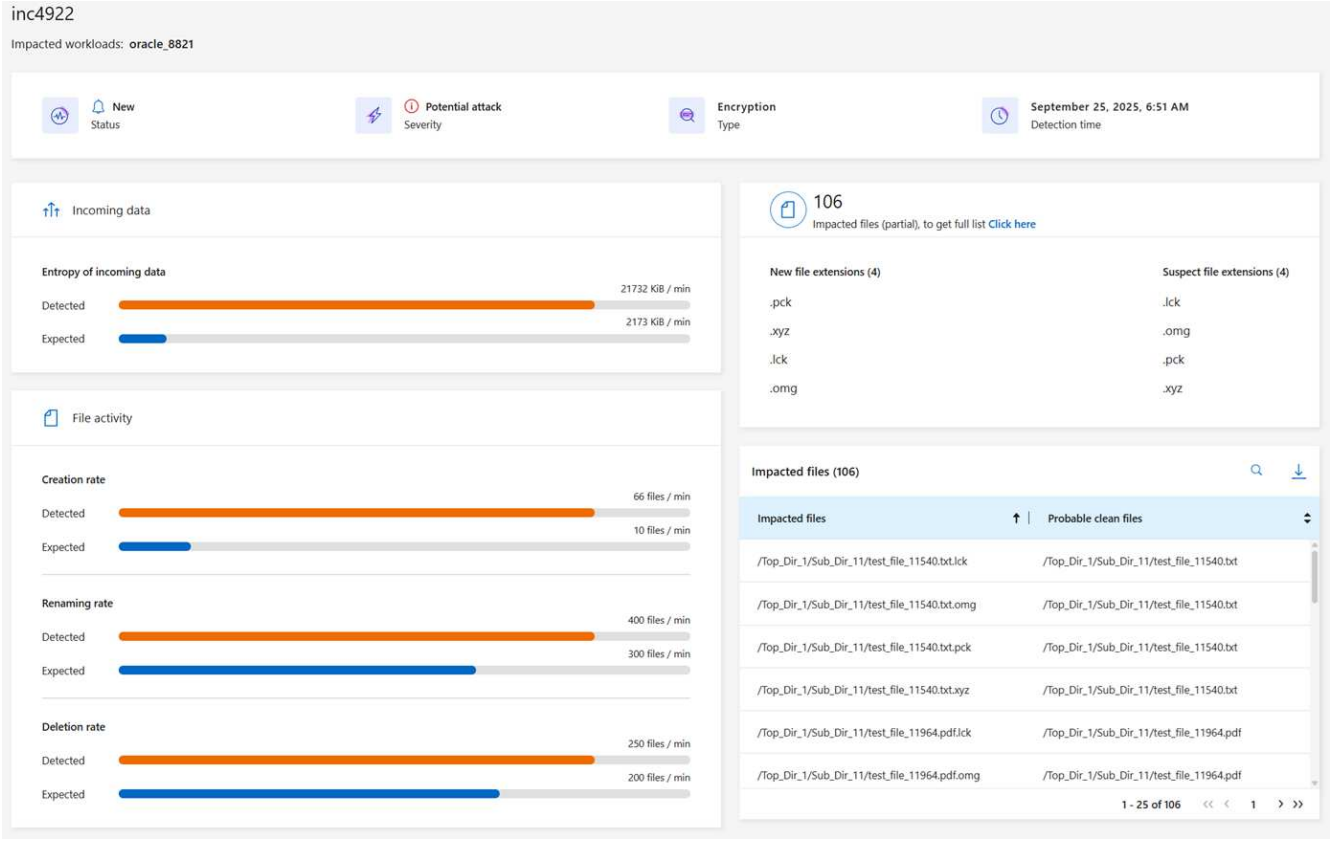
È possibile ripristinare il carico di lavoro di un'applicazione a livello di file sullo stesso sistema o su un sistema diverso.

Passaggi per ottenere l'elenco dei file interessati

Utilizzare la pagina Avvisi per recuperare l'elenco dei file interessati.

Se un volume presenta più avvisi, sarà necessario scaricare l'elenco CSV dei file interessati per ciascun avviso.

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.
2. Nella pagina Avvisi, ordina i risultati in base al carico di lavoro per visualizzare gli avvisi per il carico di lavoro dell'applicazione che desideri ripristinare.
3. Dall'elenco degli avvisi per quel carico di lavoro, seleziona un avviso.
4. Per quell'avviso, seleziona un singolo incidente.



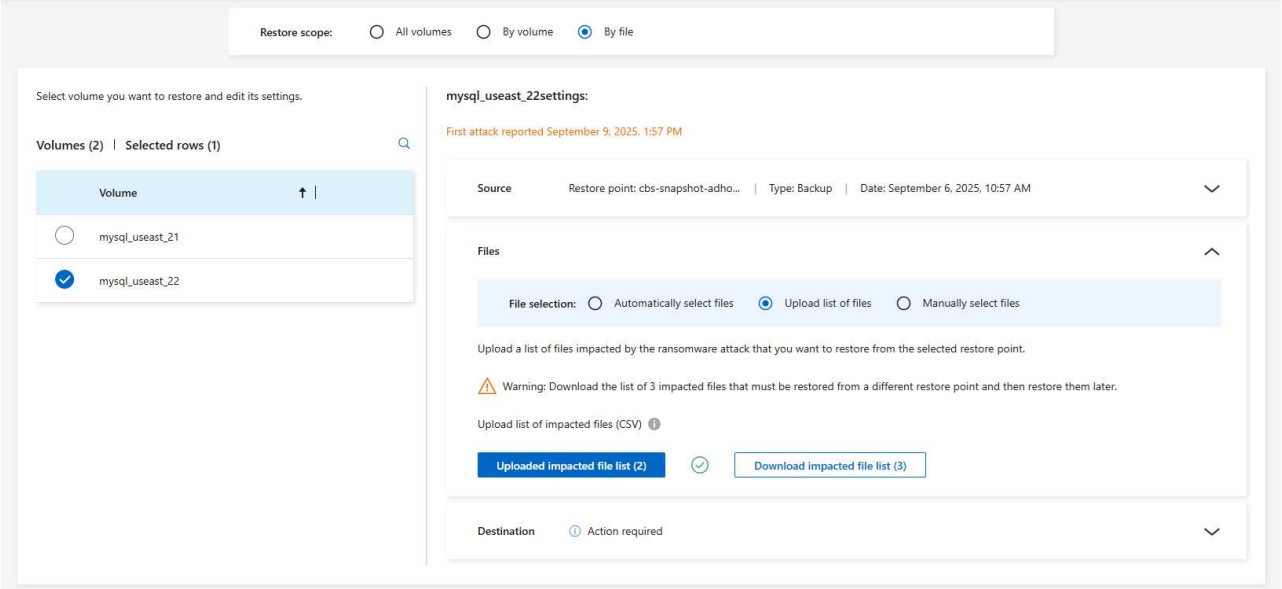
5. Per visualizzare l'elenco completo dei file, seleziona **Clicca qui** nella parte superiore del riquadro File interessati.
6. Per tale incidente, seleziona l'icona di download e scarica l'elenco dei file interessati in formato CSV.

