Proteggere i carichi di lavoro

BlueXP ransomware protection

NetApp
October 07, 2024

Sommario

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.

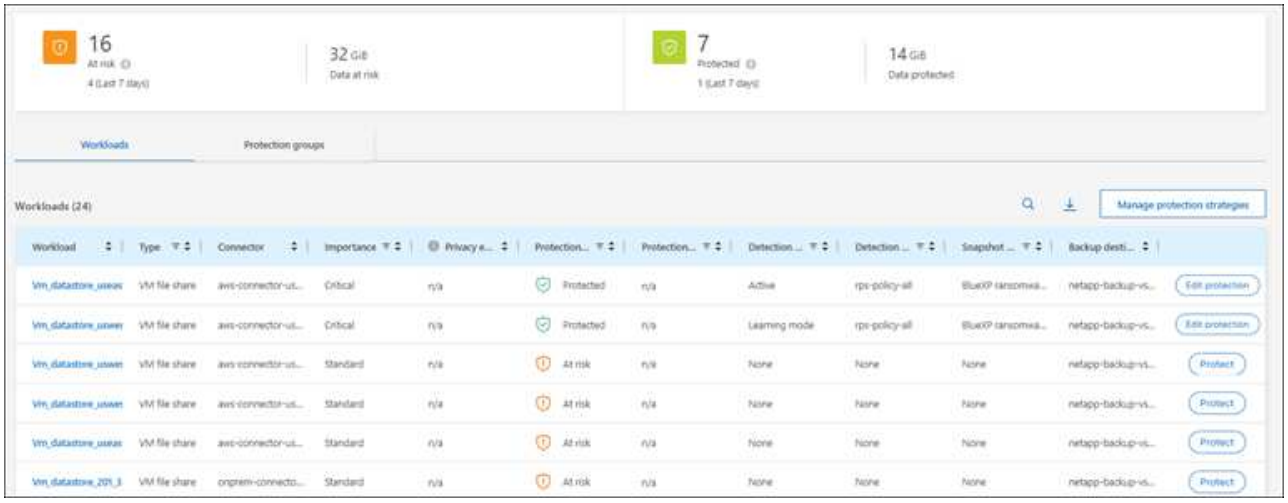
Visualizza la protezione dal ransomware su un carico di lavoro

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
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.

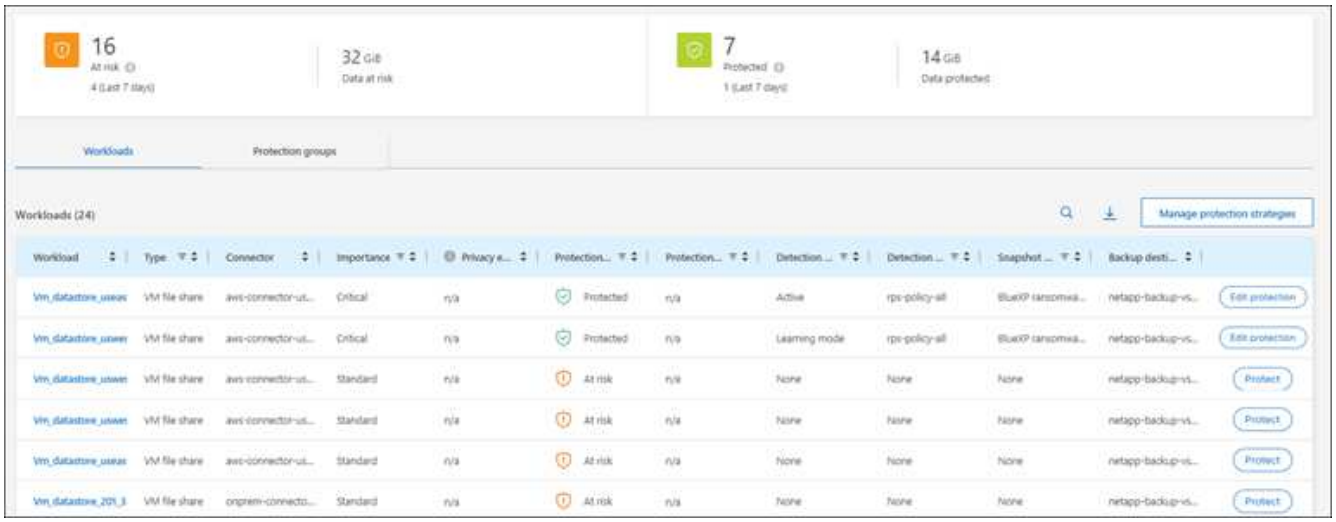
Creare una strategia di protezione dal ransomware (se non disponi di policy di backup o snapshot)

