Utilizzare la protezione ransomware BlueXP

BlueXP ransomware protection

NetApp
October 07, 2024

This PDF was generated from https://docs.netapp.com/it-it/bluexp-ransomware-protection/rp-use-overview.html on October 07, 2024. Always check docs.netapp.com for the latest.

Sommario

Utilizzare la protezione ransomware BlueXP . . . 1
Utilizzare la protezione ransomware BlueXP . . . 1
Visualizza lo stato dei carichi di lavoro con un’occhiata utilizzando la dashboard . . . 1
Proteggere i carichi di lavoro . . . 6
Rispondi a un avviso ransomware rilevato . . . 22
Ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti) . . . 27
Scarica i report . . . 37

Utilizzare la protezione ransomware BlueXP

Utilizzare la protezione ransomware BlueXP

Utilizzando la protezione dal ransomware di BlueXP, puoi visualizzare la salute dei carichi di lavoro e proteggere i carichi di lavoro.

- "Rileva i carichi di lavoro nella protezione dal ransomware di BlueXP".
- "Visualizza protezione e salute del workload dalla Dashboard".
  - Esaminare e agire in base ai consigli sulla protezione dal ransomware.
- "Proteggere i carichi di lavoro":
  - Assegna una strategia di protezione dal ransomware ai carichi di lavoro.
  - Aumentare la protezione delle applicazioni per prevenire futuri attacchi ransomware.
  - Creare, modificare o eliminare una strategia di protezione.
- "Rispondi al rilevamento di potenziali attacchi ransomware".
- "Ripristino in seguito a un attacco" (dopo che gli incidenti sono neutralizzati).
- "Configurare le impostazioni di protezione".

Visualizza lo stato dei carichi di lavoro con un'occhiata utilizzando la dashboard

La dashboard per la protezione dal ransomware di BlueXP fornisce informazioni immediate sulla salute della protezione dei workload. Puoi determinare rapidamente i workload a rischio o protetti, identificare i workload che ne sono influenzati da un incidente o nel recovery e misurare il grado di protezione tenendo conto della quantità di storage protetto o a rischio.

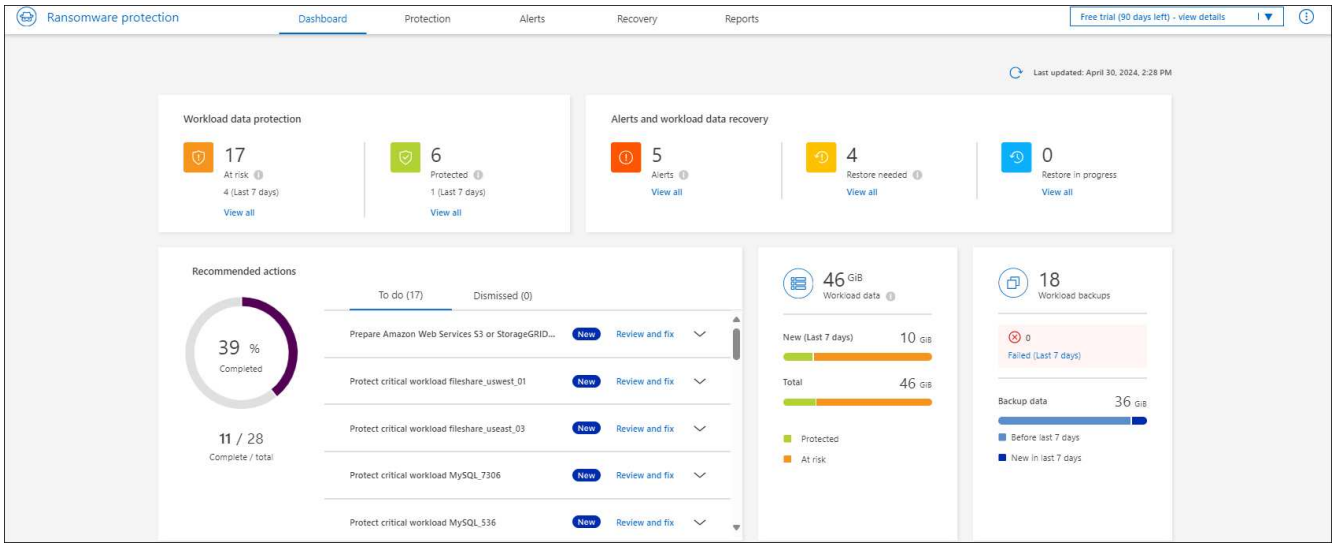
Puoi anche utilizzare la dashboard per esaminare e agire in base ai consigli sulla protezione, accedere alle impostazioni globali, scaricare i report e accedere a questa documentazione tecnica.

Esaminare lo stato dei carichi di lavoro utilizzando la dashboard

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

   Dopo il rilevamento, la Dashboard mostra la salute della data Protection dei carichi di lavoro.



2. Dal Dashboard, è possibile eseguire le seguenti azioni in ciascuno dei riquadri:

   - **Protezione dei dati del carico di lavoro**: Fare clic su **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".

     > Fare clic sulla nota i per visualizzare i suggerimenti su questi dati. Per aumentare il limite del carico di lavoro, fare clic su **aumenta limite carico di lavoro** all'interno di questa nota. Facendo clic su questo pulsante si accede alla pagina di supporto BlueXP , in cui è possibile creare un ticket per il caso.

   - **Avvisi e recupero dati del carico di lavoro**: Fare clic su **Visualizza tutto** per visualizzare gli incidenti attivi che hanno influito sul carico di lavoro, sono pronti per il ripristino dopo che gli incidenti sono stati neutralizzati o sono in fase di recupero. Fare riferimento a. "Rispondere a un avviso rilevato".
     - Un incidente è classificato in uno dei seguenti stati:
       - Novità
       - Respinto
       - Scomparire
       - Risolto
     - Un avviso può avere uno dei seguenti stati:
       - Novità
       - Inattivo
     - Un carico di lavoro può avere uno dei seguenti stati di ripristino:
       - Ripristino necessario
       - In corso
       - Ripristinato
       - Non riuscito
   - **Azioni consigliate**: Per aumentare la protezione, rivedere ogni raccomandazione e fare clic su **Rivedi e correggi**.

Fare riferimento a. "Rivedere i consigli sulla protezione sulla dashboard" oppure "Proteggere i carichi di lavoro".

Tutti i suggerimenti aggiunti dall'ultima volta che si è visitato il Dashboard sono indicati con "nuovo" per almeno 24 ore. Le azioni sono elencate in ordine di priorità, con le più importanti in alto. È possibile rivedere e agire su ciascuno di essi o eliminarlo.

Il numero totale di azioni non include le azioni respinte.

- **Dati del carico di lavoro**: Monitoraggio delle modifiche apportate alla copertura di protezione negli ultimi 7 giorni.
- **Backup del carico di lavoro**: Monitoraggio delle modifiche apportate ai backup dei carichi di lavoro creati dal servizio che non sono riusciti o sono stati completati correttamente negli ultimi 7 giorni.

Rivedere i consigli sulla protezione sulla dashboard

La protezione dal ransomware di BlueXP valuta la protezione sui carichi di lavoro e raccomanda azioni per migliorare tale protezione.

È possibile rivedere un suggerimento e agire su di esso, che cambia lo stato del suggerimento in completo. Oppure, se si desidera agire in seguito, è possibile eliminarlo. L'annullamento di un'azione sposta il suggerimento in un elenco di azioni respinte, che è possibile rivedere in un secondo momento.

Ecco un esempio delle raccomandazioni che il servizio offre.

Consiglio	Descrizione	Come risolvere il problema
Aggiungi una policy di protezione dal ransomware.	Il carico di lavoro non è attualmente protetto.	Assegnare una policy al carico di lavoro. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Connettersi a SEIM per la segnalazione delle minacce.	Inviare dati a un sistema di gestione degli eventi e della sicurezza (SIEM) per l'analisi e il rilevamento delle minacce.	Immettere i dettagli del server SIEM/XDR per abilitare il rilevamento delle minacce. Fare riferimento alla "Configurare le impostazioni di protezione".
Abilita una protezione coerente del carico di lavoro per applicazioni o VMware.	Questi workload non vengono gestiti dal software SnapCenter o dal plug-in SnapCenter per VMware vSphere.	Per farle gestire da SnapCenter, abilita una protezione coerente con il carico di lavoro. Fare riferimento a. "Proteggere il carico di lavoro dagli attacchi ransomware".
Migliora la postura di sicurezza per l'ambiente di lavoro	Il consulente digitale NetApp ha identificato almeno un rischio di protezione elevato o critico.	Esaminate tutti i rischi per la sicurezza in NetApp Digital Advisor. Fare riferimento alla "Documentazione di Digital Advisor".

Consiglio	Descrizione	Come risolvere il problema
Rafforzare una politica.	Alcuni carichi di lavoro potrebbero non disporre di una protezione sufficiente. Rafforza la protezione sui carichi di lavoro con una policy.	Aumenta la conservazione, Aggiungi i backup, applica i backup immutabili, blocca le estensioni di file sospette, abilita il rilevamento sullo storage secondario e molto altro ancora. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Preparare <backup provider> come destinazione di backup per eseguire il backup dei dati del workload.	Il workload non dispone al momento di destinazioni di backup.	Aggiungete destinazioni di backup a questo workload per proteggerlo. Fare riferimento alla "Configurare le impostazioni di protezione".
Proteggi i workload dell'applicazione critici o altamente importanti dal ransomware.	La pagina protezione visualizza i carichi di lavoro dell'applicazione critici o altamente importanti (in base al livello di priorità assegnato) che non sono protetti.	Assegnare una policy a questi carichi di lavoro. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Proteggi i carichi di lavoro di condivisione file, critici o altamente importanti, dal ransomware.	La pagina protezione visualizza i carichi di lavoro critici o molto importanti del tipo file Share o DataStore non protetti.	Assegnazione di una policy a ciascun carico di lavoro. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Registra il plug-in SnapCenter disponibile per VMware vSphere (SCV) con BlueXP	Un carico di lavoro VM non è protetto.	Assegna una protezione coerente con le VM al carico di lavoro delle VM abilitando il plug-in SnapCenter per VMware vSphere. Fare riferimento alla "Proteggi i carichi di lavoro dagli attacchi ransomware".
Registra i server SnapCenter disponibili con BlueXP	Un'applicazione non è protetta.	Assegna una protezione coerente con l'applicazione al carico di lavoro attivando il server SnapCenter. Fare riferimento alla "Proteggi i carichi di lavoro dagli attacchi ransomware".
Rivedere i nuovi avvisi.	Esistono nuovi avvisi.	Rivedere i nuovi avvisi. Fare riferimento a. "Rispondi a un avviso ransomware rilevato".

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Dal riquadro azioni consigliate, selezionare un suggerimento e selezionare **Rivedi e correggi**.
3. Per chiudere l'azione in un secondo momento, selezionare **Chiudi**.

   Il suggerimento scompare dall'elenco delle attività e viene visualizzato nell'elenco delle attività respinte.

È possibile modificare in un secondo momento un elemento da liquidare in un elemento da fare. Quando si contrassegna un elemento completato o si modifica un elemento respinto in un'azione attività, le azioni totale aumentano di 1.

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

Esportare i dati di protezione in file CSV

È possibile esportare dati e scaricare file CSV che mostrano i dettagli relativi alla protezione, agli avvisi e al ripristino.

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

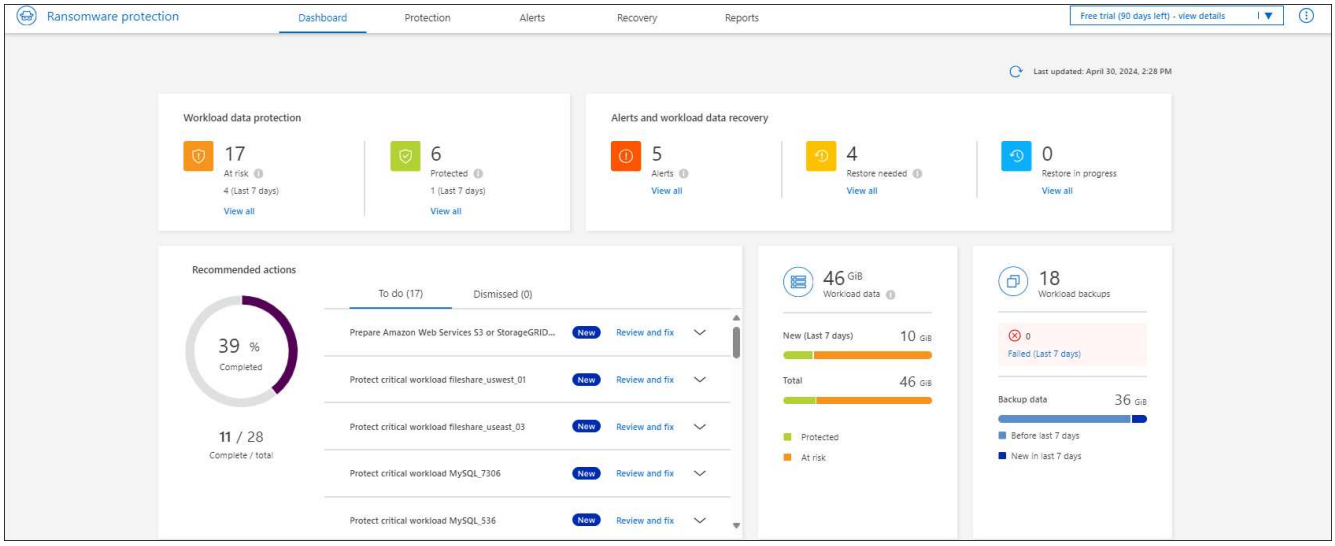
- **Protezione**: Contiene lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale protetto e a rischio.
- **Avvisi**: Include lo stato e i dettagli di tutti gli avvisi, compreso il numero totale di avvisi e istantanee automatiche.
- **Recovery**: Include lo stato e i dettagli di 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 "ripristinato correttamente".

Se si scaricano file CSV dalla pagina protezione, Avvisi o Ripristino, solo i dati contenuti in tale pagina vengono inclusi nel file CSV.

I file CSV includono i dati per tutti i carichi di lavoro su tutti gli ambienti di lavoro BlueXP.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.



2. Nella pagina, selezionare l'opzione **Aggiorna** in alto a destra per aggiornare i dati che verranno visualizzati nei file.
3. Effettuare una delle seguenti operazioni:
   - Nella pagina, selezionare l'opzione **Download** .

- Dal menu di protezione dal ransomware di BlueXP, seleziona **Report**.

4. Se è stata selezionata l'opzione **rapporti**, selezionare uno dei file preconfigurati e selezionare **Download (CSV)** o **Download (JSON)**.

Accedere alla documentazione tecnica

Puoi accedere a questa documentazione tecnica da docs.netapp.com o dall'interno del servizio di protezione dal ransomware BlueXP.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Dal dashboard, selezionare le **azioni** verticali opzione.
3. Selezionare una delle seguenti opzioni:
   - **Novità** per visualizzare le informazioni sulle funzioni delle versioni correnti o precedenti nelle Note di rilascio.
   - **Documentazione** per visualizzare la home page della documentazione relativa alla protezione dal ransomware BlueXP e questa documentazione.

Proteggere i carichi di lavoro

Proteggi i carichi di lavoro con le strategie ransomware

Puoi proteggere i workload dagli attacchi ransomware eseguendo le seguenti azioni utilizzando la protezione dal ransomware di BlueXP.

- Abilita una protezione coerente con il carico di lavoro, che funziona con il software SnapCenter o il plug-in SnapCenter per VMware vSphere.
- Crea o gestisci strategie di protezione dal ransomware, che includono policy create per snapshot, backup e protezione dal ransomware (note come *policy di rilevamento*).
- Importare una strategia e regolarla.
- Raggruppare le condivisioni dei file per semplificare la protezione dei carichi di lavoro piuttosto che proteggerli individualmente.
- Elimina una strategia di protezione dal ransomware.

Quali servizi sono utilizzati per la protezione? Per gestire i criteri di protezione è possibile utilizzare i seguenti servizi. Le informazioni di protezione provenienti da questi servizi vengono visualizzate nella protezione ransomware di BlueXP :

- Backup e recovery BlueXP per condivisioni file e file VM
- SnapCenter per VMware per datastore VM
- SnapCenter per Oracle e MySQL

Policy di protezione

Potrebbe essere utile esaminare le informazioni sui criteri di protezione che è possibile modificare e i tipi di criteri contenuti in una strategia di protezione.

Quali criteri di protezione potete modificare?