Passaggi per ripristinare quei file

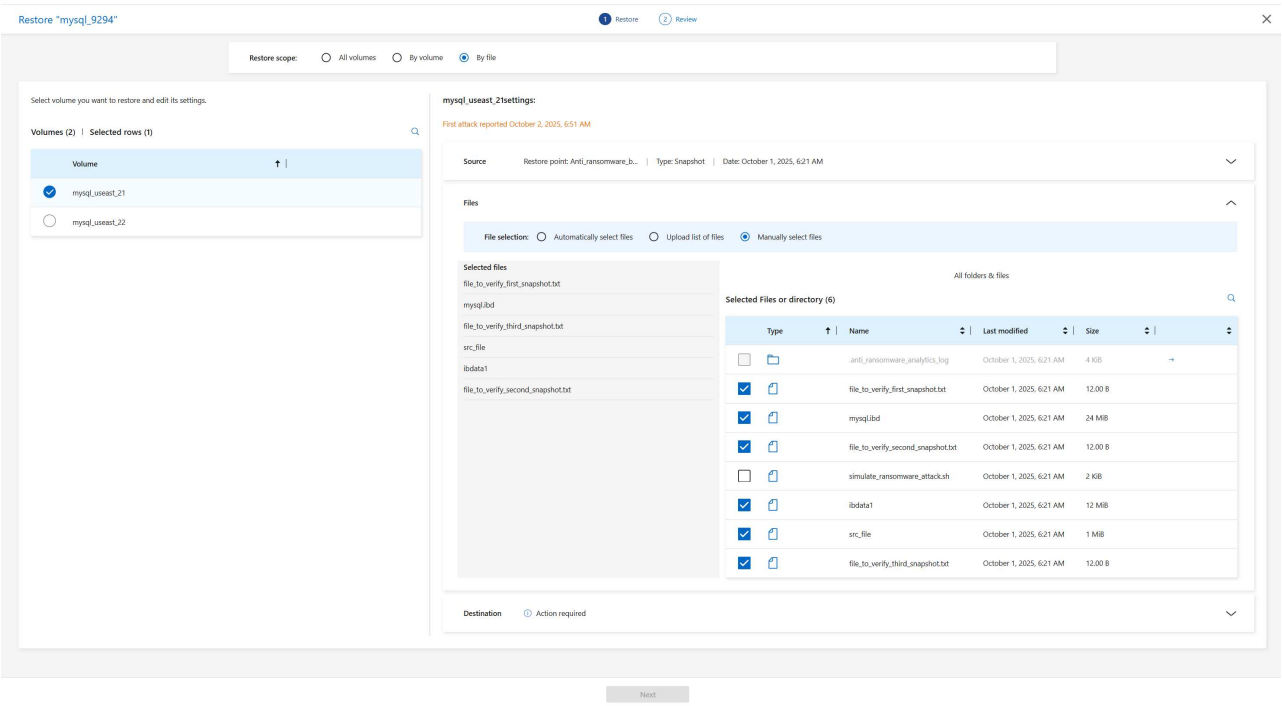
1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Selezionare un carico di lavoro applicativo che si trovi nello stato "Ripristino necessario".
3. Per ripristinare, seleziona **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, seleziona **Per file**.
5. Nell'elenco dei volumi, seleziona il volume che contiene i file che desideri ripristinare.
6. **Punto di ripristino**: seleziona la freccia rivolta verso il basso accanto a **Punto di ripristino** per visualizzare i dettagli. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> Nella colonna Motivo nel riquadro Punti di ripristino viene visualizzato il motivo dello snapshot o del backup, ovvero "Pianificato" o "Risposta automatica a un incidente ransomware".

7. **File**:
   - **Seleziona automaticamente i file**: lascia che Ransomware Resilience selezioni i file da ripristinare.
   - **Carica elenco file**: carica un file CSV contenente l'elenco dei file interessati che hai ricevuto dalla pagina Avvisi o che possiedi. È possibile ripristinare fino a 10.000 file alla volta.



- **Seleziona manualmente i file**: seleziona fino a 10.000 file o una singola cartella da ripristinare.



Se non è possibile ripristinare alcun file utilizzando il punto di ripristino selezionato, viene visualizzato un messaggio che indica il numero di file che non possono essere ripristinati e consente di scaricare l'elenco di tali file selezionando **Scarica elenco dei file interessati**.

8. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
   a. Scegli dove ripristinare i dati: la posizione di origine originale o una posizione alternativa che puoi specificare.

Sebbene i file o la directory originali verranno sovrascritti dai dati ripristinati, i nomi originali dei file e delle cartelle rimarranno gli stessi, a meno che non vengano specificati nuovi nomi.

b. Selezionare il sistema.

c. Selezionare la VM di archiviazione.

d. Facoltativamente, inserisci il percorso.

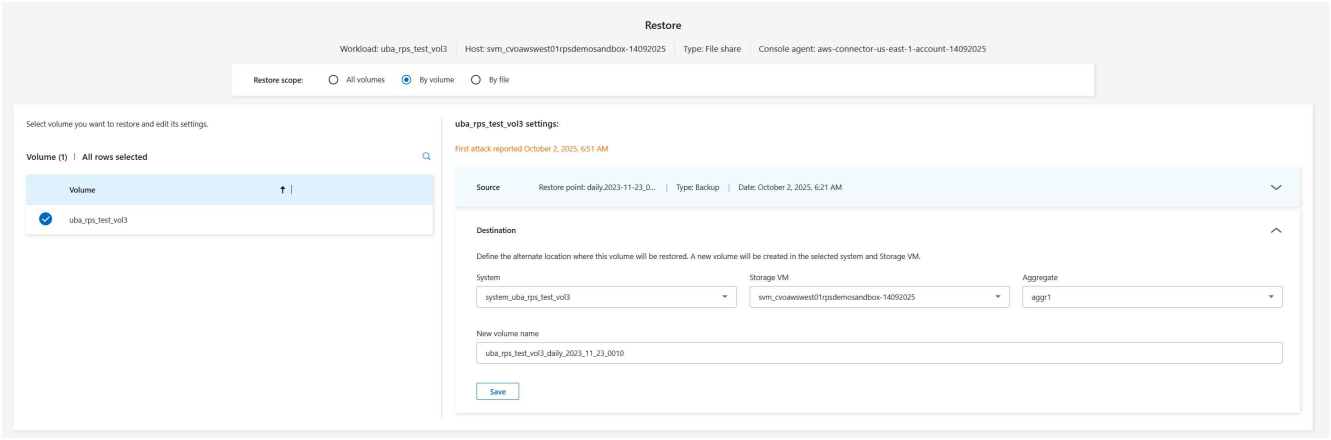
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

e. Selezionare se si desidera che i nomi dei file o delle directory ripristinati siano gli stessi della posizione corrente oppure nomi diversi.

9. Selezionare **Avanti**.
10. Rivedi le tue selezioni.
11. Selezionare **Ripristina**.
12. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati.

Ripristinare una condivisione file o un archivio dati

1. Dopo aver selezionato una condivisione file o un datastore da ripristinare, nella pagina Ripristina, nell'ambito Ripristina, seleziona **Per volume**.



2. Nell'elenco dei volumi, seleziona il volume che desideri ripristinare.
3. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli.

a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> Ransomware Resilience identifica come punto di ripristino migliore l'ultimo backup appena prima dell'incidente e mostra l'indicazione "Consigliato".

4. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.

a. Scegli dove ripristinare i dati: la posizione di origine originale o una posizione alternativa che puoi specificare.

> Sebbene i file o la directory originali verranno sovrascritti dai dati ripristinati, i nomi originali dei file e delle cartelle rimarranno gli stessi, a meno che non vengano specificati nuovi nomi.

b. Selezionare il sistema.

c. Selezionare la VM di archiviazione.

d. Facoltativamente, inserisci il percorso.

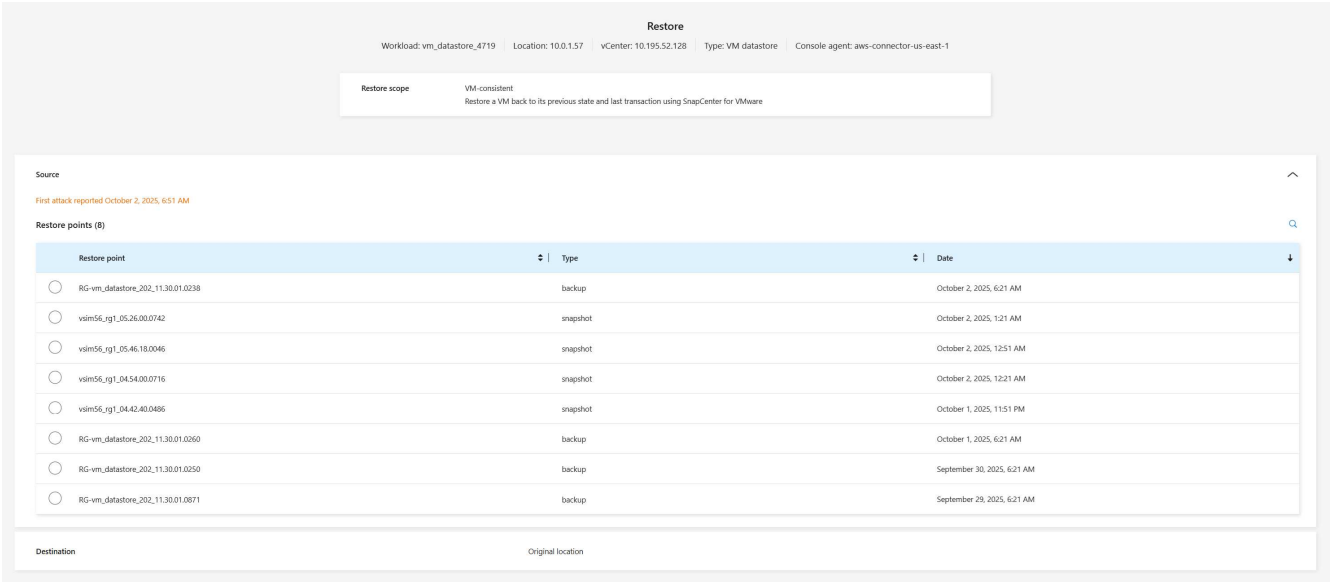
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

5. Seleziona **Salva**.
6. Rivedi le tue selezioni.
7. Selezionare **Ripristina**.
8. Dal menu, selezionare **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione passa attraverso i vari stati.

Ripristinare una condivisione file VM a livello di VM

Nella pagina Ripristino, dopo aver selezionato una VM da ripristinare, continuare con questi passaggi.

1. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli.



2. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.
3. **Destinazione**: Verso la posizione originale.
4. Selezionare **Avanti**.
5. Rivedi le tue selezioni.
6. Selezionare **Ripristina**.
7. Dal menu, selezionare **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione passa attraverso i vari stati.

Esegui un’esercitazione di preparazione agli attacchi ransomware in NetApp Ransomware Resilience

Esegui un’esercitazione di preparazione ad un attacco ransomware simulando un attacco su un nuovo carico di lavoro di esempio. Esaminare l’attacco simulato e recuperare il carico di lavoro. Utilizzare questa funzione per testare le notifiche di avviso, la risposta e il ripristino. Eseguire il trapano tutte le volte che è necessario.

I dati del tuo carico di lavoro reale non subiscono alcun impatto.

È possibile eseguire esercitazioni di preparazione sui carichi di lavoro NFS e CIFS (SMB).

Configurare un’esercitazione di preparazione all’attacco ransomware

Prima di eseguire una simulazione, imposta un’esercitazione nella pagina Impostazioni. Accedi alla pagina Impostazioni dall’opzione Azioni nel menu in alto.

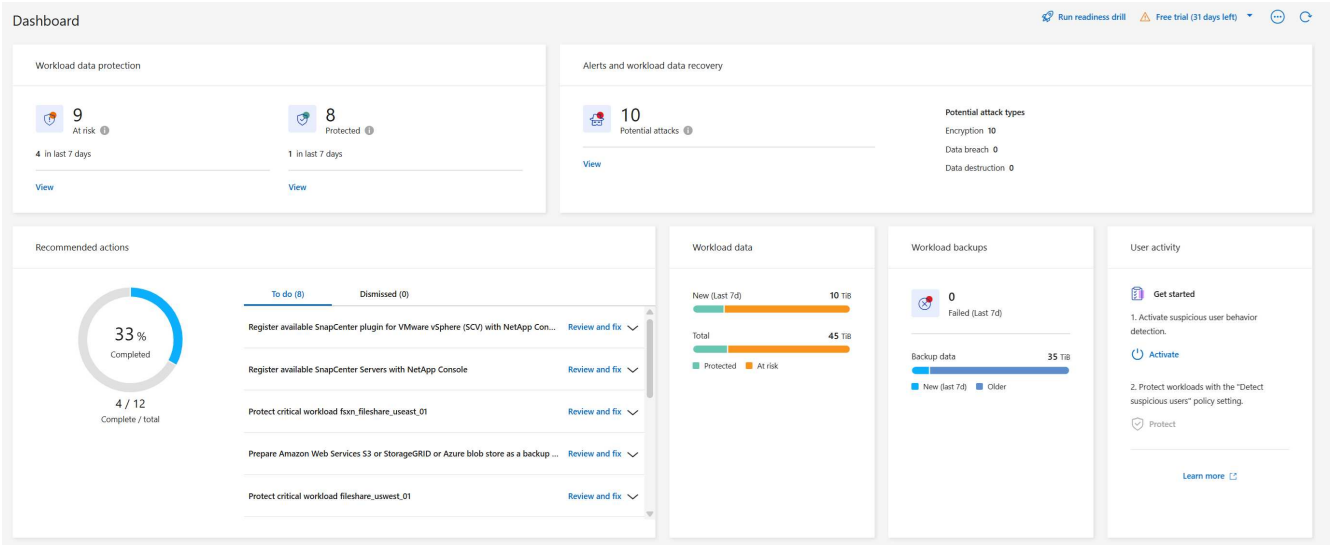
È necessario immettere un nome utente e una password nelle seguenti situazioni:

- Se si sono verificate modifiche al nome utente o alla password per la VM di archiviazione selezionata in precedenza
- Se selezioni una VM di archiviazione CIFS (SMB) diversa
- Se si immette un nome di carico di lavoro di prova diverso

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell’organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