Puoi modificare le policy di protezione in base alla protezione dei workload di cui disponi:

- **Workload non protetti dalle applicazioni NetApp**: Questi workload non sono gestiti da backup e ripristino SnapCenter, SnapCenter Plug-in per VMware vSphere o BlueXP . Questi carichi di lavoro potrebbero avere snapshot creati come parte di ONTAP o di altri prodotti. Se è attiva la protezione FPolicy di ONTAP, è possibile modificare la protezione FPolicy utilizzando ONTAP.
- **Workload con protezione esistente da parte delle applicazioni NetApp**: Questi workload dispongono di policy di backup o snapshot gestite da SnapCenter, SnapCenter per VMware vSphere o backup e ripristino BlueXP .
  - Se le policy di backup o snapshot vengono gestite da backup e ripristino SnapCenter, SnapCenter per VMware o BlueXP , queste applicazioni continueranno a essere gestite da esse. Utilizzando la protezione dal ransomware di BlueXP , puoi anche applicare una policy di rilevamento del ransomware a questi carichi di lavoro.
  - Se una policy di rilevamento del ransomware viene gestita da protezione autonoma dal ransomware (ARP) e FPolicy in ONTAP, quei workload sono protetti e continueranno a essere gestiti da ARP e FPolicy.

Quali policy sono richieste in una strategia di protezione dal ransomware?

Nella strategia di protezione dal ransomware sono richieste le seguenti policy:

- Policy di rilevamento del ransomware
- Policy di Snapshot

Nella strategia di protezione dal ransomware BlueXP non è necessaria una policy di backup.

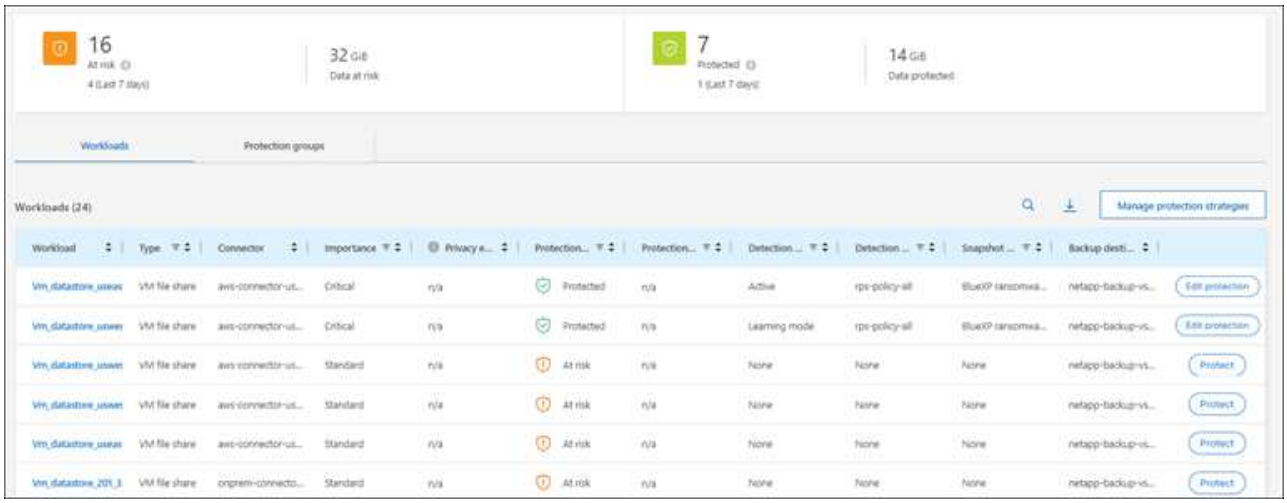
Visualizza la protezione dal ransomware su un carico di lavoro

Uno dei primi passi nella protezione dei carichi di lavoro è la visualizzazione dei carichi di lavoro attuali e del loro stato di protezione. Sono visualizzabili i seguenti tipi di carichi di lavoro:

- Workload delle applicazioni
- Workload VM
- Workload di condivisione di file

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Effettuare una delle seguenti operazioni:
   - Nel riquadro protezione dati del dashboard, selezionare **Visualizza tutto**.
   - Dal menu, selezionare **protezione**.



3. Da questa pagina è possibile visualizzare e modificare i dettagli relativi alla protezione del carico di lavoro.

> Per i workload che hanno già una policy di protezione con il servizio di backup e recovery di SnapCenter o BlueXP, non puoi modificare la data Protection. Per questi workload, il ransomware BlueXP abilita la protezione autonoma dal ransomware e/o la protezione FPolicy, se sono già attivati in altri servizi. Ulteriori informazioni su "Protezione ransomware autonoma", "Backup e ripristino BlueXP"e "FPolicy di ONTAP".

Dettagli sulla protezione nella pagina protezione

La pagina protezione mostra le seguenti informazioni sulla protezione del carico di lavoro:

Stato di protezione: Un carico di lavoro può mostrare uno dei seguenti stati di protezione per indicare se un criterio è applicato o meno:

- **Protetto**: Viene applicato un criterio. ARP 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 una policy di rilevamento primaria abilitata, è "a rischio" anche se ha una policy di backup e snapshot attivate.
- **In corso**: È in corso l'applicazione di un criterio, ma non è ancora stato completato.
- **Non riuscito**: Un criterio è applicato ma non funziona.

Stato di rilevamento: Un carico di lavoro può avere uno dei seguenti stati di rilevamento ransomware:

- **Apprendimento**: Al carico di lavoro è stata recentemente assegnata una policy di rilevamento del ransomware e il servizio sta analizzando i workload.
- **Attivo**: Viene assegnato un criterio di protezione dal rilevamento ransomware.
- **Non impostato**: Non è stata assegnata una policy di protezione dal rilevamento ransomware.
- **Errore**: È stata assegnata una policy di rilevamento ransomware, ma il servizio ha riscontrato un errore.

> Quando la protezione è abilitata nella protezione ransomware BlueXP , il rilevamento di avvisi e il reporting iniziano dopo che lo stato della policy di rilevamento del ransomware passa dalla modalità di apprendimento alla modalità attiva.

Criterio di rilevamento: Viene visualizzato il nome del criterio di rilevamento ransomware, se ne è stato assegnato uno. Se il criterio di rilevamento non è stato assegnato, viene visualizzato "N/A".

Criteri di snapshot e backup: In questa colonna vengono visualizzati i criteri di snapshot e backup applicati al carico di lavoro e al prodotto o servizio che gestisce tali criteri.

- Gestito da SnapCenter
- Gestito dal plug-in SnapCenter per VMware vSphere
- Gestito da backup e recovery di BlueXP
- Nome della policy di protezione ransomware che gestisce snapshot e backup
- Nessuno

Importanza del carico di lavoro

La protezione dal ransomware di BlueXP assegna un'importanza o una priorità a ogni workload durante il rilevamento, in base a un'analisi di ogni workload. L'importanza del carico di lavoro è determinata dalle seguenti frequenze di snapshot:

- **Critico**: Le copie snapshot sono acquisite più di 1 TB all'ora (programma di protezione altamente aggressivo)
- **Importante**: Le copie snapshot sono state acquisite meno di 1 TB all'ora ma più di 1 TB al giorno
- **Standard**: Le copie snapshot sono state acquisite più di 1 copie al giorno

Criteri di rilevamento predefiniti

Puoi scegliere una delle seguenti policy predefinite di protezione dal ransomware BlueXP , allineate con l'importanza dei carichi di lavoro:

Livello dei criteri	Snapshot	Frequenza	Conservazione (giorni)	n. di copie snapshot	Numero massimo totale di copie snapshot
Politica critica dei carichi di lavoro	Quarto ogni ora	Ogni 15 minuti	3	288	309
	Ogni giorno	Ogni 1 giorni	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni	60	2	309
Policy importante sui carichi di lavoro	Quarto ogni ora	Ogni 30 minuti	3	144	165
	Ogni giorno	Ogni 1 giorni	14	14	165
	Settimanale	Ogni 1 settimana	35	5	165
	Mensile	Ogni 30 giorni	60	2	165

Livello dei criteri	Snapshot	Frequenza	Conservazione (giorni)	n. di copie snapshot	Numero massimo totale di copie snapshot
Norma sui carichi di lavoro standard	Quarto ogni ora	Ogni 30 minuti	3	72	93
	Ogni giorno	Ogni 1 giorni	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93

Abilita una protezione coerente con applicazioni o VM con SnapCenter

L'attivazione della protezione coerente con le applicazioni o le VM consente di proteggere le applicazioni o i carichi di lavoro delle VM in modo coerente, raggiungendo uno stato di inattività e coerente per evitare potenziali perdite di dati successivamente se il ripristino è necessario.

Questo processo avvia la registrazione del server software SnapCenter per le applicazioni o del plug-in SnapCenter per VMware vSphere per le VM utilizzando il backup e il ripristino BlueXP.

Una volta abilitata una protezione coerente con il carico di lavoro, puoi gestire le strategie di protezione nella protezione dal ransomware di BlueXP. La strategia di protezione include le policy di backup e snapshot gestite altrove, oltre a una policy di rilevamento del ransomware gestita nella protezione dal ransomware BlueXP .

Per ulteriori informazioni sulla registrazione di SnapCenter o del plug-in SnapCenter per VMware vSphere utilizzando il backup e recovery di BlueXP, consulta le seguenti informazioni:

- "Registrare il software del server SnapCenter"
- "Registra il plug-in SnapCenter per VMware vSphere"

Fasi

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Dashboard**.
2. Nel riquadro Recommendations (raccomandazioni), individuare uno dei seguenti suggerimenti e selezionare **Review and Fix** (Rivedi e correggi*):
   - Registra i server SnapCenter disponibili con BlueXP
   - Registra il plug-in SnapCenter disponibile per VMware vSphere (SCV) con BlueXP
3. Segui le informazioni per registrare il plug-in SnapCenter o SnapCenter per l'host VMware vSphere utilizzando il backup e recovery di BlueXP.
4. Torna alla protezione dal ransomware di BlueXP.
5. Dalla protezione ransomware di BlueXP, vai alla Dashboard e avvia di nuovo il processo di rilevamento.
6. Da BlueXP ransomware Protection, seleziona **Protection** per visualizzare la pagina Protection.
7. Esaminare i dettagli nella colonna Criteri di backup e snapshot nella pagina protezione per verificare che i criteri siano gestiti altrove.

Aggiungi una strategia di protezione dal ransomware

Puoi aggiungere una strategia di protezione dal ransomware ai carichi di lavoro. Le modalità di esecuzione dipendono dalla presenza o meno di criteri di snapshot e backup:

- **Crea una strategia di protezione dal ransomware se non disponi di policy di backup o snapshot**. Se sul workload non esistono policy di backup o snapshot, puoi creare una strategia di protezione dal ransomware, che può includere le seguenti policy che crei nella protezione dal ransomware BlueXP :
  - Policy di Snapshot
  - Policy di backup
  - Policy di rilevamento del ransomware
- **Creare un criterio di rilevamento per i workload che dispongono già di criteri di snapshot e backup**, che sono gestiti in altri prodotti o servizi NetApp. Il criterio di rilevamento non modifica i criteri gestiti in altri prodotti.

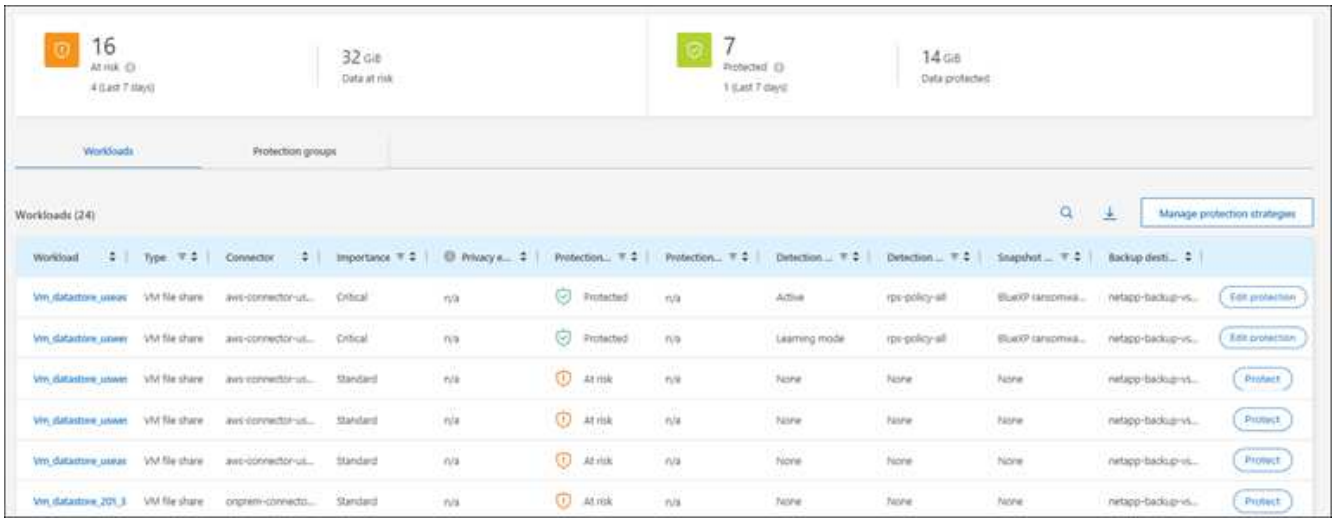
Creare una strategia di protezione dal ransomware (se non disponi di policy di backup o snapshot)

Se sul workload non esistono policy di backup o snapshot, puoi creare una strategia di protezione dal ransomware, che può includere le seguenti policy che crei nella protezione dal ransomware BlueXP :

- Policy di Snapshot
- policy di backup
- Policy di rilevamento del ransomware

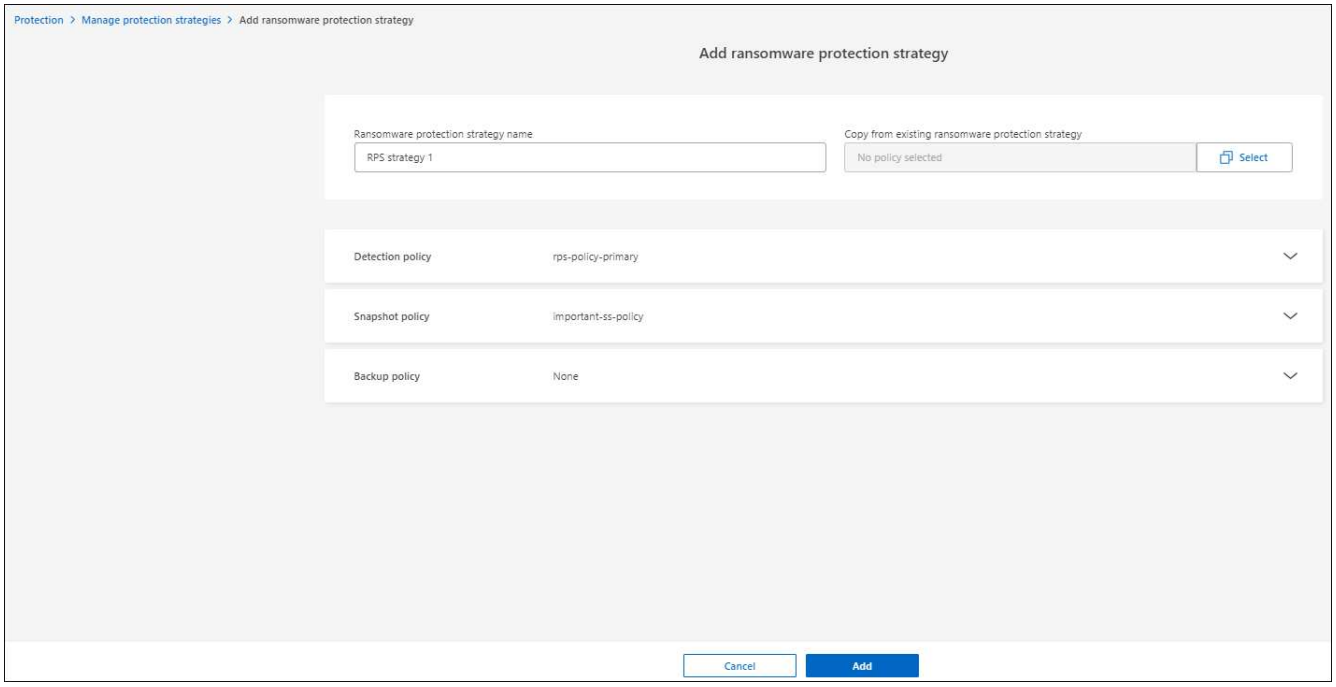
Passaggi per creare una strategia di protezione dal ransomware

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



2. Nella pagina protezione, selezionare **Gestisci strategie di protezione**.

3. Dalla pagina delle strategie di protezione dal ransomware, seleziona **Aggiungi**.



4. Immettere un nuovo nome di strategia o un nome esistente per copiarlo. Se si immette un nome esistente, scegliere quale copiare e selezionare **Copia**.

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

5. Per ciascun elemento, selezionare la **freccia giù**.
   - **Criteri di rilevamento**:
     - **Policy**: Scegliere uno dei criteri di rilevamento preprogettati.
     - **Rilevamento primario**: Abilitare il rilevamento ransomware per fare in modo che il servizio rilevi potenziali attacchi ransomware.
     - **Blocca estensioni file**: Abilitare questa opzione affinché il blocco di servizio conosca le estensioni file sospette. Quando è abilitato il rilevamento primario, il servizio crea copie snapshot automatizzate.

       Se si desidera modificare le estensioni dei file bloccati, modificarle in System Manager.

- **Snapshot policy**:
  - **Snapshot policy base ame**: Selezionare un criterio o selezionare **Create** (Crea*) e immettere un nome per il criterio snapshot.
  - **Snapshot locking**: Permette di bloccare le copie snapshot sullo storage primario in modo che non possano essere modificate o eliminate per un certo periodo di tempo, anche se un attacco ransomware gestisce la destinazione storage di backup. Questo viene anche chiamato *storage immutabile*. Ciò consente tempi di ripristino più rapidi.

    Quando uno snapshot è bloccato, l'ora di scadenza del volume è impostata sull'ora di scadenza della copia snapshot.

  Il blocco della copia snapshot è disponibile con ONTAP 9.12.1 e versioni successive. Per ulteriori informazioni su SnapLock, fare riferimento a. "SnapLock a ONTAP".

  - **Pianificazioni istantanee**: Scegliere le opzioni di pianificazione, il numero di copie snapshot da conservare e selezionare per attivare la pianificazione.
- **Politica di backup**:
  - **Backup policy basename**: Immettere un nuovo nome o scegliere un nome esistente.
  - **Pianificazioni di backup**: Scegliere le opzioni di pianificazione per l'archiviazione secondaria e attivare la pianificazione.

> Per abilitare il blocco dei backup nell'archiviazione secondaria, configurare le destinazioni di backup utilizzando l'opzione **Impostazioni**. Per ulteriori informazioni, vedere "Configurare le impostazioni".

6. Selezionare **Aggiungi**.

Aggiungere una policy di rilevamento ai carichi di lavoro che dispongono già di policy di backup e snapshot

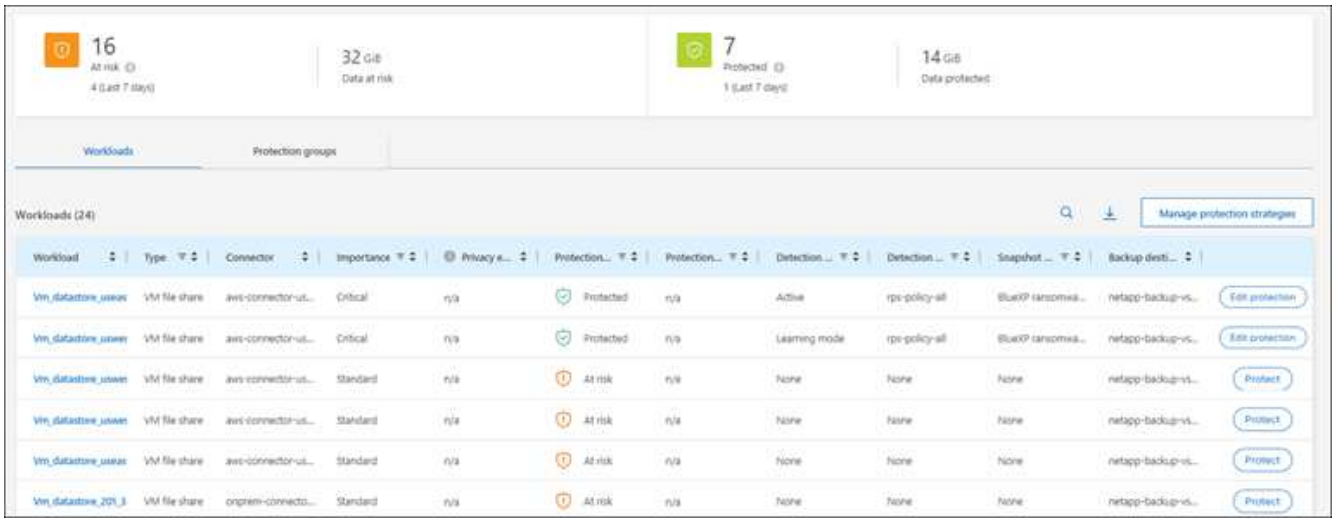
Con la protezione dal ransomware di BlueXP puoi assegnare una policy di rilevamento del ransomware a workload che dispongono già di policy di backup e snapshot, gestite in altri prodotti o servizi NetApp. Il criterio di rilevamento non modifica i criteri gestiti in altri prodotti.

Altri servizi, come backup e recovery di BlueXP e SnapCenter, utilizzano i seguenti tipi di policy per gestire i workload:

- Policy che governano gli snapshot
- Policy che governano la replica sullo storage secondario
- Policy che governano i backup nello storage a oggetti

Fasi

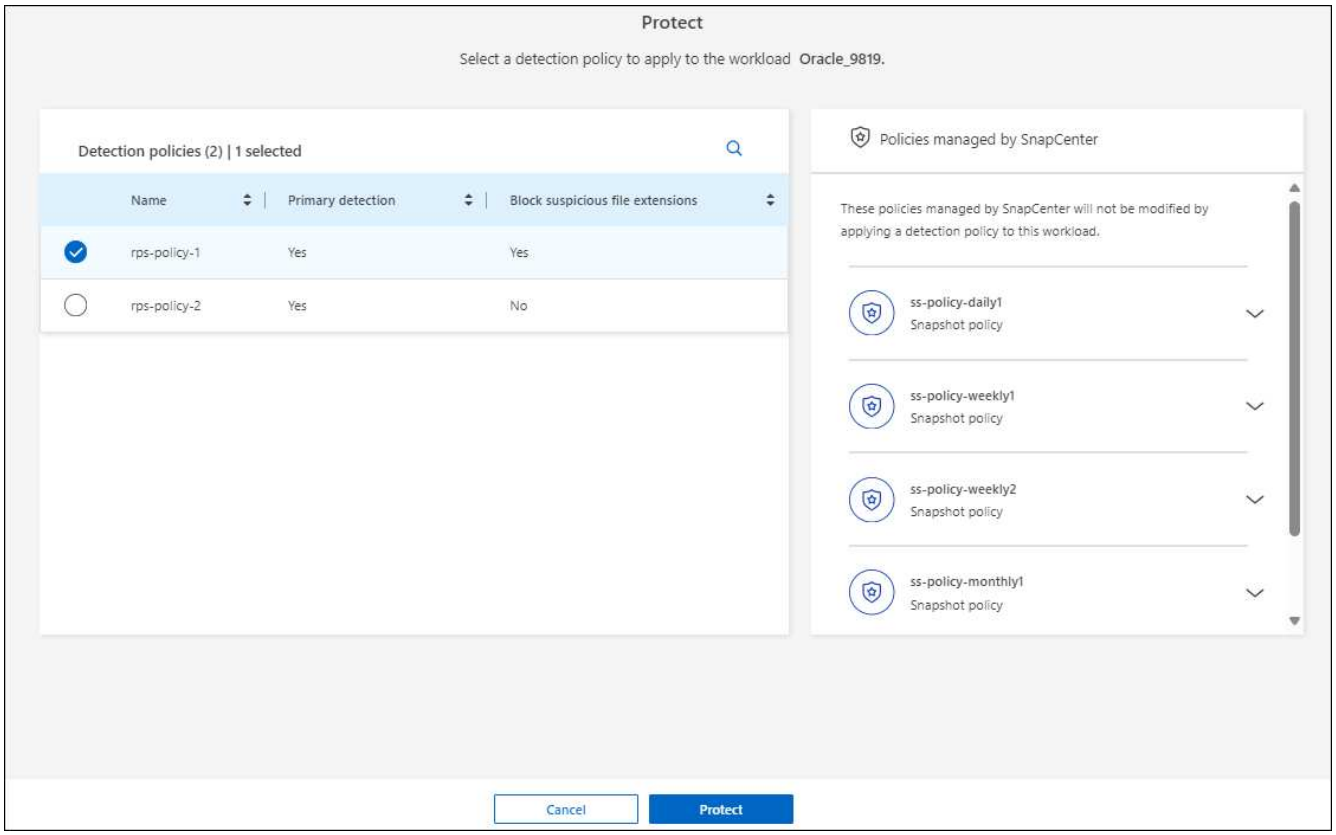
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



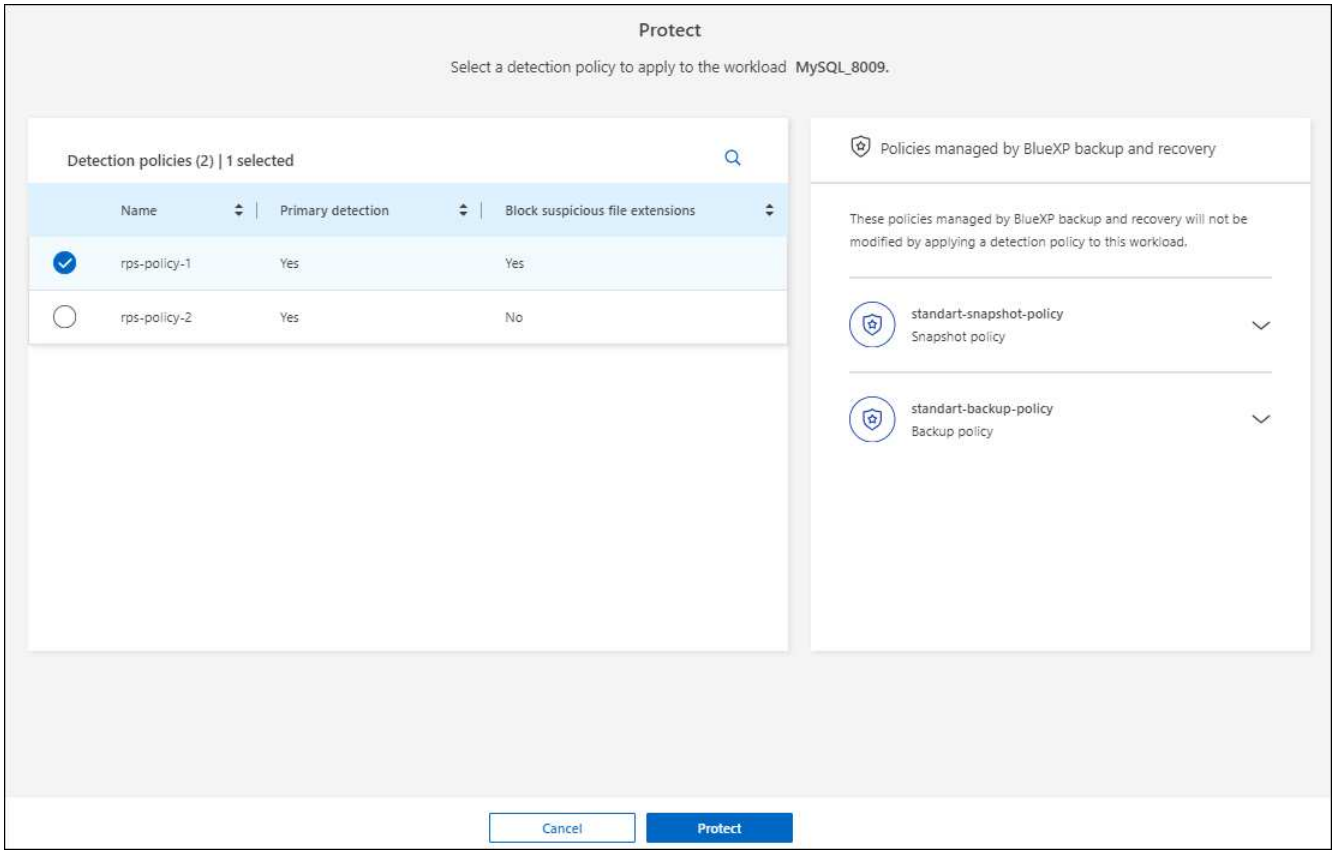
2. Nella pagina protezione, selezionare un carico di lavoro e selezionare **Proteggi**.

   La pagina di protezione mostra le policy gestite dal software SnapCenter, da SnapCenter per VMware vSphere e dal backup e recovery di BlueXP.

   Nell'esempio seguente vengono illustrati i criteri gestiti da SnapCenter:



   Il seguente esempio mostra le policy gestite dal backup e recovery di BlueXP:



3. Per visualizzare i dettagli dei criteri gestiti altrove, fare clic sulla freccia **giù**.
4. Per applicare un criterio di rilevamento oltre ai criteri di snapshot e backup gestiti altrove, selezionare il criterio di rilevamento.
5. Selezionare **Proteggi**.
6. Nella pagina protezione, esaminare la colonna Criteri di rilevamento per vedere il criterio di rilevamento assegnato. Inoltre, nella colonna Criteri di backup e snapshot viene visualizzato il nome del prodotto o servizio che gestisce i criteri.

Assegnare un criterio diverso

È possibile assegnare un criterio di protezione diverso sostituendo quello corrente.

Fasi

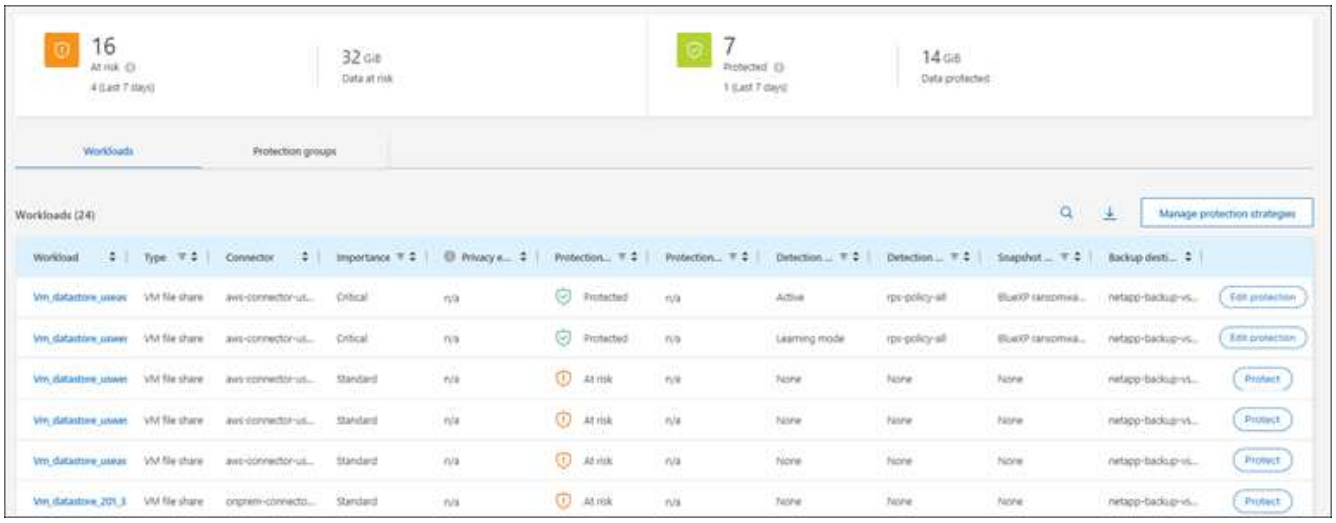
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, nella riga del carico di lavoro, selezionare **Modifica protezione**.
3. Nella pagina Criteri, fare clic sulla freccia verso il basso relativa al criterio che si desidera assegnare per rivedere i dettagli.
4. Selezionare il criterio che si desidera assegnare.
5. Selezionare **Proteggi** per terminare la modifica.