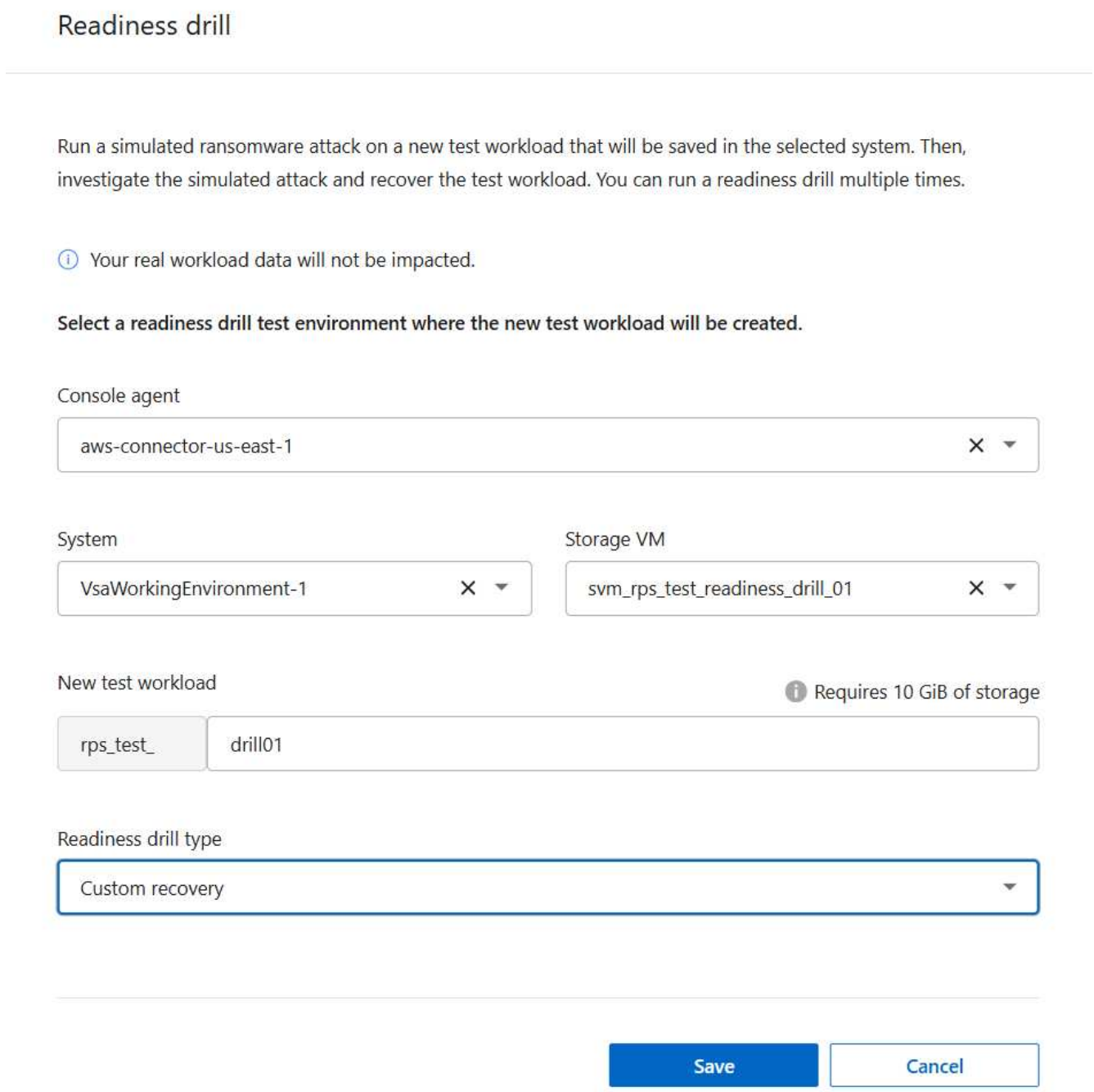
Passi

1. Dal menu NetApp Ransomware Resilience , seleziona il pulsante **Esegui esercitazione di preparazione** in alto a destra.



2. Nella scheda di esercitazione sulla prontezza nella pagina Impostazioni, seleziona **Configura**.

La Console visualizza la pagina di configurazione dell'esercitazione di preparazione.



3. Procedi come segue:
   a. Selezionare l'agente della console che si desidera utilizzare per l'esercitazione di preparazione.
   b. Selezionare un sistema di prova.
   c. Selezionare un SVM di archiviazione di prova.
   d. Se hai selezionato una VM di archiviazione CIFS (SMB), vengono visualizzati i campi **Nome utente** e **Password**. Immettere il nome utente e la password per la VM di archiviazione.
   e. Selezionare il tipo di esercitazione di preparazione. Per un ripristino manuale da una violazione dei dati crittografati, seleziona **Ripristino personalizzato**. Per il ripristino in caso di attività sospette degli

utenti, seleziona **Violazione dei dati**.

f. Immettere il nome del nuovo carico di lavoro di test da creare. Non includere trattini nel nome.

4. Seleziona **Salva**.

È possibile modificare la configurazione dell'esercitazione di preparazione in un secondo momento utilizzando la pagina Impostazioni.

Avviare un'esercitazione di preparazione

Dopo aver configurato l'esercitazione di preparazione, è possibile avviarla.

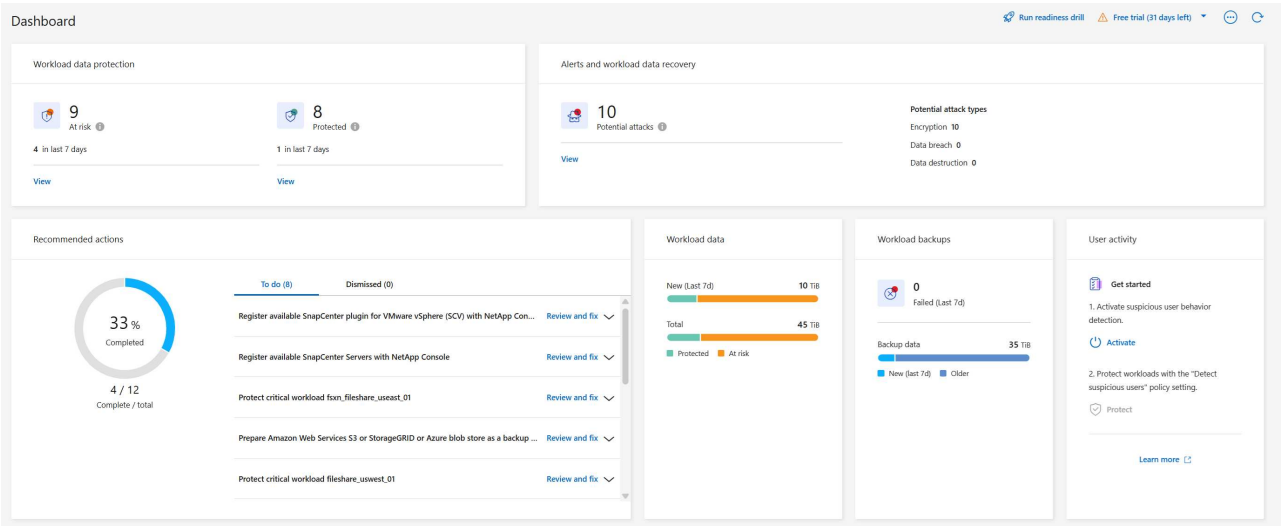
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Quando si avvia l'esercitazione di preparazione, Ransomware Resilience salta la modalità di apprendimento e avvia l'esercitazione in modalità attiva. Lo stato di rilevamento del carico di lavoro è Attivo.

Un carico di lavoro può avere uno stato di **Modalità di apprendimento** per il rilevamento ransomware quando di recente è stato assegnato un criterio di rilevamento e Ransomware Resilience esegue la scansione dei carichi di lavoro.

Passi

1. Eseguire una delle seguenti operazioni:
   - Dal menu Ransomware Resilience, seleziona il pulsante **Esegui esercitazione di preparazione** in alto a destra.



   - OPPURE, dalla pagina Impostazioni, nella scheda Esercizio di preparazione, seleziona **Avvia**.

Non è possibile modificare la configurazione dell'esercitazione di preparazione mentre l'esercitazione è in esecuzione. È possibile reimpostare il trapano per fermarlo e modificarne la configurazione.

Rispondere a un avviso di esercitazione di prontezza

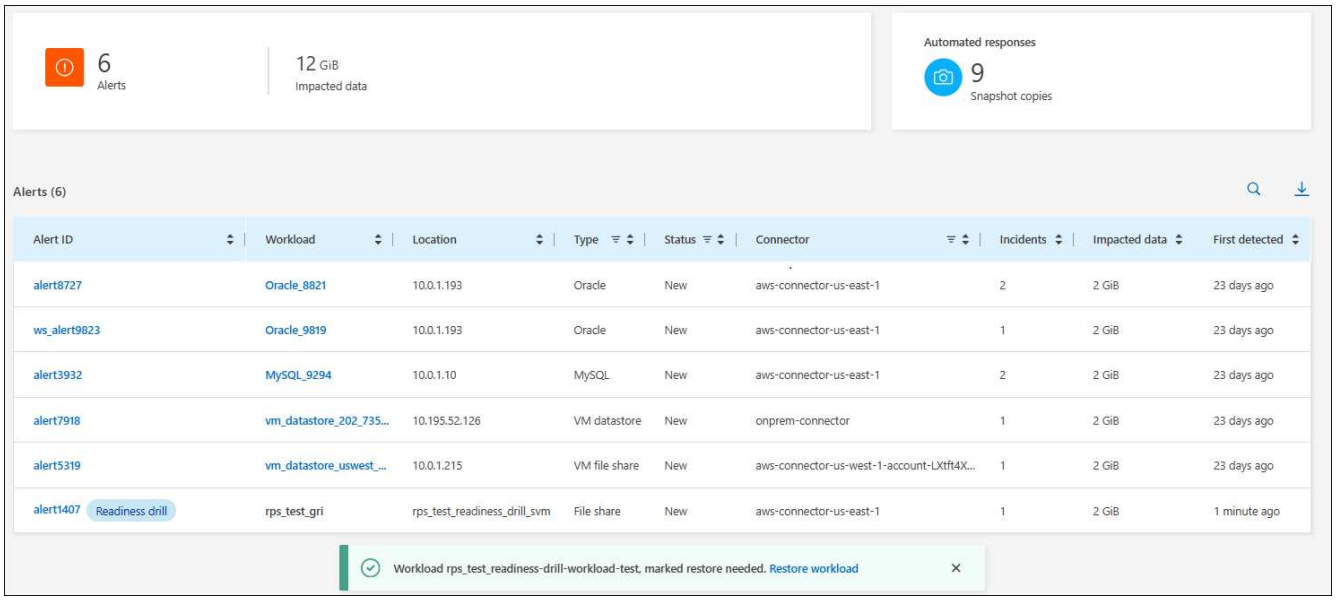
Metti alla prova la tua prontezza rispondendo a un avviso di esercitazione di prontezza.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

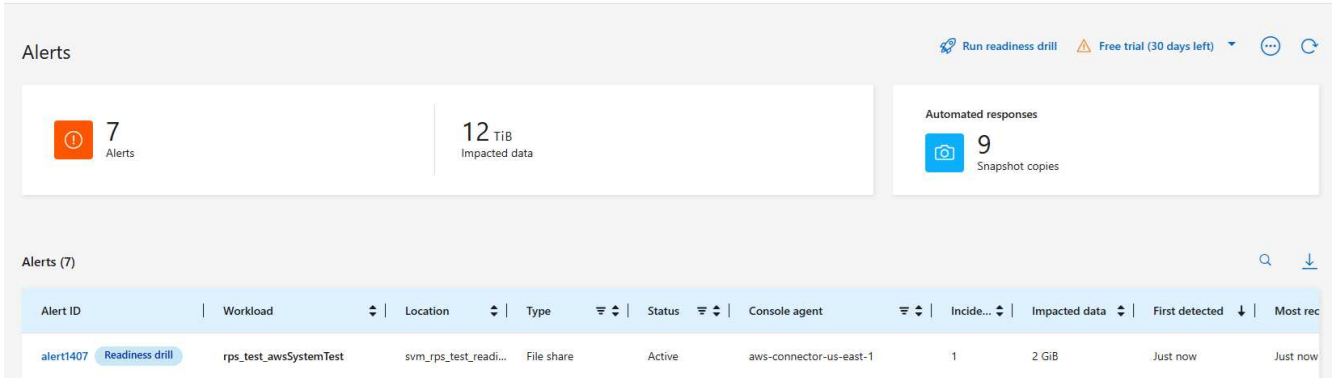
Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.

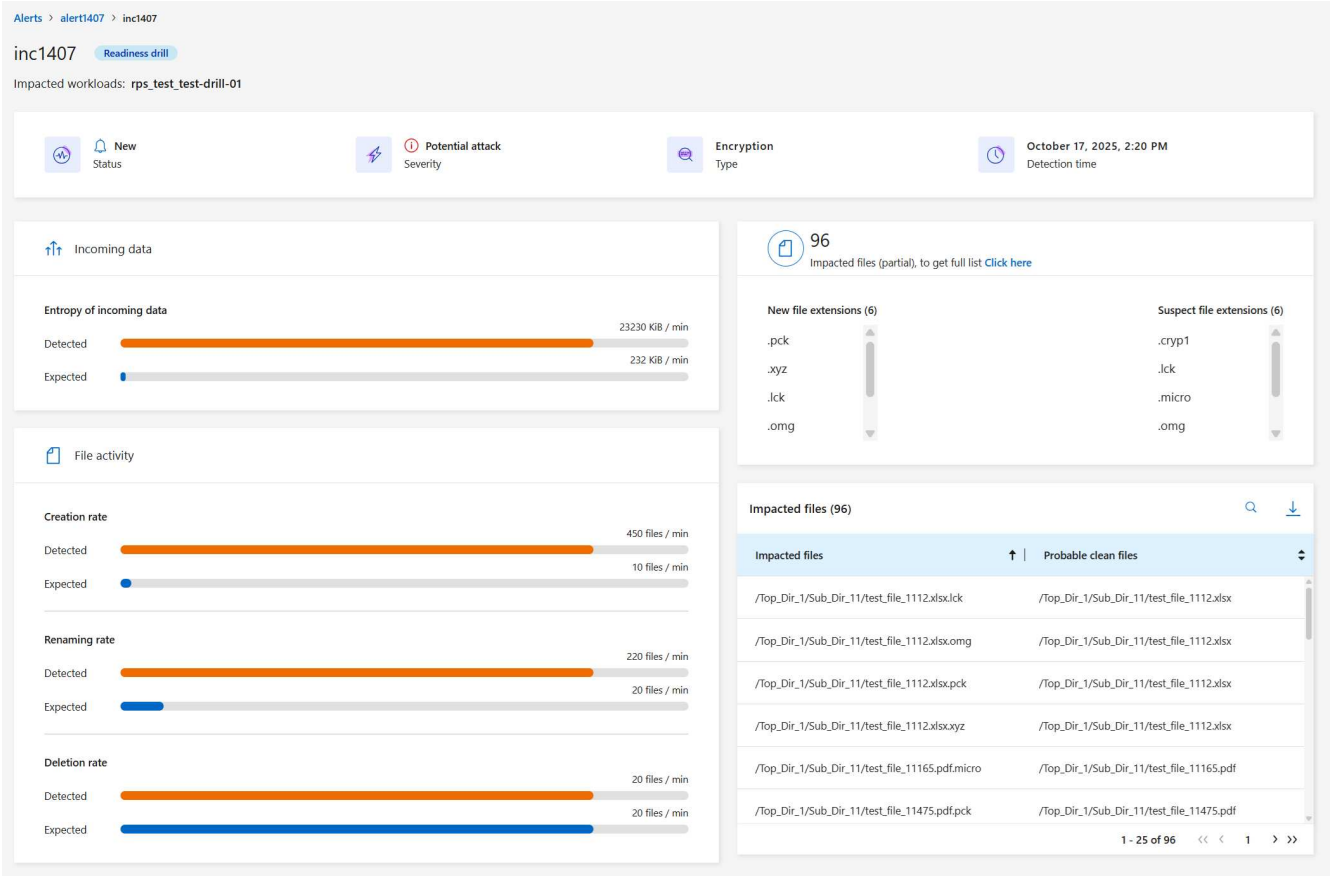
   La Console visualizza la pagina Avvisi. Nella colonna ID avviso, accanto all'ID viene visualizzato "Esercitazione di preparazione".



2. Selezionare l'avviso con l'indicazione "Esercitazione di prontezza". Nella pagina dei dettagli degli avvisi viene visualizzato un elenco degli avvisi di incidente.



3. Esaminare gli incidenti di allerta.
4. Seleziona un incidente di allerta.



Ecco alcune cose da tenere a mente:

- Osserva la potenziale gravità dell'attacco.

  Se la gravità indica che un utente è sospettato di attività dannose, rivedere il nome utente. Puoi anche"bloccare l'utente."

- Esaminare l'attività del file e i processi sospetti:
  - Confrontare i dati rilevati in arrivo con i dati previsti.
  - Confronta la velocità di creazione dei file rilevata con quella prevista.
  - Confronta la frequenza di rinominazione dei file rilevata con quella prevista.
  - Osserva il tasso di eliminazione rispetto al tasso previsto.
- Guarda l'elenco dei file interessati. Esamina le estensioni che potrebbero causare l'attacco.
- Determinare l'impatto e l'ampiezza dell'attacco esaminando il numero di file e directory interessati.

Ripristinare il carico di lavoro del test

Dopo aver esaminato l'avviso di esercitazione di preparazione, ripristinare il carico di lavoro del test, se necessario.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Torna alla pagina dei dettagli dell'avviso.
2. Se il carico di lavoro del test deve essere ripristinato, procedere come segue:
   - Seleziona **Segna come ripristino necessario**.
   - Rivedi la conferma e seleziona **Segna come ripristino necessario** nella casella di conferma.
     - Dal menu Ransomware Resilience, seleziona **Ripristino**.
     - Selezionare il carico di lavoro di prova contrassegnato con "Esercitazione di preparazione" che si desidera ripristinare.
     - Selezionare **Ripristina**.
     - Nella pagina Ripristina, fornisci le informazioni per il ripristino:
   - Selezionare la copia dello snapshot di origine.
   - Selezionare il volume di destinazione.
3. Nella pagina di revisione del ripristino, seleziona **Ripristina**.