Condivisione di file di gruppo per una protezione più semplice

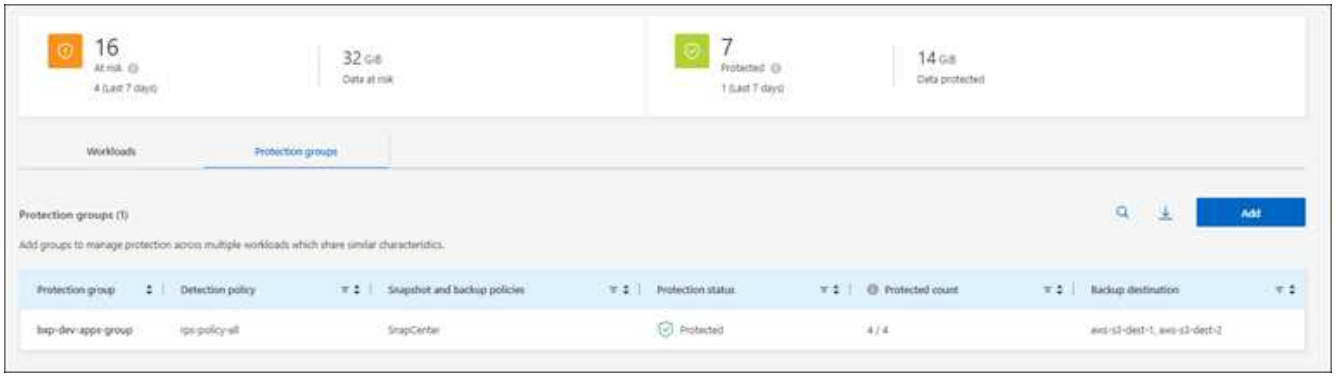
Il raggruppamento delle condivisioni dei file semplifica la protezione dell'ambiente dati. Il servizio consente di proteggere contemporaneamente tutti i volumi di un gruppo piuttosto che proteggere ogni volume separatamente.

Fasi

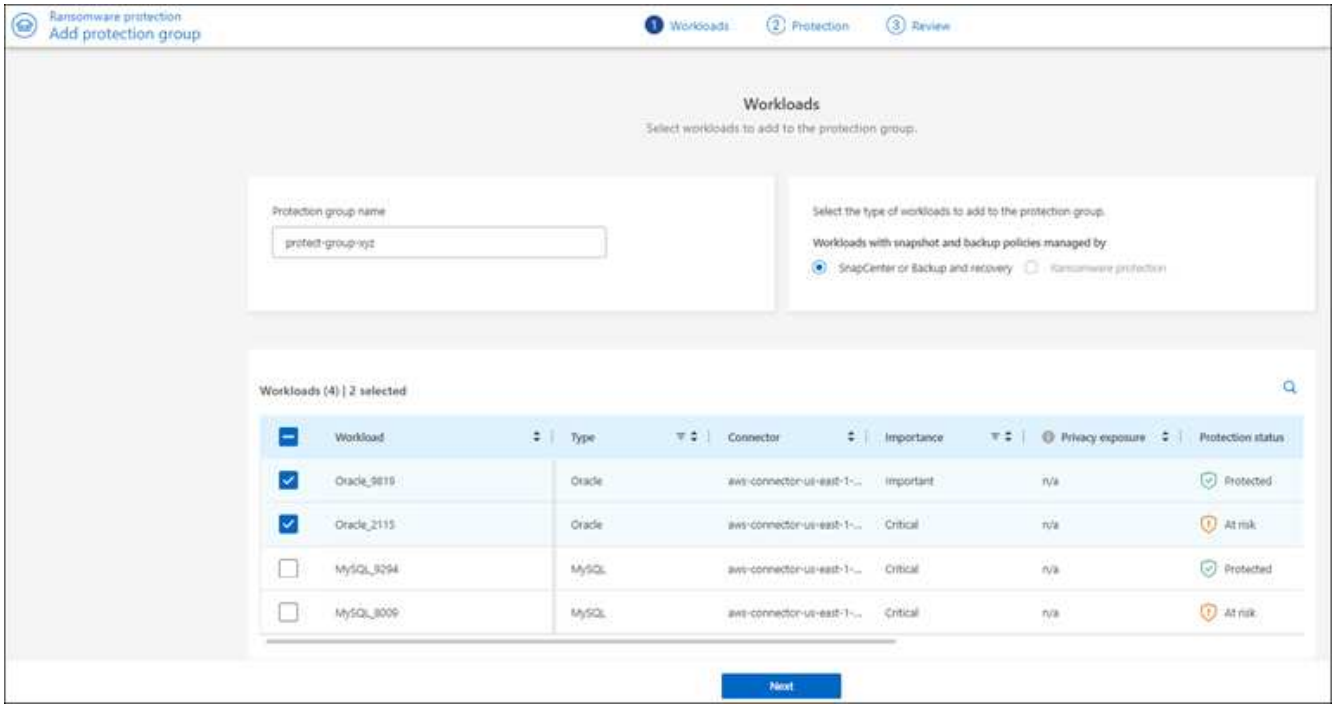
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



2. Nella pagina protezione, selezionare la scheda **gruppi protezione**.



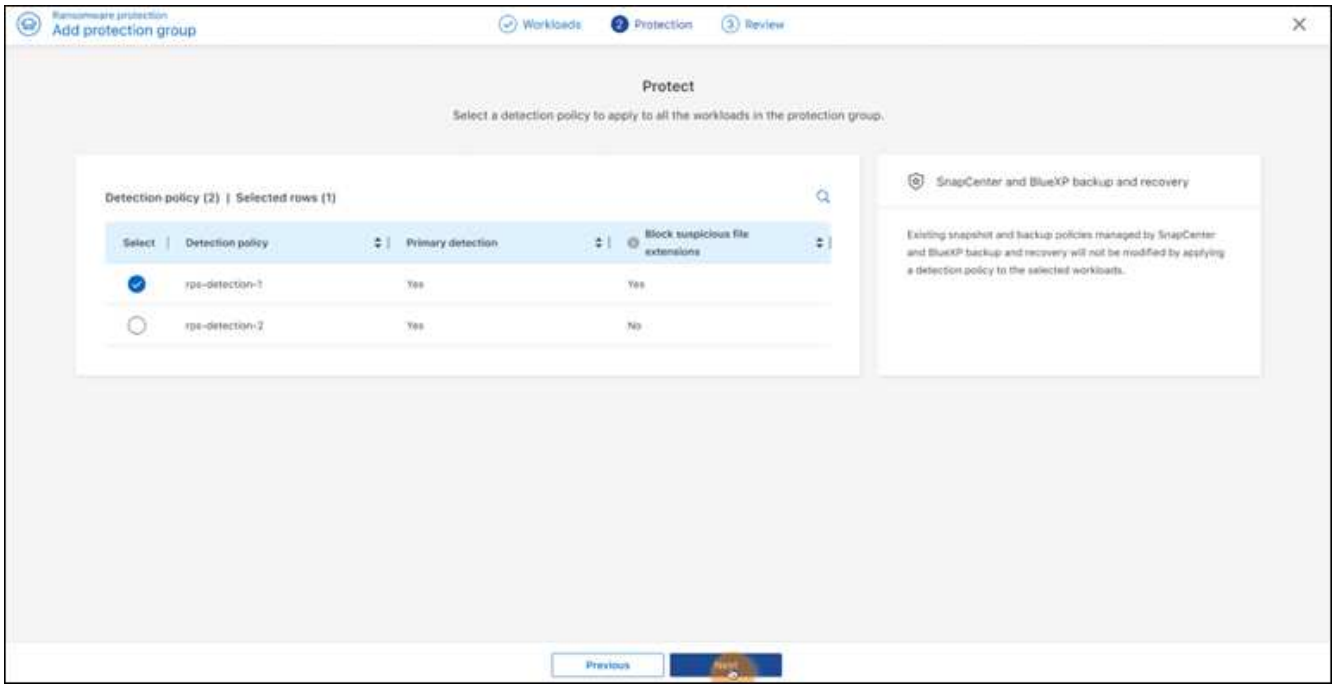
3. Selezionare **Aggiungi**.



4. Immettere un nome per il gruppo protezione.
5. Completare una delle seguenti operazioni:
   a. Se disponi già di policy di protezione, seleziona se vuoi raggruppare i carichi di lavoro in base alla loro gestione da uno dei seguenti elementi:
      - Protezione ransomware BlueXP
      - Backup e recovery di SnapCenter o BlueXP
   b. Se non disponi già di policy di protezione, viene visualizzata la pagina delle strategie di protezione dal ransomware preconfigurate.
      i. Scegliere un'opzione per proteggere il gruppo e selezionare **Avanti**.
      ii. Se il workload scelto dispone di volumi in più ambienti di lavoro, seleziona la destinazione di backup per i diversi ambienti di lavoro in modo che possa essere eseguito il backup nel cloud.
6. Selezionare i carichi di lavoro da aggiungere al gruppo.

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

7. Selezionare **Avanti**.



8. Selezionare il criterio che regolerà la protezione per questo gruppo.
9. Selezionare **Avanti**.
10. Esaminare le selezioni per il gruppo protezione.
11. Selezionare **Aggiungi**.

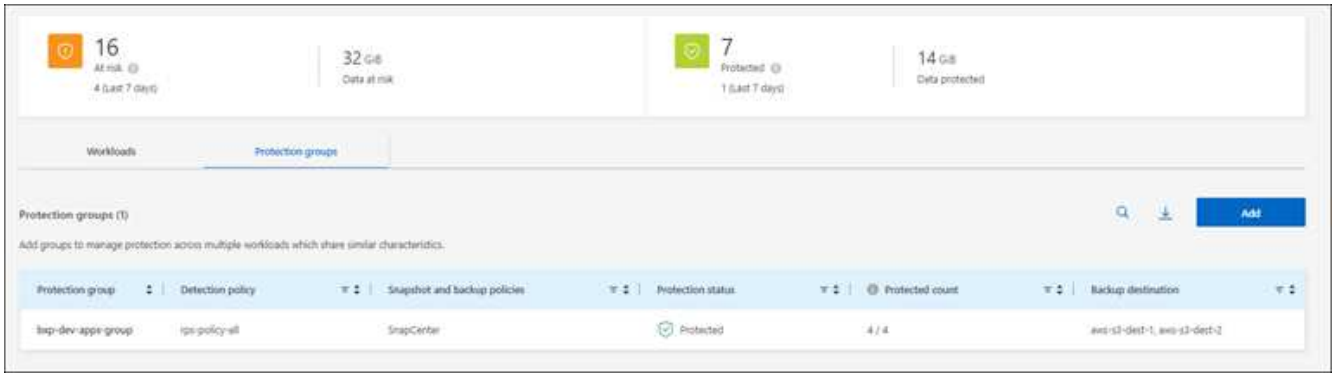
Aggiungere altri carichi di lavoro a un gruppo

In seguito, potrebbe essere necessario aggiungere altri carichi di lavoro a un gruppo esistente.

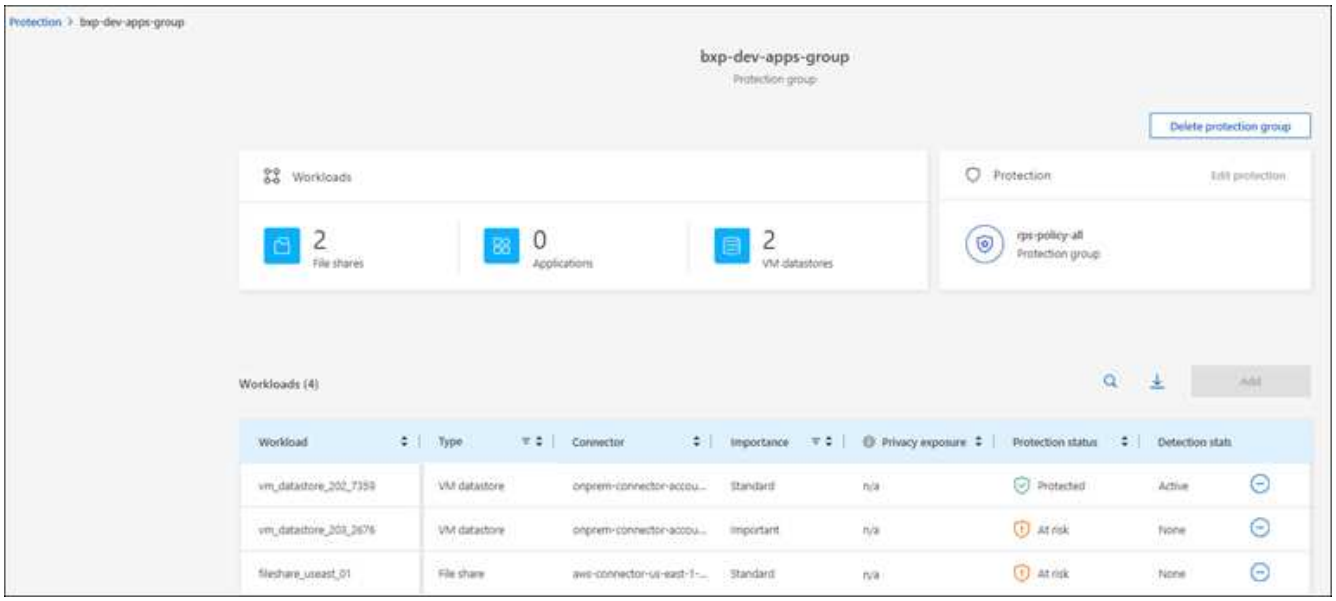
Se il gruppo include carichi di lavoro gestiti solo dalla protezione anti-ransomware BlueXP (e non dal backup e recovery di SnapCenter o BlueXP), dovresti utilizzare gruppi separati per i carichi di lavoro gestiti solo dalla protezione anti-ransomware BlueXP e un altro gruppo per i carichi di lavoro gestiti da altri servizi.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare la scheda **gruppi protezione**.



3. Selezionare il gruppo a cui si desidera aggiungere altri carichi di lavoro.



4. Dalla pagina Gruppo protezione selezionato, selezionare **Aggiungi**.

   La protezione ransomware di BlueXP mostra solo i workload che non sono già nel gruppo che utilizzano le stesse policy di backup e snapshot del gruppo.

   Nella parte superiore della pagina viene visualizzato il servizio che gestisce le policy di snapshot, backup e rilevamento.

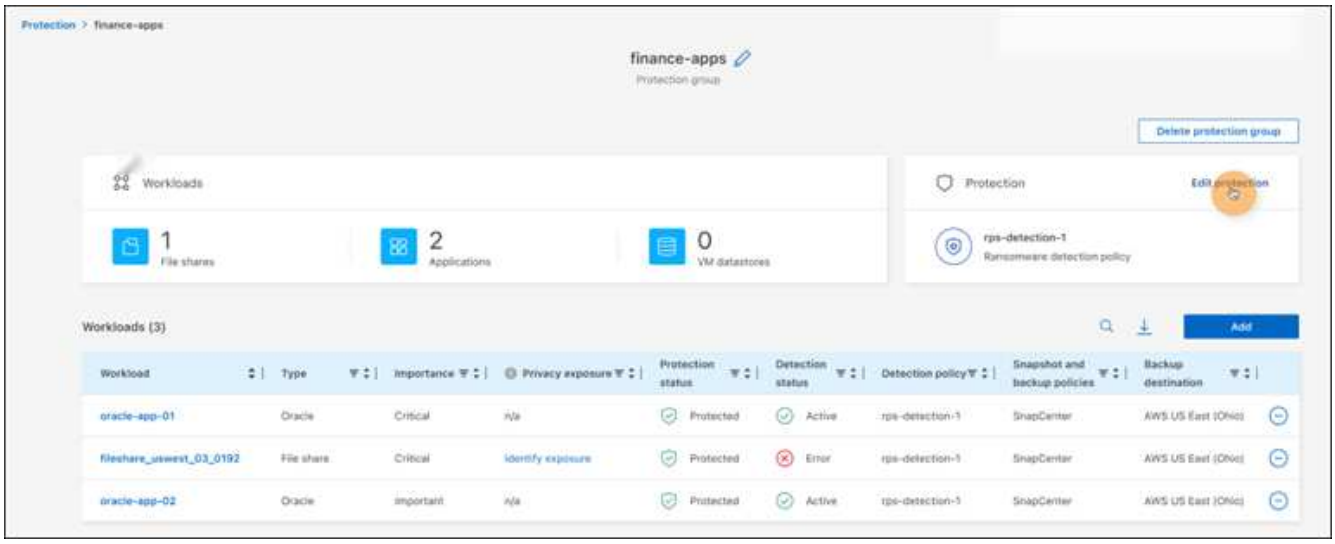
5. Selezionare i carichi di lavoro aggiuntivi da aggiungere al gruppo.
6. Selezionare **Salva**.

Modifica protezione gruppo

È possibile modificare il criterio di rilevamento in un gruppo esistente. Se il criterio di rilevamento non è già stato aggiunto a questo gruppo, è possibile aggiungerlo ora.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare la scheda **gruppi protezione**.