   La Console visualizza lo stato del ripristino del drill di prontezza come "In corso" nella pagina Ripristino.

   Una volta completato il ripristino, la Console modifica lo stato del carico di lavoro in **Ripristinato**.

4. Esaminare il carico di lavoro ripristinato.

Per i dettagli sul processo di ripristino, vedere"Recuperare da un attacco ransomware (dopo che gli incidenti sono stati neutralizzati)" .

Modificare lo stato degli avvisi dopo l'esercitazione di preparazione

Dopo aver esaminato l'avviso di esercitazione di prontezza e aver ripristinato il carico di lavoro, modificare lo stato dell'avviso, se necessario.

È richiesto il ruolo Console Amministratore dell'organizzazione, Amministratore di cartelle o progetti o Amministratore di Ransomware Resilience. "Scopri di più sui ruoli di accesso alla console per tutti i servizi" .

Passi

1. Torna alla pagina dei dettagli dell'avviso.
2. Selezionare nuovamente l'avviso.
3. Indicare lo stato selezionando **Modifica stato** e cambiare lo stato in uno dei seguenti:
   - Ignorato: se sospetti che l'attività non sia un attacco ransomware, modifica lo stato in Ignorato.

     Dopo aver respinto un attacco, non è possibile ripristinarlo. Se si ignora un carico di lavoro, tutte le copie snapshot eseguite automaticamente in risposta al potenziale attacco ransomware verranno eliminate definitivamente. Se si ignora l'avviso, l'esercitazione di preparazione è considerata completata.

   - Risolto: l'incidente è stato mitigato.

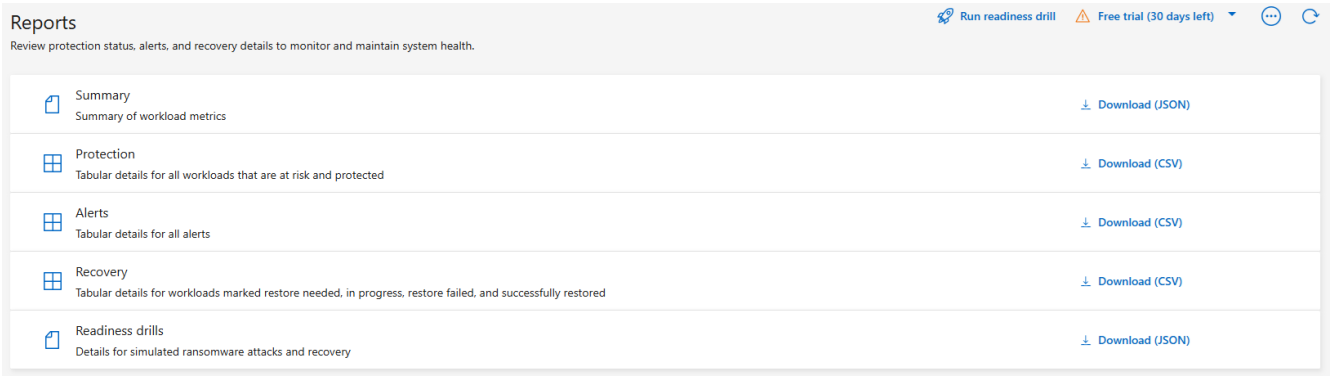
Rivedere i rapporti sull'esercitazione di preparazione

Una volta completata l'esercitazione di preparazione, potresti voler rivedere e salvare un report sull'esercitazione.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Dal menu Ransomware Resilience, seleziona **Report**.



2. Selezionare **Esercitazioni di preparazione** e **Scarica** per scaricare il report delle esercitazioni di preparazione.

Collega NetApp Ransomware Resilience al sistema di gestione della sicurezza e degli eventi (SIEM) per l'analisi e il rilevamento delle minacce

Un sistema di gestione della sicurezza e degli eventi (SIEM) centralizza i dati di log ed eventi per fornire informazioni sugli eventi di sicurezza e sulla conformità. NetApp Ransomware Resilience supporta l'invio automatico dei dati al SIEM per semplificare l'analisi e il rilevamento delle minacce.

Ransomware Resilience supporta i seguenti SIEM:

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

Prima di abilitare SIEM in Ransomware Resilience, è necessario configurare il sistema SIEM.

Dati evento inviati a un SIEM

Ransomware Resilience può inviare i seguenti dati sugli eventi al tuo sistema SIEM:

- **contesto**:
  - **os**: Questa è una costante con il valore di ONTAP.
  - **os_version**: la versione di ONTAP in esecuzione sul sistema.
  - **connector_id**: ID dell'agente della console che gestisce il sistema.
  - **cluster_id**: ID del cluster segnalato da ONTAP per il sistema.

- **svm_name**: Nome dell'SVM in cui è stato trovato l'avviso.
- **volume_name**: Nome del volume su cui si trova l'avviso.
- **volume_id**: ID del volume segnalato da ONTAP per il sistema.

- **incidente**:
  - **incident_id**: ID incidente generato da Ransomware Resilience per il volume sottoposto ad attacco in Ransomware Resilience.
  - **alert_id**: ID generato da Ransomware Resilience per il carico di lavoro.
  - **gravità**: Uno dei seguenti livelli di allerta: "CRITICO", "ALTO", "MEDIO", "BASSO".
  - **descrizione**: Dettagli sull'avviso rilevato, ad esempio "Un potenziale attacco ransomware rilevato sul carico di lavoro arp_learning_mode_test_2630"

Configurare AWS Security Hub per il rilevamento delle minacce

Prima di abilitare AWS Security Hub in Ransomware Resilience, è necessario eseguire i seguenti passaggi di alto livello in AWS Security Hub:

- Imposta le autorizzazioni in AWS Security Hub.
- Imposta la chiave di accesso all'autenticazione e la chiave segreta in AWS Security Hub. (Questi passaggi non sono forniti qui.)

Passaggi per impostare le autorizzazioni in AWS Security Hub

1. Vai alla **console AWS IAM**.
2. Selezionare **Politiche**.
3. Crea una policy utilizzando il seguente codice in formato JSON:

```
{
  "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"
      ]
    }
  ]
}
```

Configurare Microsoft Sentinel per il rilevamento delle minacce

Prima di abilitare Microsoft Sentinel in Ransomware Resilience, è necessario eseguire i seguenti passaggi di alto livello in Microsoft Sentinel:

- **Prerequisiti**
  - Abilita Microsoft Sentinel.
  - Crea un ruolo personalizzato in Microsoft Sentinel.
- **Registrazione**
  - Registra Ransomware Resilience per ricevere eventi da Microsoft Sentinel.
  - Crea un segreto per la registrazione.
- **Autorizzazioni**: assegna le autorizzazioni all'applicazione.
- **Autenticazione**: immettere le credenziali di autenticazione per l'applicazione.

Passaggi per abilitare Microsoft Sentinel

1. Vai a Microsoft Sentinel.
2. Creare un'**area di lavoro di Log Analytics**.
3. Abilita Microsoft Sentinel per utilizzare l'area di lavoro Log Analytics appena creata.

Passaggi per creare un ruolo personalizzato in Microsoft Sentinel

1. Vai a Microsoft Sentinel.
2. Selezionare **Abbonamento** > **Controllo accessi (IAM)**.
3. Inserisci un nome di ruolo personalizzato. Utilizzare il nome **Ransomware Resilience Sentinel Configurator**.
4. Copia il seguente JSON e incollalo nella scheda **JSON**.