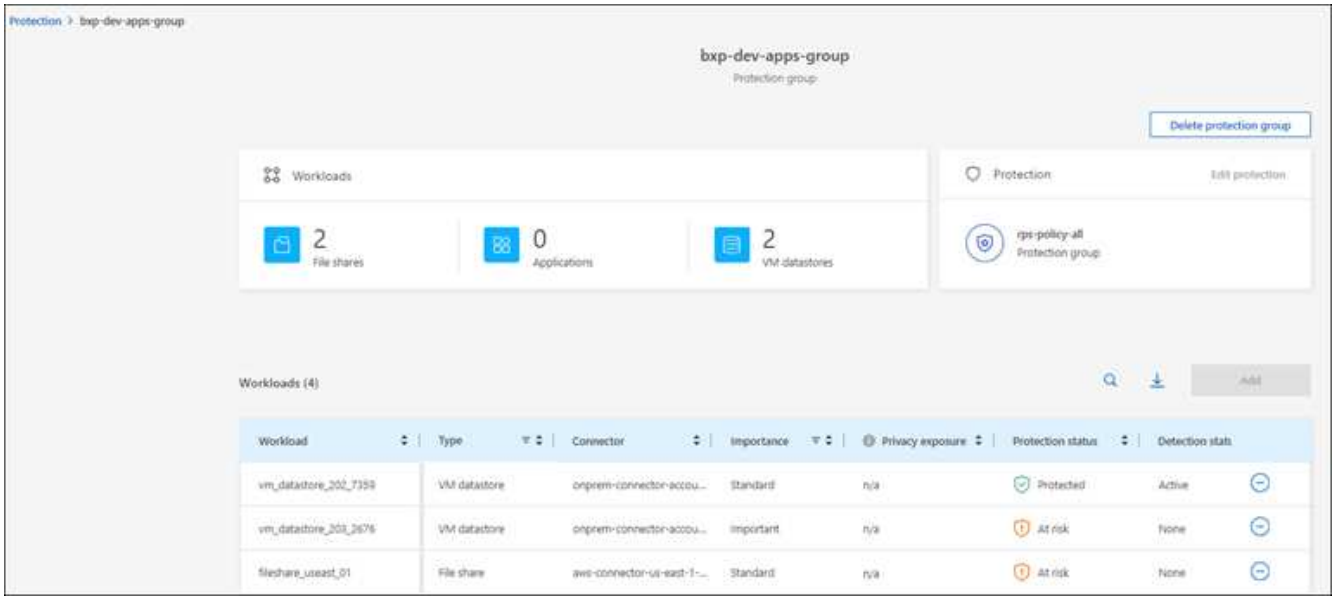
3. Dal riquadro protezione, selezionare **Modifica protezione**.
4. Selezionare o aggiungere un criterio di rilevamento a questo gruppo.

Rimuovere i carichi di lavoro da un gruppo

In seguito, potrebbe essere necessario rimuovere i carichi di lavoro da un gruppo esistente.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare la scheda **gruppi protezione**.
3. Selezionare il gruppo dal quale si desidera rimuovere uno o più carichi di lavoro.



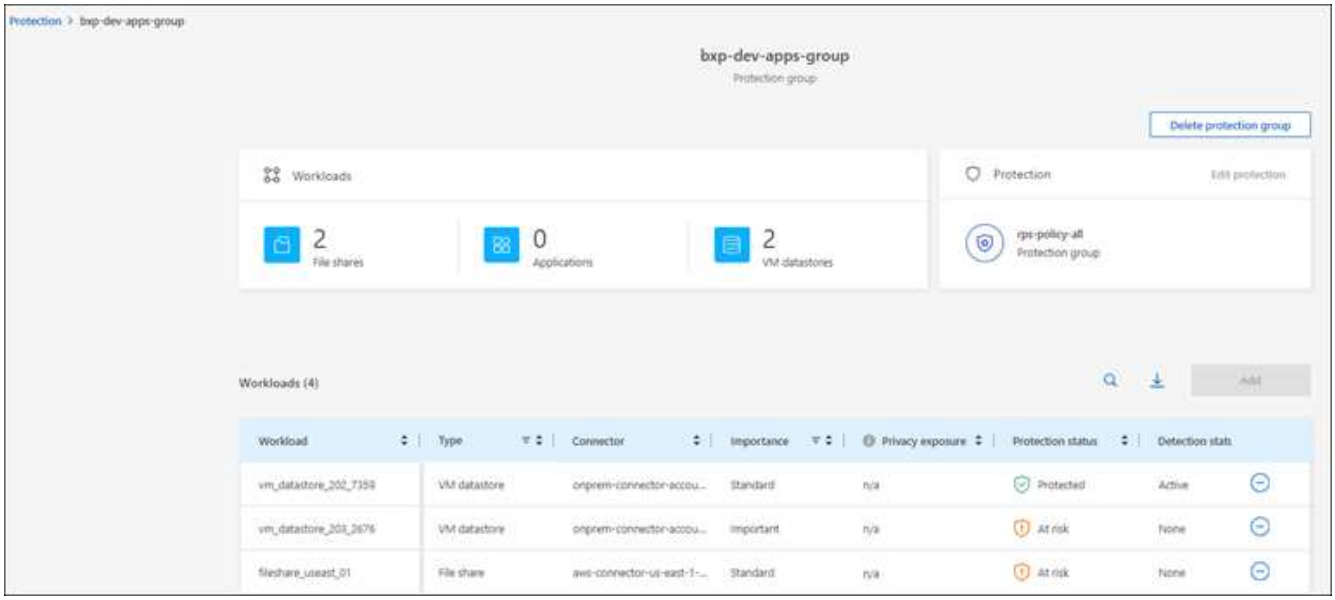
4. Dalla pagina Gruppo protezione selezionato, selezionare il carico di lavoro che si desidera rimuovere dal gruppo e selezionare l'opzione *azioni*•••.
5. Dal menu azioni, selezionare **Rimuovi carico di lavoro**.
6. Confermare che si desidera rimuovere il carico di lavoro e selezionare **Rimuovi**.

Eliminare il gruppo protezione

L'eliminazione del gruppo di protezione rimuove il gruppo e la relativa protezione, ma non rimuove i singoli carichi di lavoro.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare la scheda **gruppi protezione**.
3. Selezionare il gruppo dal quale si desidera rimuovere uno o più carichi di lavoro.



4. Nella pagina Gruppo protezione selezionato, in alto a destra, selezionare **Elimina gruppo protezione**.
5. Confermare che si desidera eliminare il gruppo e selezionare **Elimina**.

Gestire le strategie di protezione dal ransomware

Puoi eliminare una strategia ransomware.

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

Prima di eliminare una strategia di protezione dal ransomware, potresti voler visualizzare i carichi di lavoro protetti da tale strategia.

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

Procedura per la visualizzazione dell'elenco delle strategie

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare **Gestisci strategie di protezione**.

   La pagina delle strategie di protezione dal ransomware visualizza un elenco di strategie.

3. Nella pagina strategie di protezione dal ransomware, nella colonna carichi di lavoro protetti, fare clic sulla freccia verso il basso alla fine della riga.

Elimina una strategia di protezione dal ransomware

Puoi eliminare una strategia di protezione non attualmente associata a alcun carico di lavoro.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare **Gestisci strategie di protezione**.
3. Nella pagina Gestisci strategie, selezionare l'opzione **azioni** ••• per la strategia che si desidera eliminare.
4. Dal menu azioni, selezionare **Elimina criterio**.

Rispondi a un avviso ransomware rilevato

Se la protezione ransomware di BlueXP rileva un possibile attacco, viene visualizzato un avviso nella dashboard di protezione dal ransomware di BlueXP e nelle notifiche di BlueXP, in alto a destra, che indica un potenziale attacco ransomware. Inoltre, il servizio avvia immediatamente l'acquisizione di una copia Snapshot. A questo punto, dovresti valutare il rischio potenziale nella scheda **Avvisi** della protezione dal ransomware di BlueXP.

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

> Se si decide di ignorare l'avviso, il servizio apprenderà questo comportamento e lo assocerà alle normali operazioni e non avvierà nuovamente un avviso su tale comportamento.

Per iniziare il ripristino dei dati, contrassegnare l'avviso come pronto per il ripristino in modo che l'amministratore dello storage possa avviare il processo di ripristino.

Ogni avviso potrebbe avere più incidenti su volumi diversi con stati diversi, quindi assicurati di esaminare tutti gli incidenti.

Il servizio fornisce informazioni denominate *prove* su ciò che ha causato l'emissione dell'avviso, come le seguenti:

- Le estensioni dei file sono state create o modificate

- Si è verificata la creazione del file ed è stato aumentato di una percentuale elencata
- Si è verificata l'eliminazione dei file e l'aumento è stato calcolato in percentuale

Un avviso si basa sui seguenti tipi di comportamento:

- **Potenziale attacco**: Si verifica un avviso quando la protezione autonoma dal ransomware rileva una nuova estensione e l'evento viene ripetuto più di 20 volte nelle ultime 24 ore (comportamento predefinito).
- **Avvertenza**: Si verifica un avviso basato sui seguenti comportamenti:
  - Il rilevamento di una nuova estensione non è stato identificato in precedenza e lo stesso comportamento non si ripete abbastanza volte per dichiararla come attacco.
  - Si osserva un'elevata entropia.
  - Le operazioni di lettura/scrittura/ridenominazione/eliminazione dei file hanno subito un aumento dell'attività del 100% oltre la baseline.

Le prove si basano sulle informazioni fornite dalla protezione autonoma dal ransomware in ONTAP. Per ulteriori informazioni, fare riferimento a. "Panoramica della protezione ransomware autonoma".

Un avviso può avere uno dei seguenti stati:

- **Nuovo**
- **Inattivo**

Un incidente di avviso è classificato in uno dei seguenti stati:

- **Nuovo**: Tutti gli incidenti sono contrassegnati come "nuovi" quando vengono identificati per la prima volta.
- **Respinto**: Se sospetti che l'attività non sia un attacco ransomware, puoi cambiare lo stato in "respinto".

> Dopo aver respinto un attacco, non è possibile modificarlo. Se elimini un carico di lavoro, tutte le copie Snapshot acquisite automaticamente in risposta al potenziale attacco ransomware verranno eliminate in maniera permanente.

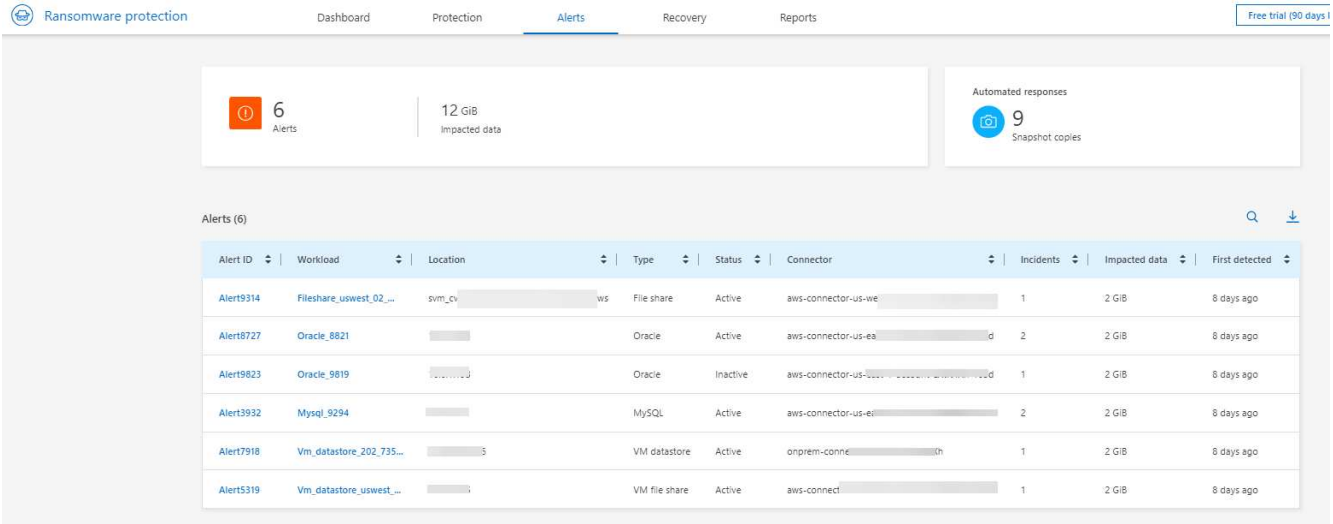
- **Licenziamento**: L'incidente è in fase di licenziamento.
- **Risolto**: L'incidente è stato mitigato.

Visualizza avvisi

Puoi accedere agli avvisi dalla dashboard della protezione dal ransomware di BlueXP o dalla scheda **Alerts**.

Fasi

1. Nella dashboard di protezione dal ransomware di BlueXP, consulta il pannello Alerts.
2. Selezionare **Visualizza tutto** sotto una delle statue.
3. Fare clic su un avviso per esaminare tutti gli incidenti su ciascun volume per ciascun avviso.
4. Per rivedere gli avvisi aggiuntivi, fare clic su **Alert** nella barra di navigazione in alto a sinistra.
5. Esaminare gli avvisi nella pagina Avvisi.



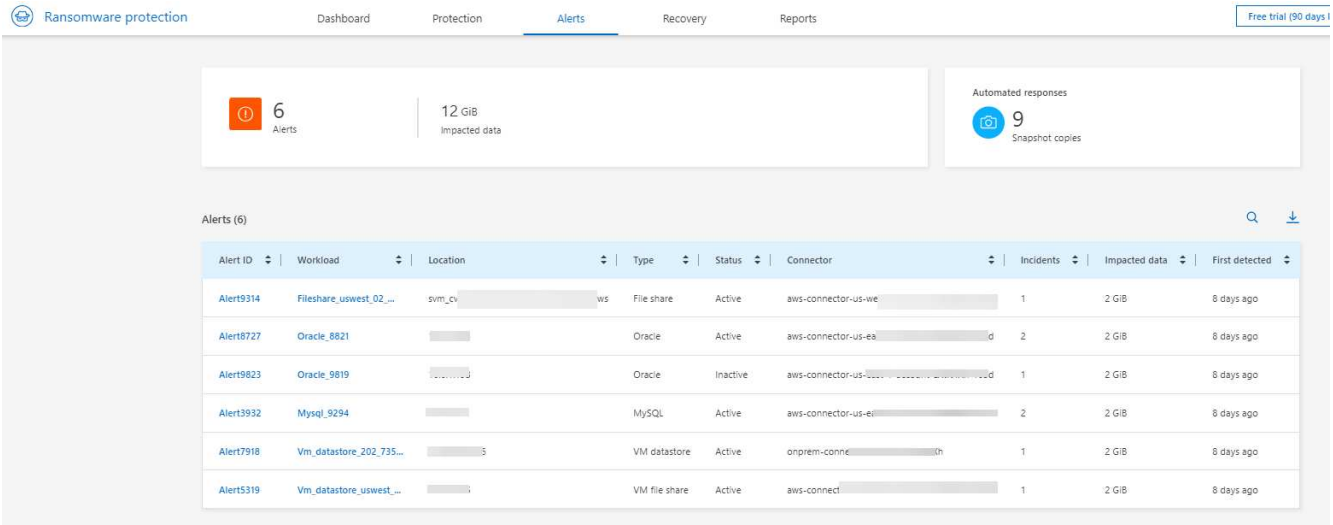
6. Continua:
   - Contrassegna gli incidenti ransomware come pronti per il recovery (dopo la neutralizzazione degli incidenti).
   - Elimina gli incidenti che non sono potenziali attacchi.

Contrassegna gli incidenti ransomware come pronti per il recovery (dopo la neutralizzazione degli incidenti)

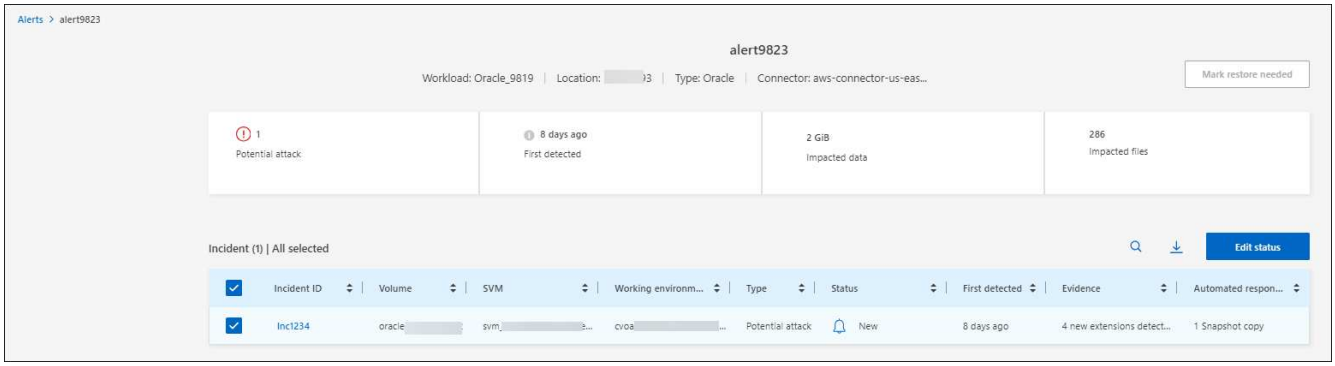
Una volta mitigato l'attacco e sei pronto a ripristinare i carichi di lavoro, dovresti comunicare con il tuo team di amministrazione dello storage che i dati sono pronti per il recovery, in modo che possano avviare il processo di recovery.