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

  ]
}
```

5. Rivedi e salva le tue impostazioni.

Passaggi per registrare Ransomware Resilience per ricevere eventi da Microsoft Sentinel

1. Vai a Microsoft Sentinel.
2. Selezionare **Entra ID** > **Applicazioni** > **Registrazioni app**.
3. Per il **Nome visualizzato** dell'applicazione, immettere "**Ransomware Resilience**".
4. Nel campo **Tipo di account supportato**, seleziona **Solo account in questa directory organizzativa**.
5. Selezionare un **Indice predefinito** in cui verranno inviati gli eventi.

6. Seleziona **Recensione**.
7. Seleziona **Registra** per salvare le tue impostazioni.

   Dopo la registrazione, l'interfaccia di amministrazione di Microsoft Entra visualizza il riquadro Panoramica dell'applicazione.

Passaggi per creare un segreto per la registrazione

1. Vai a Microsoft Sentinel.
2. Selezionare **Certificati e segreti** > **Segreti client** > **Nuovo segreto client**.
3. Aggiungi una descrizione per il segreto della tua applicazione.
4. Seleziona una **Scadenza** per il segreto oppure specifica una durata personalizzata.

   La durata del segreto del cliente è limitata a due anni (24 mesi) o meno. Microsoft consiglia di impostare un valore di scadenza inferiore a 12 mesi.

5. Seleziona **Aggiungi** per creare il tuo segreto.
6. Registrare il segreto da utilizzare nella fase di autenticazione. Una volta che avrai abbandonato questa pagina, il segreto non verrà più visualizzato.

Passaggi per assegnare le autorizzazioni all'applicazione

1. Vai a Microsoft Sentinel.
2. Selezionare **Abbonamento** > **Controllo accessi (IAM)**.
3. Selezionare **Aggiungi** > **Aggiungi assegnazione ruolo**.
4. Per il campo **Ruoli di amministratore privilegiato**, selezionare **Ransomware Resilience Sentinel Configurator**.

   Questo è il ruolo personalizzato che hai creato in precedenza.

5. Selezionare **Avanti**.
6. Nel campo **Assegna accesso a**, seleziona **Utente, gruppo o entità servizio**.
7. Seleziona **Seleziona membri**. Quindi, seleziona **Ransomware Resilience Sentinel Configurator**.
8. Selezionare **Avanti**.
9. Nel campo **Cosa può fare l'utente**, seleziona **Consenti all'utente di assegnare tutti i ruoli eccetto i ruoli di amministratore con privilegi Proprietario, UAA, RBAC (consigliato)**.
10. Selezionare **Avanti**.
11. Selezionare **Rivedi e assegna** per assegnare le autorizzazioni.

Passaggi per immettere le credenziali di autenticazione per l'applicazione

1. Vai a Microsoft Sentinel.
2. Inserisci le credenziali:
   a. Immettere l'ID tenant, l'ID applicazione client e il segreto dell'applicazione client.
   b. Seleziona **Authenticate**.

   Una volta completata l'autenticazione, verrà visualizzato il messaggio "Autenticato".

3. Immettere i dettagli dell'area di lavoro di Log Analytics per l'applicazione.
    a. Selezionare l'ID dell'abbonamento, il gruppo di risorse e l'area di lavoro Log Analytics.

Configurare Splunk Cloud per il rilevamento delle minacce

Prima di abilitare Splunk Cloud in Ransomware Resilience, è necessario eseguire i seguenti passaggi generali in Splunk Cloud:

- Abilita un HTTP Event Collector in Splunk Cloud per ricevere dati sugli eventi tramite HTTP o HTTPS dalla Console.
- Crea un token Event Collector in Splunk Cloud.

Passaggi per abilitare un HTTP Event Collector in Splunk

1. Vai a Splunk Cloud.
2. Selezionare **Impostazioni** > **Inserimento dati**.
3. Selezionare **HTTP Event Collector** > **Impostazioni globali**.
4. Nel menu a discesa Tutti i token, seleziona **Abilitato**.
5. Per fare in modo che Event Collector ascolti e comunichi tramite HTTPS anziché HTTP, selezionare **Abilita SSL**.
6. Immettere una porta in **Numero porta HTTP** per HTTP Event Collector.

Passaggi per creare un token Event Collector in Splunk