Fasi

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Avvisi**.



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



4. Se si stabilisce che gli incidenti sono pronti per il ripristino, selezionare **Segna ripristino necessario**.
5. Confermare l'azione e selezionare **Segna ripristino necessario**.
6. Per avviare il ripristino del carico di lavoro, selezionare **Recupera** carico di lavoro nel messaggio o selezionare la scheda **Recovery**.

Risultato

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

Elimina gli incidenti che non sono potenziali attacchi

Dopo aver esaminato gli incidenti, è necessario determinare se si tratta di potenziali attacchi. In caso contrario, possono essere respinte.

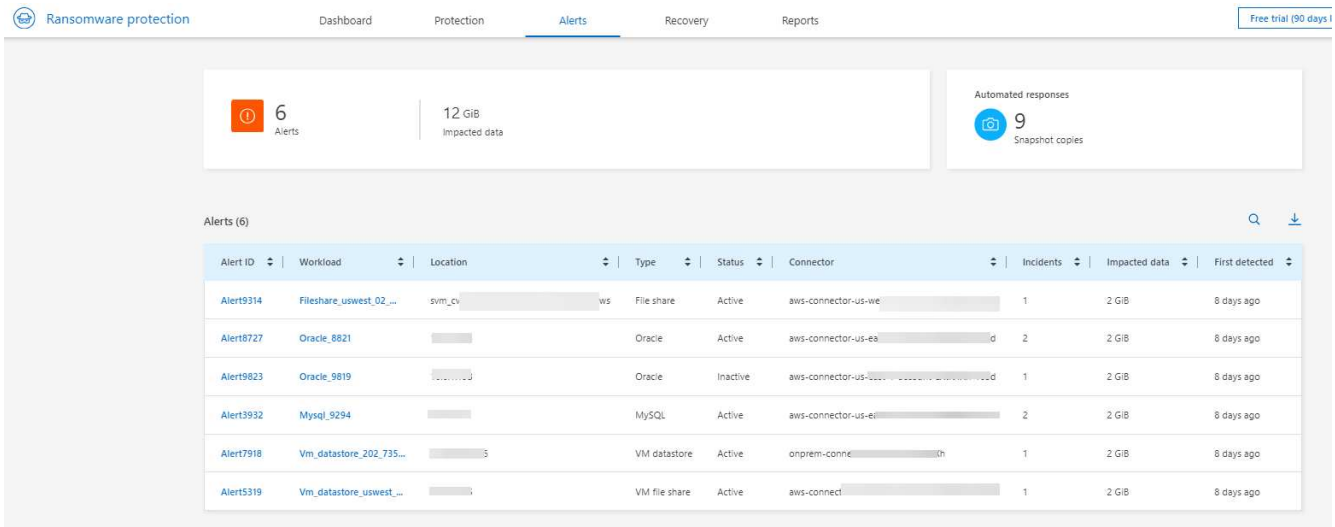
Puoi liquidare i falsi positivi o decidere di recuperare immediatamente i tuoi dati. Se si decide di ignorare l'avviso, il servizio apprenderà questo comportamento e lo assocerà alle normali operazioni e non avvierà nuovamente un avviso su tale comportamento.

Se elimini un carico di lavoro, tutte le copie Snapshot acquisite automaticamente in risposta al potenziale attacco ransomware verranno eliminate in maniera permanente.

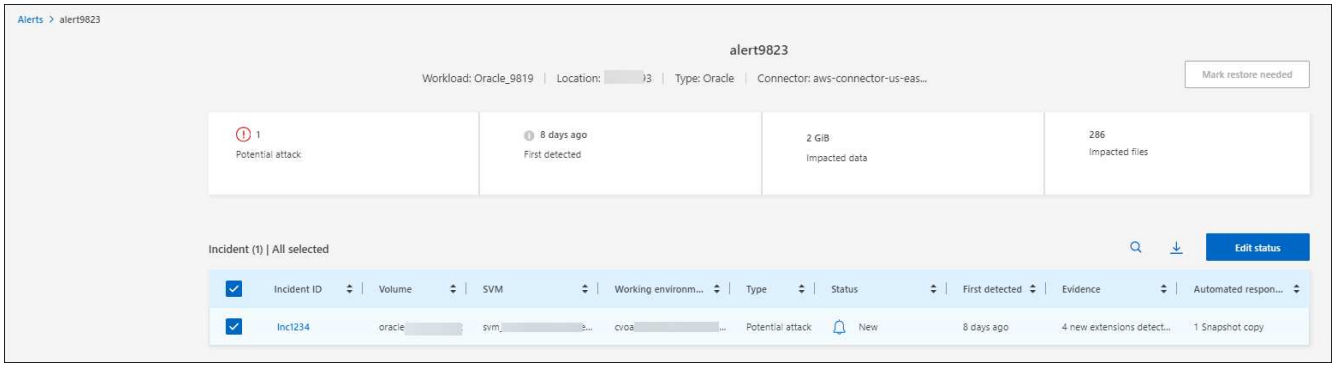
> Se si ignora un avviso, non è possibile ripristinare lo stato in qualsiasi altro stato e non è possibile annullare la modifica.

Fasi

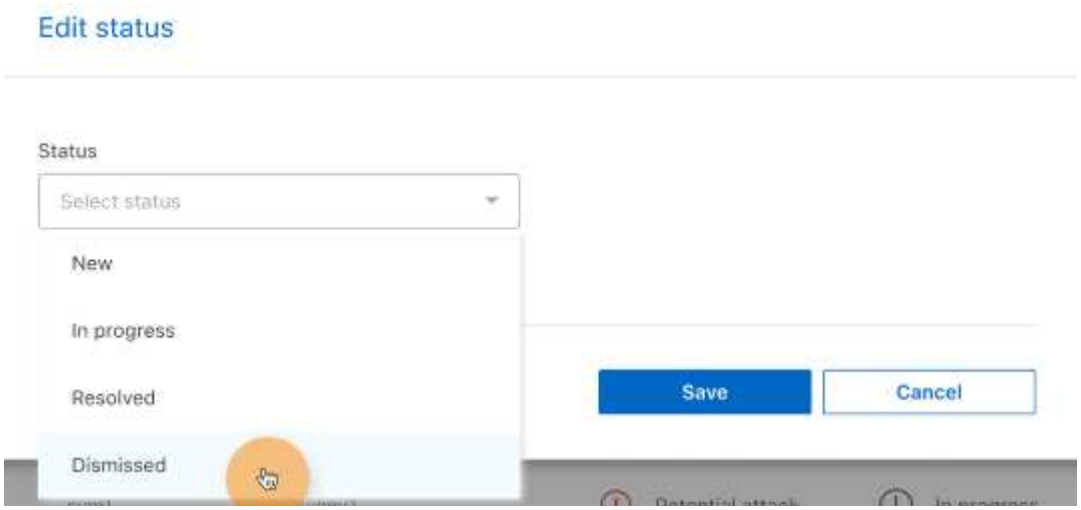
1. Dal menu di protezione dal ransomware BlueXP, seleziona **Avvisi**.



2. Nella pagina Avvisi, selezionare l'avviso.



3. Selezionare uno o più incidenti. In alternativa, selezionare tutti gli incidenti selezionando la casella ID incidente nella parte superiore sinistra della tabella.
4. Se si stabilisce che l'incidente non è una minaccia, eliminarlo come falso positivo:
   - Se è stato selezionato un incidente, selezionare **azioni** … A destra, selezionare **Modifica stato**.
   - Se sono stati selezionati più incidenti, selezionare il pulsante **Modifica stato** sopra la tabella.



5. Nella casella Modifica stato, selezionare lo stato **"respinto"**.

   Vengono visualizzate ulteriori informazioni sul carico di lavoro e sulle copie Snapshot che verranno eliminate.

6. Selezionare **Salva**.

   Lo stato dell'incidente o degli incidenti diventa "respinto".

Consente di visualizzare un elenco dei file interessati

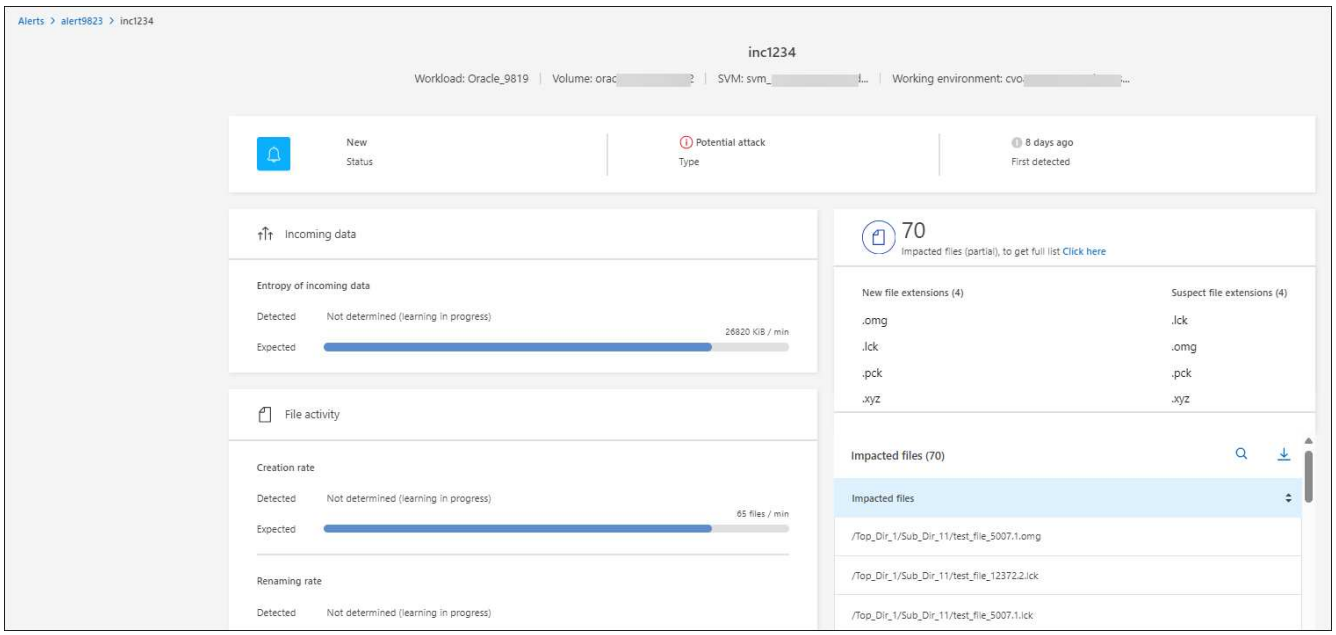
Prima di ripristinare un workload dell'applicazione a livello di file, è possibile visualizzare un elenco di file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco di file interessati. Quindi, utilizzare la pagina di ripristino per caricare l'elenco e scegliere i file da ripristinare.

Fasi

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 di protezione dal ransomware BlueXP, seleziona **Avvisi**.
2. Nella pagina Avvisi, ordinare i risultati per carico di lavoro per visualizzare gli avvisi per il carico di lavoro dell'applicazione che si desidera ripristinare.
3. Dall'elenco degli avvisi per il carico di lavoro, selezionare un avviso.
4. Per tale avviso, selezionare un singolo incidente.



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

Ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti)

Dopo che i carichi di lavoro sono stati contrassegnati come "ripristino necessario", la protezione dal ransomware di BlueXP consiglia un recovery point effettivo (RPA) e orchestra il workflow per un recovery resistente ai crash.

- Se l'applicazione o la macchina virtuale è gestita da SnapCenter, la protezione dal ransomware di BlueXP ripristina lo stato precedente dell'applicazione o della macchina virtuale e l'ultima transazione mediante un processo coerente con l'applicazione o con le macchine virtuali. Il ripristino coerente con l'applicazione o con la macchina virtuale aggiunge i dati che non sono stati inseriti nello storage, ad esempio i dati in cache o in un'operazione di i/o, ai dati del volume.
- Se l'applicazione o la macchina virtuale è *non* gestita da SnapCenter ed è gestita da backup e recovery di BlueXP o dalla protezione dal ransomware di BlueXP, la protezione dal ransomware di BlueXP esegue un ripristino coerente con il crash, in cui tutti i dati che erano nel volume nello stesso point of time vengono ripristinati, ad esempio, se il sistema si è bloccato.

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

Il ripristino dei workload può avere un impatto negativo sui workload in esecuzione. È necessario coordinare i processi di ripristino con gli stakeholder appropriati.

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

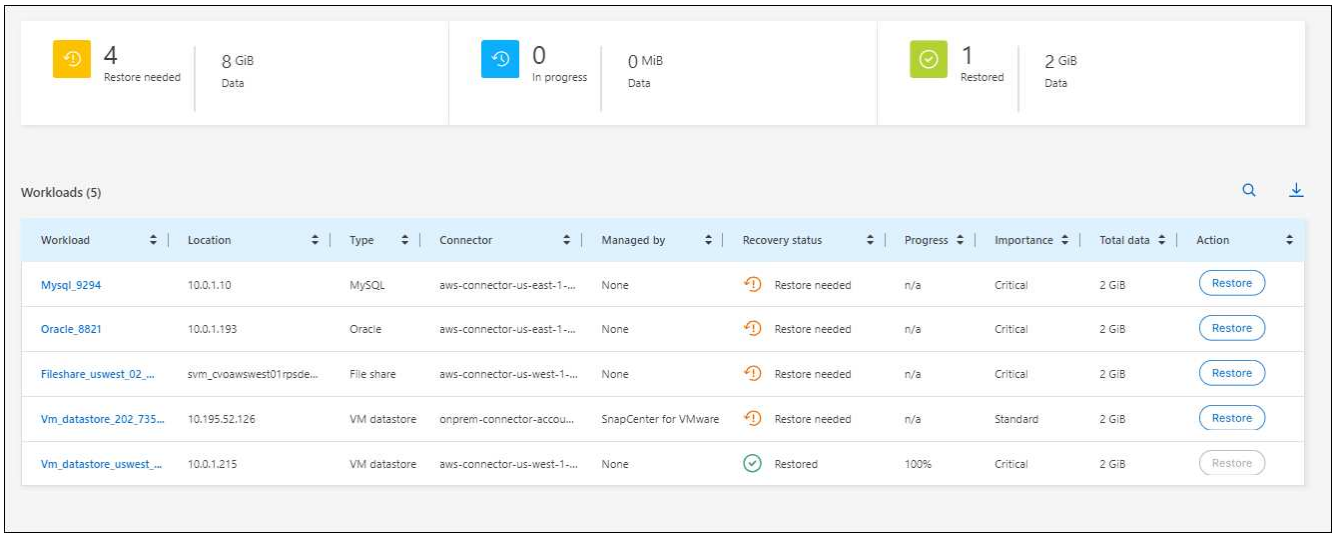
- **Necessario ripristino**: Il carico di lavoro deve essere ripristinato.
- **In corso**: L'operazione di ripristino è attualmente in corso.
- **Ripristinato**: Il carico di lavoro è stato ripristinato.
- **Non riuscito**: Impossibile completare il processo di ripristino del workload.

Visualizza i carichi di lavoro pronti per il ripristino

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

Fasi

1. Effettuare una delle seguenti operazioni:
    - Dal dashboard, esaminare i totali "Ripristina necessario" nel riquadro Avvisi e selezionare **Visualizza tutto**.
    - Dal menu, selezionare **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Ripristino**.



Ripristinare un carico di lavoro gestito da SnapCenter

Utilizzando la protezione dal ransomware di BlueXP, l'amministratore dello storage può determinare la modalità migliore per ripristinare i workload dal punto di ripristino consigliato o dal punto di ripristino preferito.

Lo stato dell'applicazione cambia se necessario per il ripristino. L'applicazione verrà ripristinata allo stato precedente dai file di controllo, se inclusi nel backup. Al termine del ripristino, l'applicazione si apre in modalità LETTURA/SCRITTURA.

Fasi

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Ripristino**.

3. Seleziona un carico di lavoro in stato "Ripristino necessario".
4. Per ripristinare, selezionare **Ripristina**.
5. **Ambito di ripristino**: Coerente con l'applicazione (o per SnapCenter per VM, l'ambito di ripristino è "per VM")
6. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione "consigliata".

7. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Selezionare la posizione originale o alternativa.
   b. Selezionare l'ambiente di lavoro.
   c. Selezionare la VM di storage.
8. Se la destinazione originale non dispone di spazio sufficiente per ripristinare il carico di lavoro, viene visualizzata la riga "archiviazione temporanea". È possibile selezionare la memoria temporanea per ripristinare i dati del carico di lavoro. I dati ripristinati verranno copiati dalla memoria temporanea alla posizione originale. Fare clic sulla freccia **giù** nella riga archiviazione temporanea e impostare il cluster di destinazione, la VM di archiviazione e il livello locale.
9. Selezionare **Salva**.
10. Selezionare **Avanti**.
11. Rivedere le selezioni.
12. Selezionare **Restore** (Ripristina).
13. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati.

Ripristino di un carico di lavoro non gestito da SnapCenter

Utilizzando la protezione dal ransomware di BlueXP, l'amministratore dello storage può determinare la modalità migliore per ripristinare i workload dal punto di ripristino consigliato o dal punto di ripristino preferito.

L'amministratore dello storage di sicurezza può ripristinare i dati a diversi livelli:

- Recovery di tutti i volumi
- Ripristinare un'applicazione a livello di volume o di file e cartella.
- Ripristinare una condivisione file a livello di volume, directory o file/cartella.
- Eseguire il ripristino da un datastore a livello di macchina virtuale.

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

Fasi

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Ripristino**.
3. Seleziona un carico di lavoro in stato "Ripristino necessario".
4. Per ripristinare, selezionare **Ripristina**.

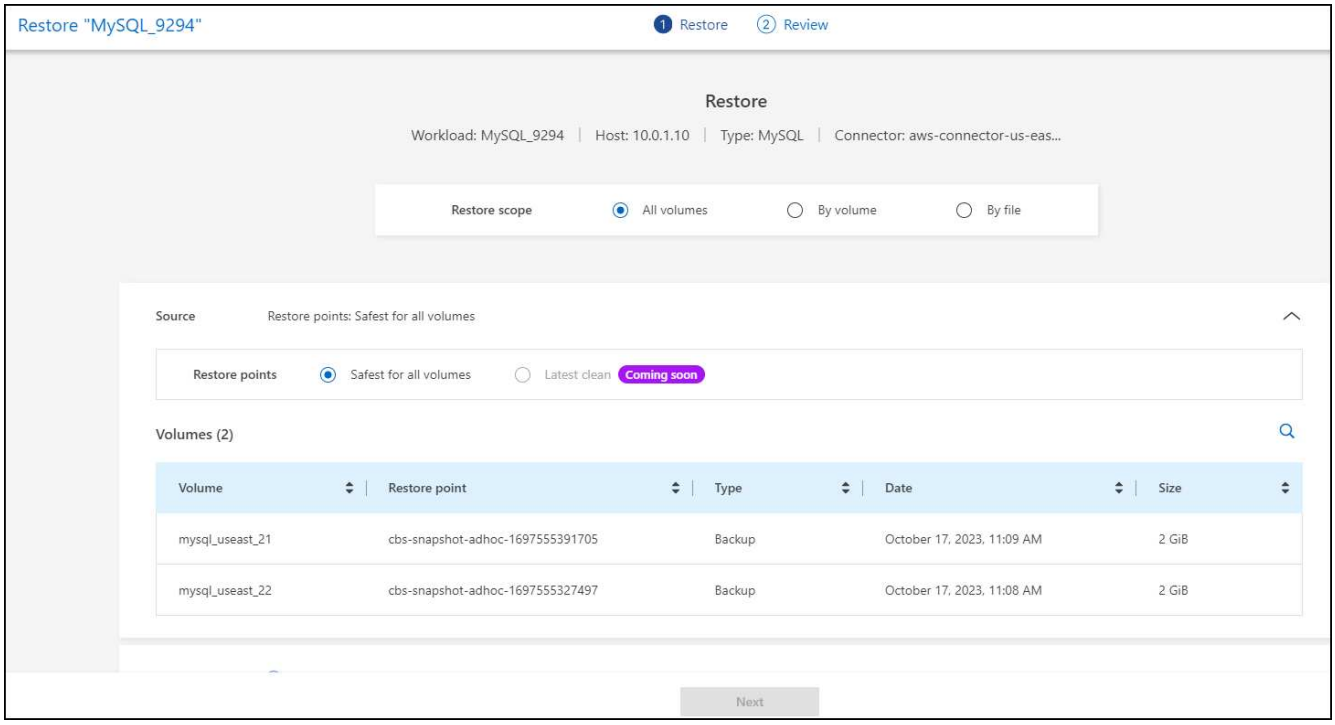
5. **Ripristina ambito**: Selezionare il tipo di ripristino che si desidera completare:
   - Tutti i volumi
   - Per volume
   - Per file: È possibile specificare una cartella o singoli file da ripristinare.

> È possibile selezionare fino a 100 file o una singola cartella.

6. Continuare con una delle seguenti procedure a seconda che sia stata scelta l'applicazione, il volume o il file.

Ripristinare tutti i volumi

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Seleziona un carico di lavoro in stato "Ripristino necessario".
3. Per ripristinare, selezionare **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, selezionare **tutti i volumi**.



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

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione di "più sicuro per tutti i volumi". Ciò significa che tutti i volumi verranno ripristinati in una copia prima del primo attacco sul primo volume rilevato.

6. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Selezionare l'ambiente di lavoro.

b. Selezionare la VM di storage.

c. Selezionare l’aggregato.

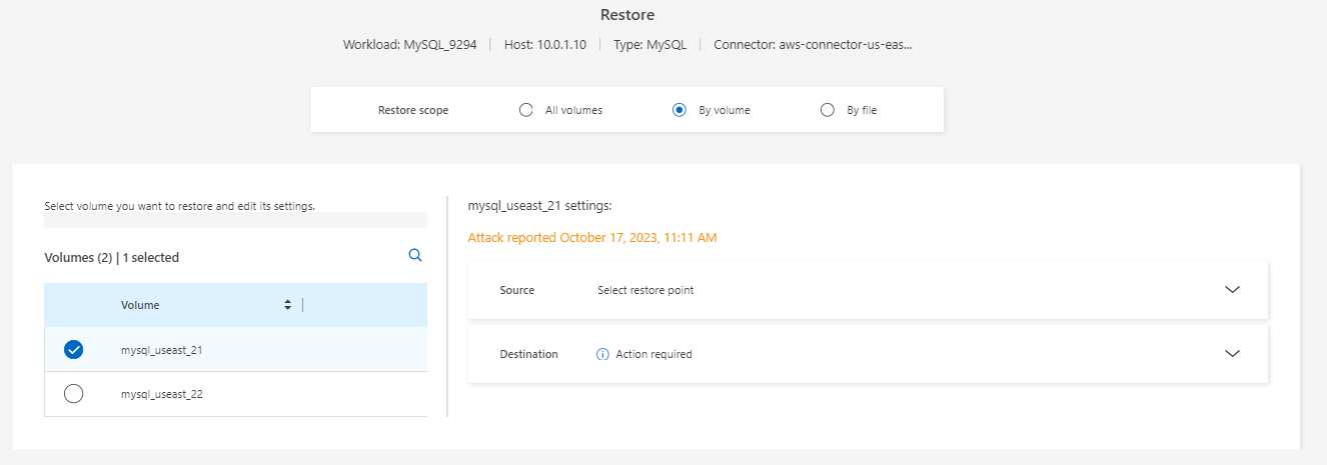
d. Modificare il prefisso del volume che verrà anteposto a tutti i nuovi volumi.

> Il nome del nuovo volume viene visualizzato come prefisso + nome del volume originale + nome del backup + data di backup.

7. Selezionare **Salva**.
8. Selezionare **Avanti**.
9. Rivedere le selezioni.
10. Selezionare **Restore** (Ripristina).
11. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell’operazione si sposta tra gli stati.

Ripristinare un workload dell’applicazione a livello di volume

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Seleziona un carico di lavoro dell’applicazione in stato "Ripristino necessario".
3. Per ripristinare, selezionare **Ripristina**.
4. Nella pagina Ripristina, nell’ambito Ripristina, selezionare **per volume**.



5. Nell’elenco dei volumi, selezionare il volume che si desidera ripristinare.
6. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.
   a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l’ultimo backup poco prima dell’incidente e mostra un’indicazione "consigliata".

7. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Selezionare l’ambiente di lavoro.
   b. Selezionare la VM di storage.
   c. Selezionare l’aggregato.

d. Rivedere il nuovo nome del volume.

> Il nome del nuovo volume viene visualizzato come nome originale del volume + nome del backup + data di backup.

8. Selezionare **Salva**.
9. Selezionare **Avanti**.
10. Rivedere le selezioni.
11. Selezionare **Restore** (Ripristina).
12. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati.

Ripristinare un workload dell'applicazione a livello di file

Prima di ripristinare un workload dell'applicazione a livello di file, è possibile visualizzare un elenco di file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco di file interessati. Quindi, utilizzare la pagina di ripristino per caricare l'elenco e scegliere i file da ripristinare.

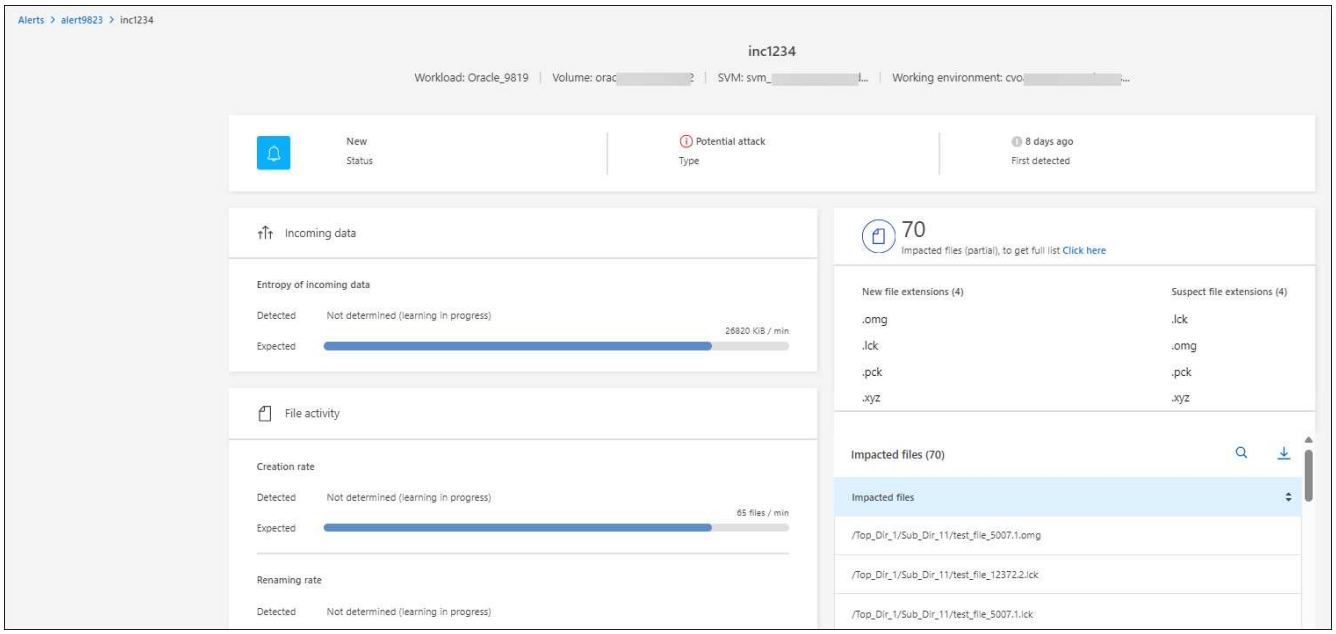
È possibile ripristinare un workload dell'applicazione a livello di file nello stesso ambiente di lavoro o in un ambiente diverso.

Procedura 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 di protezione dal ransomware BlueXP, seleziona **Avvisi**.
2. Nella pagina Avvisi, ordinare i risultati per carico di lavoro per visualizzare gli avvisi per il carico di lavoro dell'applicazione che si desidera ripristinare.
3. Dall'elenco degli avvisi per il carico di lavoro, selezionare un avviso.
4. Per tale avviso, selezionare un singolo incidente.



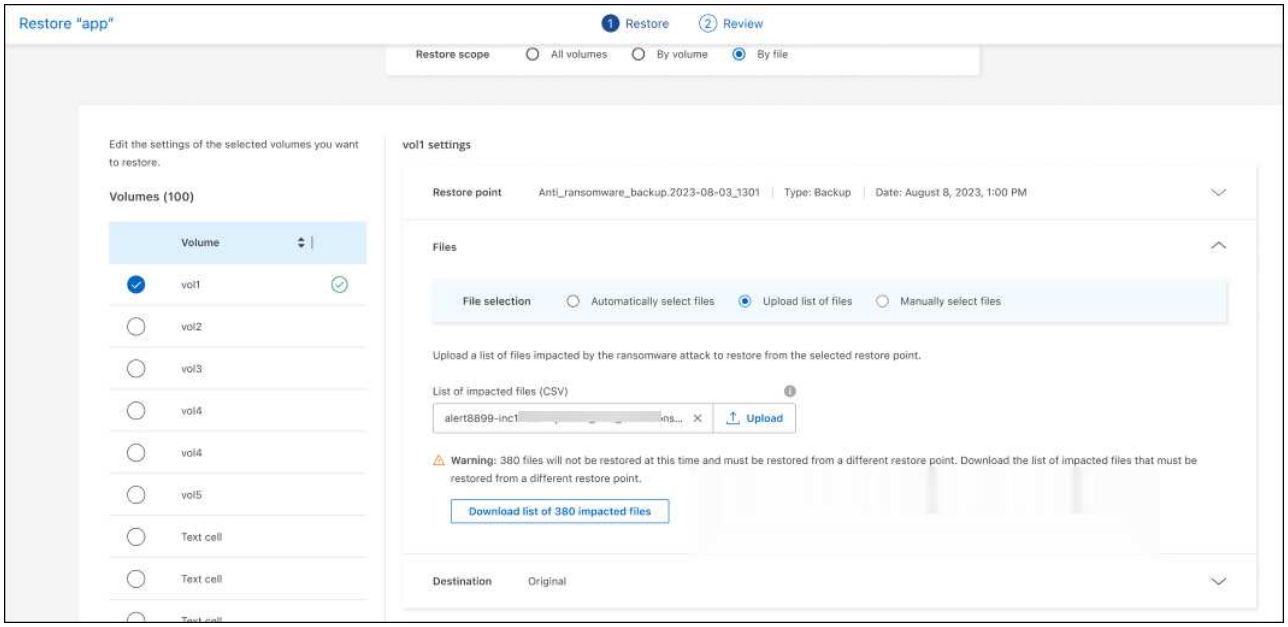
5. Per visualizzare l'elenco completo dei file, selezionare **fare clic qui** nella parte superiore del riquadro file interessati.
6. Per quell'incidente, selezionare l'icona di download e scaricare l'elenco dei file interessati in formato CSV.

Procedura per ripristinare tali file

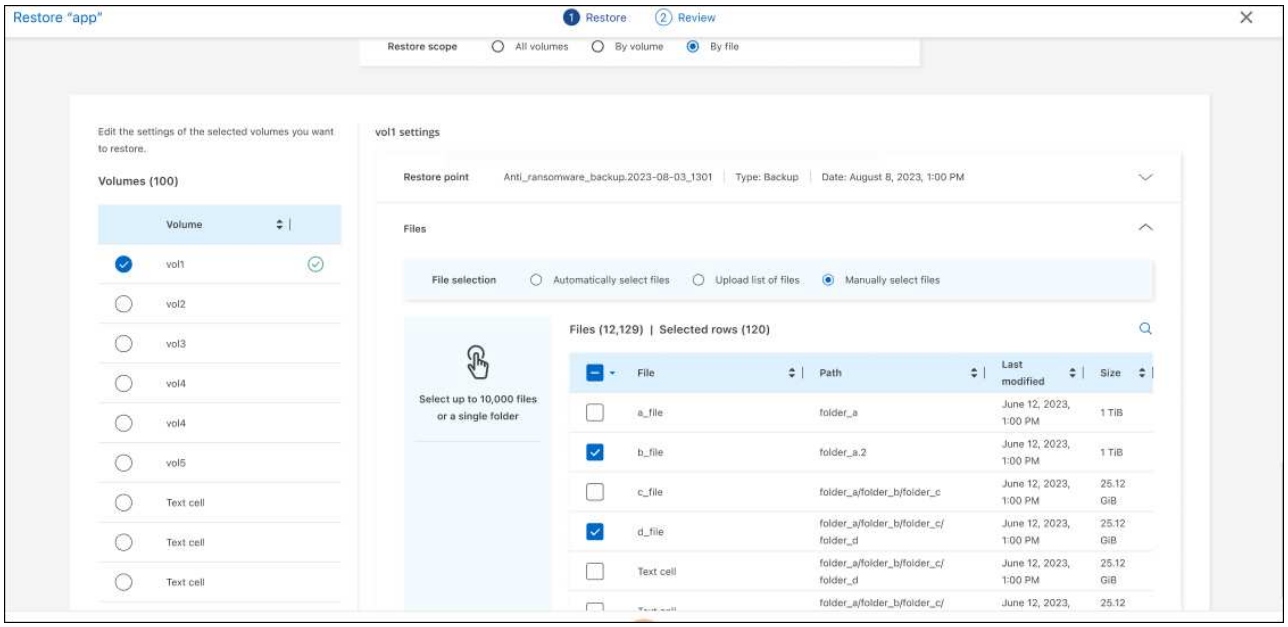
1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Seleziona un carico di lavoro dell'applicazione in stato "Ripristino necessario".
3. Per ripristinare, selezionare **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, selezionare **per file**.
5. Nell'elenco dei volumi, selezionare il volume contenente i file che si desidera ripristinare.
6. **Punto di ripristino**: Selezionare la freccia 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.

> La colonna Reason (motivo) nel riquadro Restore Points (punti di ripristino) mostra il motivo dell'istantanea o del backup come "Scheduled" (programmato) o "Automated Response to ransomware Incident" (Risposta automatizzata all'incidente ransomware).

7. **File**:
   - **Seleziona automaticamente i file**: Lascia che la protezione anti-ransomware di BlueXP selezioni i file da ripristinare.
   - **Carica elenco di file**: Carica un file CSV che contiene l'elenco dei file interessati dalla pagina Avvisi o di quelli in uso. È possibile ripristinare fino a 10.000 file alla volta.



- **Selezione manuale dei file**: Selezionare fino a 10.000 file o una singola cartella da ripristinare.



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

8. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Scegliere dove ripristinare i dati: Percorso di origine originale o percorso alternativo che è possibile specificare.

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

   b. Selezionare l'ambiente di lavoro.

c. Selezionare la VM di storage.

d. Facoltativamente, immettere il percorso.

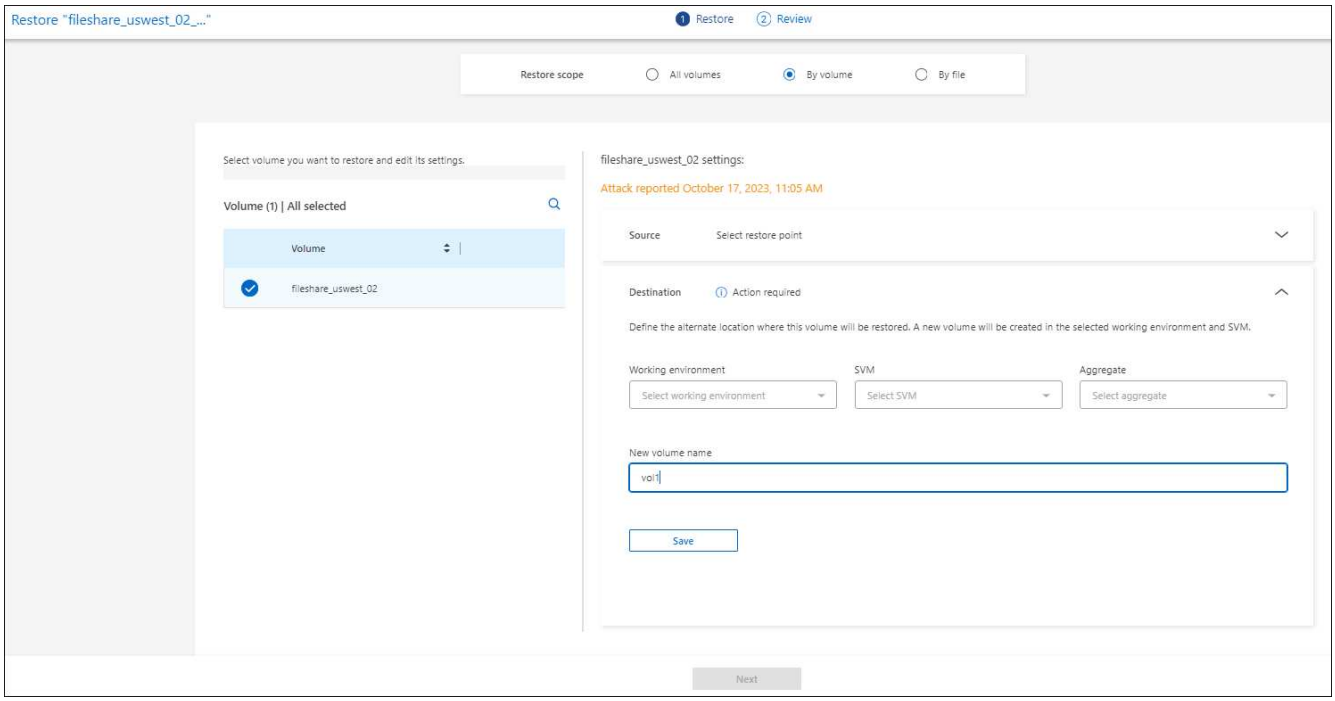
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

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

9. Selezionare **Avanti**.
10. Rivedere le selezioni.
11. Selezionare **Restore** (Ripristina).
12. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati.

Ripristinare una condivisione di file o un datastore

1. Dopo aver selezionato una condivisione di file o un archivio dati da ripristinare, nella pagina Ripristina, nell'ambito Ripristina, selezionare **per volume**.



2. Nell'elenco dei volumi, selezionare il volume che si desidera ripristinare.
3. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.

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

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione "consigliata".

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

   a. Scegliere dove ripristinare i dati: Percorso di origine originale o percorso alternativo che è possibile

specificare.

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

b. Selezionare l'ambiente di lavoro.
c. Selezionare la VM di storage.
d. Facoltativamente, immettere il percorso.

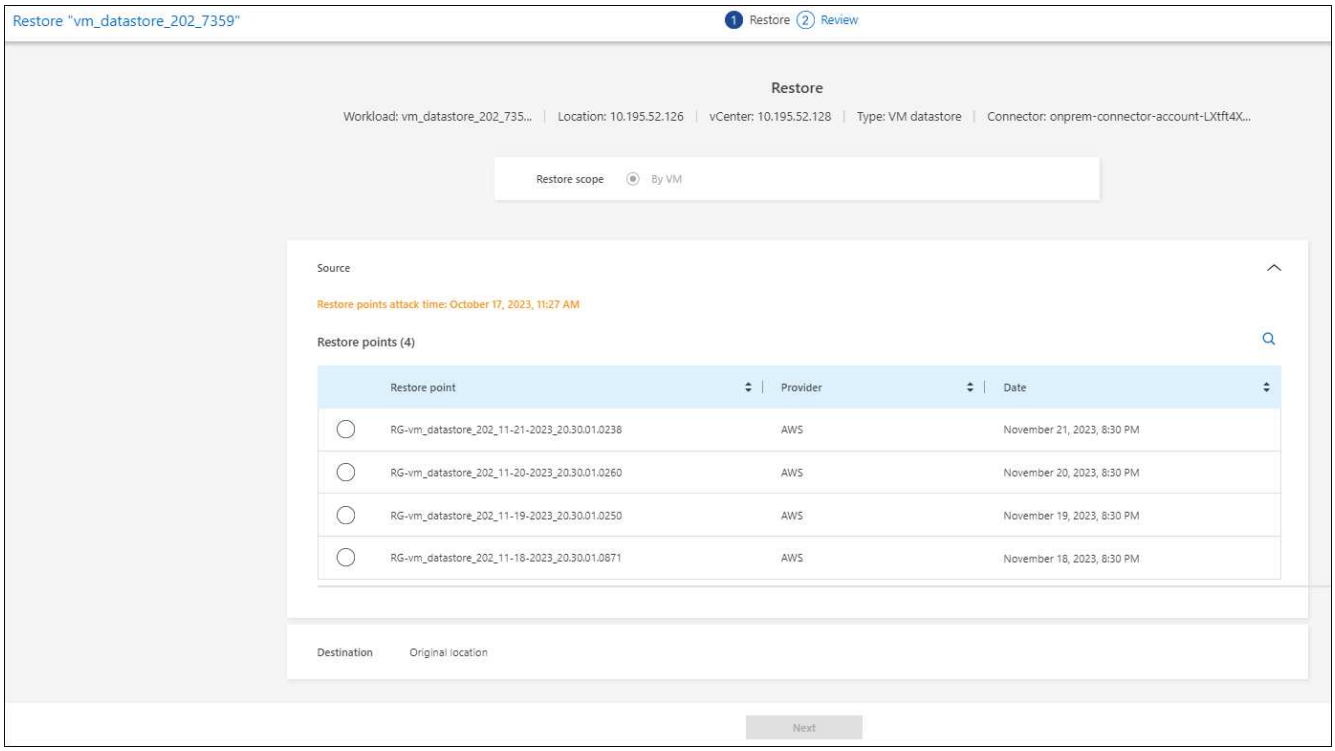
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

5. Selezionare **Salva**.
6. Rivedere le selezioni.
7. Selezionare **Restore** (Ripristina).
8. Dal menu, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione passa attraverso gli stati.

Ripristinare una condivisione di file VM a livello di VM

Nella pagina Recovery (Ripristino), dopo aver selezionato una macchina virtuale da ripristinare, continuare con la procedura descritta di seguito.

1. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.



2. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.
3. **Destinazione**: Alla posizione originale.

4. Selezionare **Avanti**.
5. Rivedere le selezioni.
6. Selezionare **Restore** (Ripristina).
7. Dal menu, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione passa attraverso gli stati.

Scarica i report

È possibile esportare i dati di protezione e scaricare i file CSV o JSON che mostrano i dettagli di protezione, avvisi e ripristino.

Prima di scaricare i file CSV o JSON, è necessario aggiornare i dati, che aggiornano anche i dati che verranno visualizzati nei file.

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

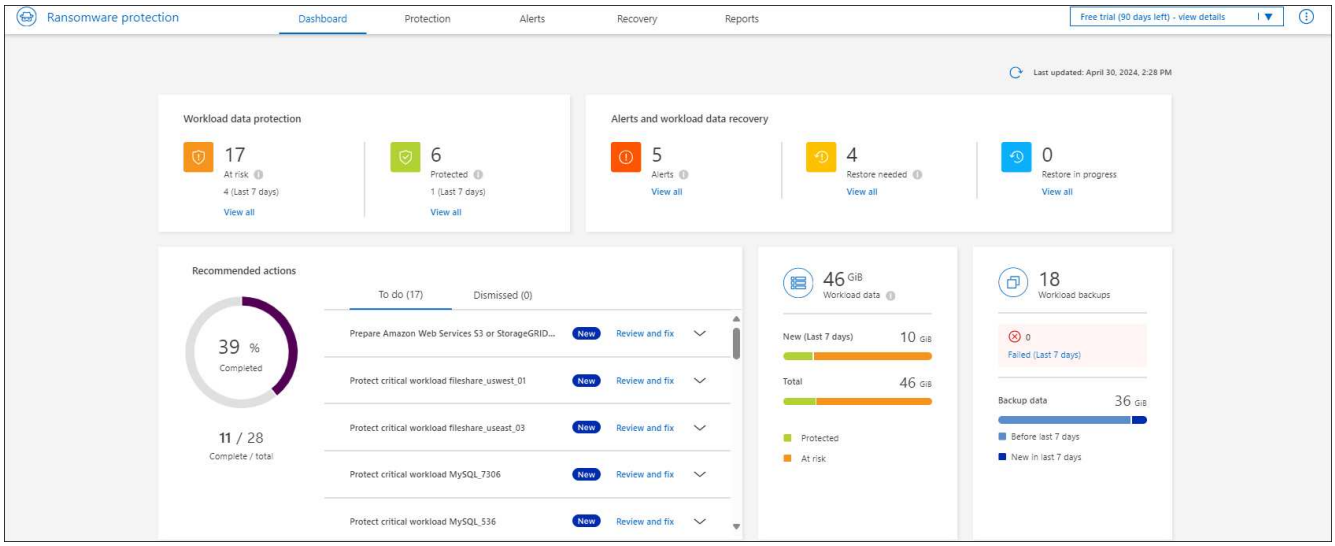
- **Protezione**: Contiene lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale protetto e a rischio.
- **Avvisi**: Include lo stato e i dettagli di tutti gli avvisi, compreso il numero totale di avvisi e istantanee automatiche.
- **Recovery**: Include lo stato e i dettagli di 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 "ripristinato correttamente".
- **Rapporti**: È possibile esportare i dati da una qualsiasi delle pagine e scaricare i file.

Se si scaricano file CSV dalla pagina protezione, Avvisi o Ripristino, i dati visualizzano solo i dati contenuti in tale pagina.

I file CSV includono i dati per tutti i carichi di lavoro su tutti gli ambienti di lavoro BlueXP.

Fasi

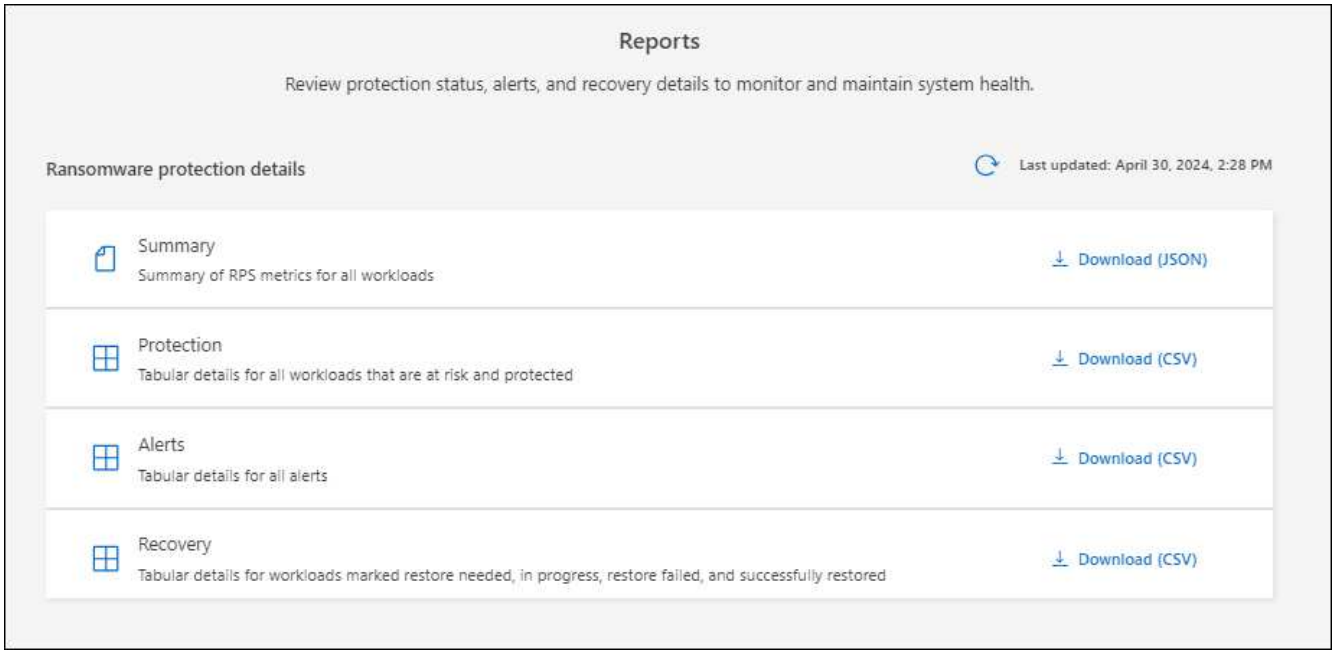
1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.



2.

Dalla dashboard o da un'altra pagina, selezionare **Aggiorna** in alto a destra per aggiornare i dati che verranno visualizzati nei rapporti.

3. Effettuare una delle seguenti operazioni:
   - Nella pagina, selezionare l'opzione **Download** .
   - Dal menu di protezione dal ransomware di BlueXP, seleziona **Report**.
4. Se è stata selezionata l'opzione **rapporti**, selezionare uno dei nomi file CSV preconfigurati e selezionare **Download (CSV)** o **Download (JSON)**.



Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.