1. Vai a Splunk Cloud.
2. Selezionare **Impostazioni** > **Aggiungi dati**.
3. Selezionare **Monitor** > **HTTP Event Collector**.
4. Inserisci un nome per il token e seleziona **Avanti**.
5. Selezionare un **Indice predefinito** in cui verranno inviati gli eventi, quindi selezionare **Revisiona**.
6. Verificare che tutte le impostazioni per l'endpoint siano corrette, quindi selezionare **Invia**.
7. Copia il token e incollalo in un altro documento per averlo pronto per la fase di autenticazione.

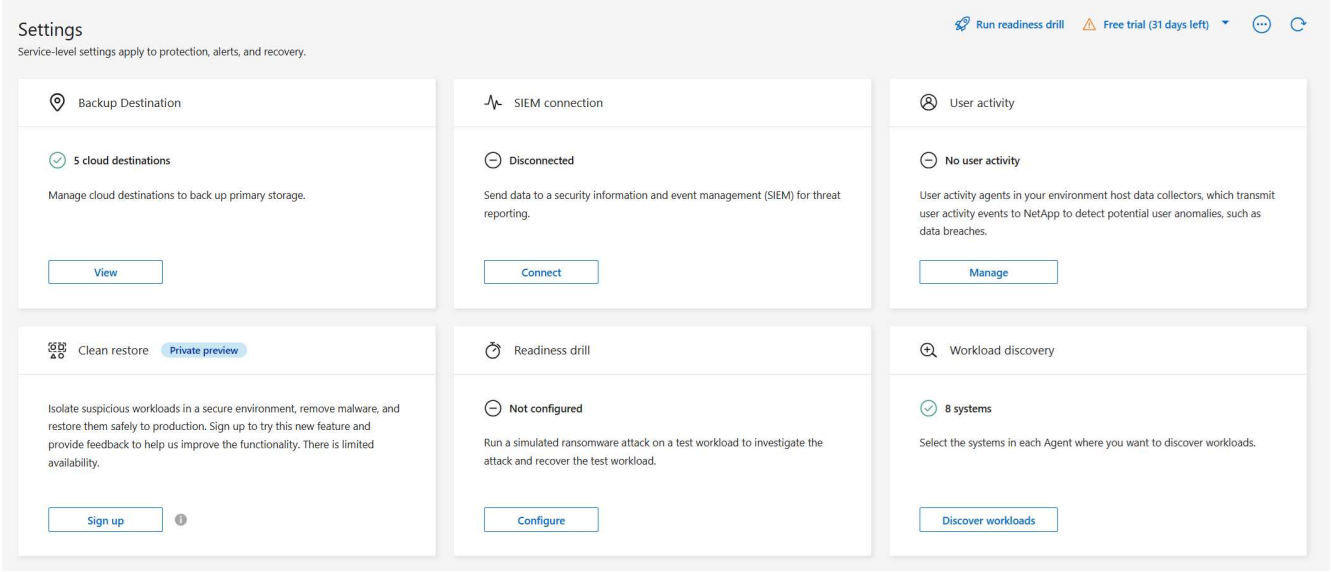
Connetti SIEM alla resilienza del ransomware

Abilitando SIEM, i dati da Ransomware Resilience vengono inviati al server SIEM per l'analisi e la segnalazione delle minacce.

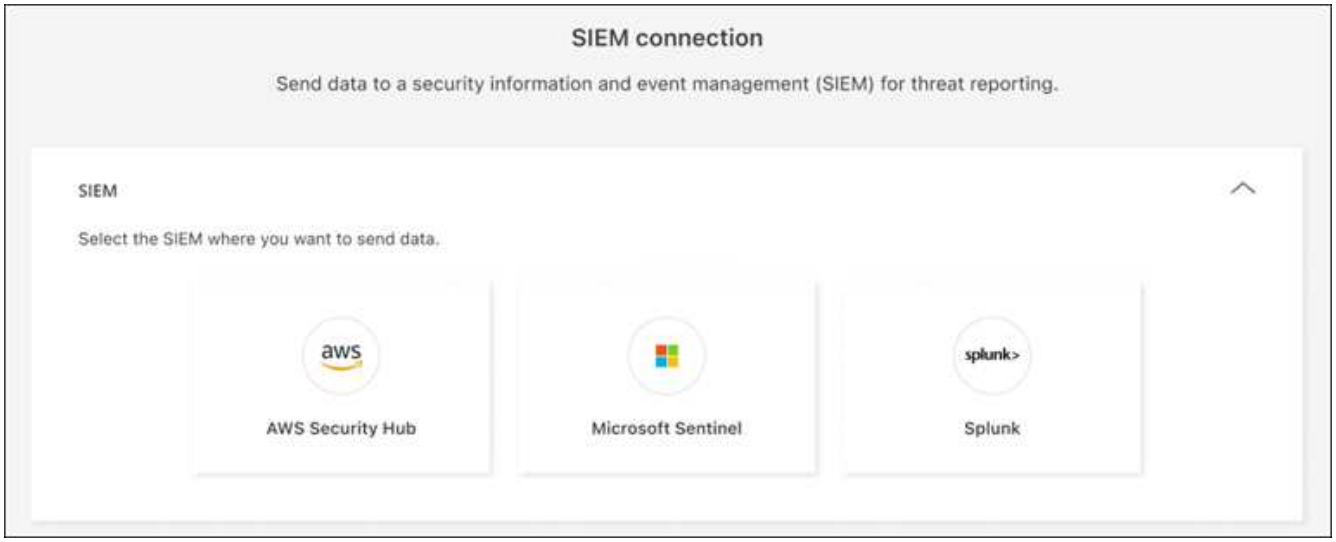
Passi

1. Dal menu Console, seleziona **Protezione** > **Ransomware Resilience**.
2. Dal menu Ransomware Resilience, seleziona la verticale … opzione in alto a destra.
3. Selezionare **Impostazioni**.

    Viene visualizzata la pagina Impostazioni.



4. Nella pagina Impostazioni, seleziona **Connetti** nel riquadro Connessione SIEM.



5. Scegli uno dei sistemi SIEM.
6. Inserisci il token e i dettagli di autenticazione configurati in AWS Security Hub o Splunk Cloud.

   Le informazioni da immettere dipendono dal SIEM selezionato.

7. Selezionare **Abilita**.

   Nella pagina Impostazioni viene visualizzato "Connesso".

Scarica i report in NetApp Ransomware Resilience

NetApp Ransomware Resilience fornisce report in formato CSV e JSON che mostrano i dettagli dei volumi supportati e non supportati, esercitazioni di preparazione agli attacchi, protezione, avvisi e ripristino. Con i report, puoi salvare e rivedere offline report su esercitazioni, stato di protezione, avvisi ed eventi di ripristino.

Prima di scaricare i file, aggiorna la dashboard per acquisire i dati più recenti nei tuoi report.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Quali dati puoi scaricare? È possibile scaricare i file da una qualsiasi delle opzioni del menu principale:

- **Riepilogo**: include elenchi di carichi di lavoro supportati e non supportati, azioni consigliate per migliorare la tua postura di resilienza informatica e informazioni acquisite nella dashboard Ransomware Resilience.
- **Protezione**: include lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale di quelli protetti e a rischio.
- **Avvisi**: include lo stato e i dettagli di tutti gli avvisi, tra cui il numero totale di avvisi e snapshot automatici.
- **Ripristino**: include lo stato e i dettagli di tutti i carichi di lavoro che devono essere ripristinati, incluso il numero totale di carichi di lavoro contrassegnati come "Ripristino necessario", "In corso", "Ripristino non riuscito" e "Ripristino riuscito".
- **Report**: puoi esportare i dati da qualsiasi pagina e scaricare i file.

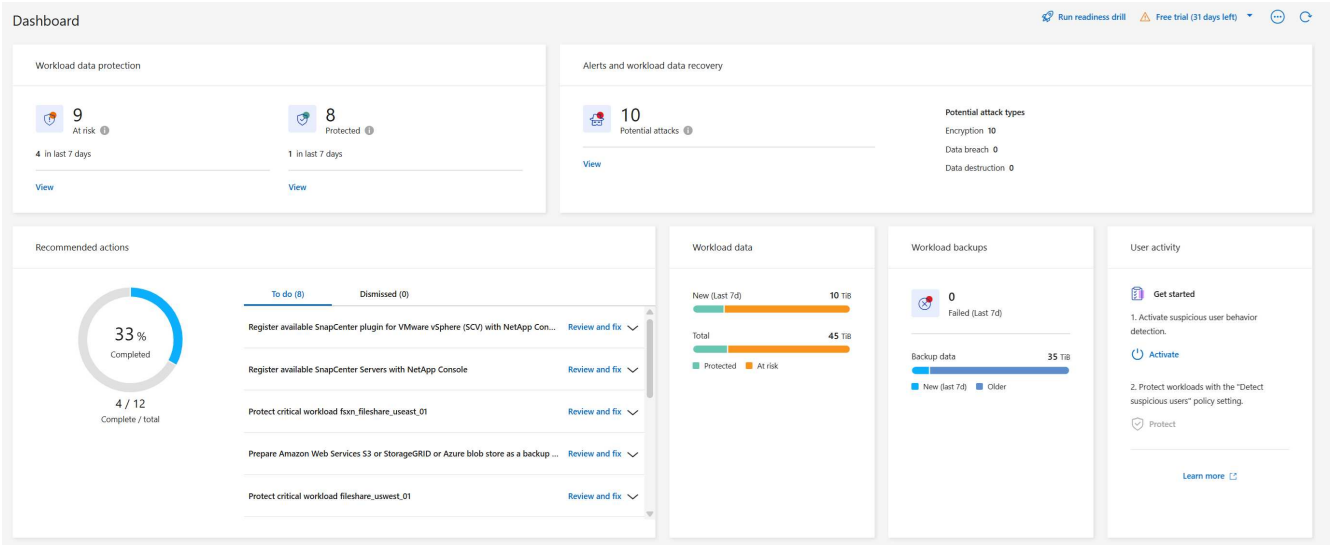
  È possibile scaricare i report delle esercitazioni di preparazione solo dalla pagina **Report**.

Se scarichi file CSV o JSON dalla pagina Protezione, Avvisi o Ripristino, i dati mostrano solo i dati presenti in quella pagina.

I file CSV o JSON includono dati per tutti i carichi di lavoro su tutti i sistemi Console.

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.

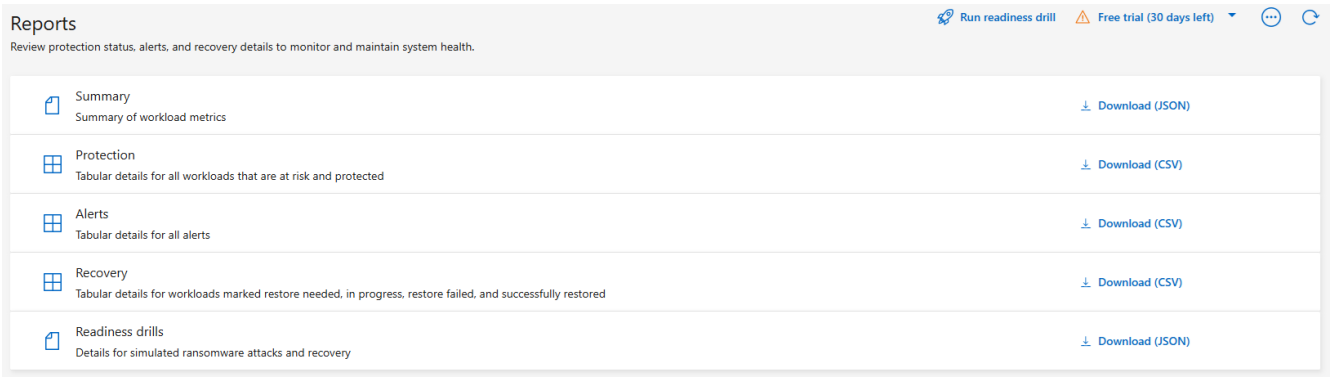


2. Dalla dashboard o da un'altra pagina, seleziona l'opzione **Aggiorna** in alto a destra per aggiornare i dati che verranno visualizzati nei report.
3. Eseguire una delle seguenti operazioni:
   -

Dalla pagina, seleziona *Download* opzione.

- Dal menu NetApp Ransomware Resilience , seleziona **Report**.

4. Se hai selezionato l'opzione **Report**, seleziona uno dei nomi di file preconfigurati e seleziona **Scarica**.



Informazioni sul copyright

Informazioni sul marchio commerciale