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

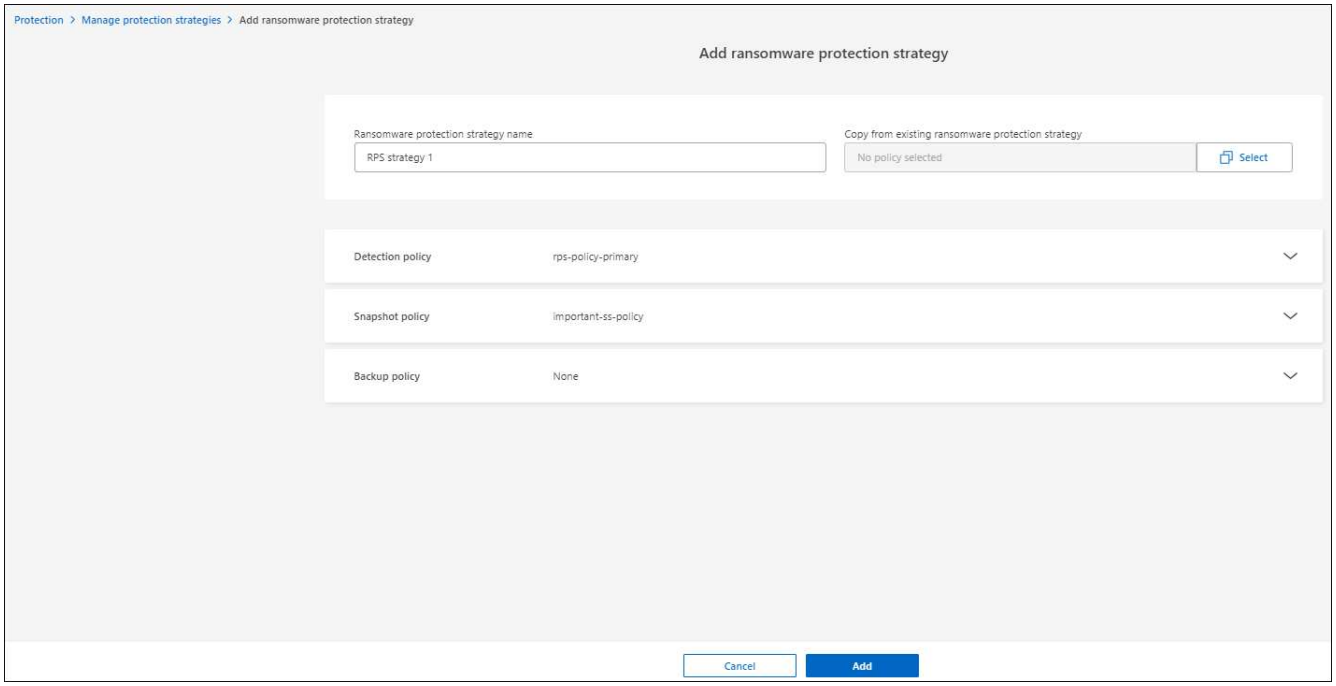
Passaggi per creare una strategia di protezione dal ransomware

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

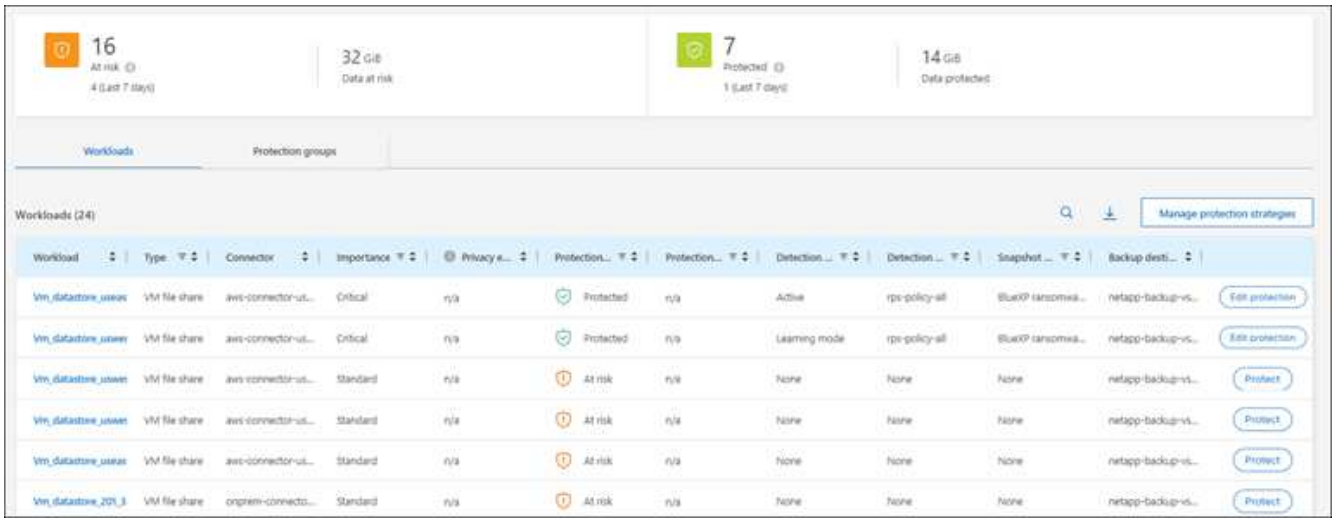
Con la protezione dal ransomware di BlueXP puoi assegnare una policy di rilevamento del ransomware a workload che dispongono già di policy di backup e snapshot, gestite in altri prodotti o servizi NetApp. Il criterio di rilevamento non modifica i criteri gestiti in altri prodotti.

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

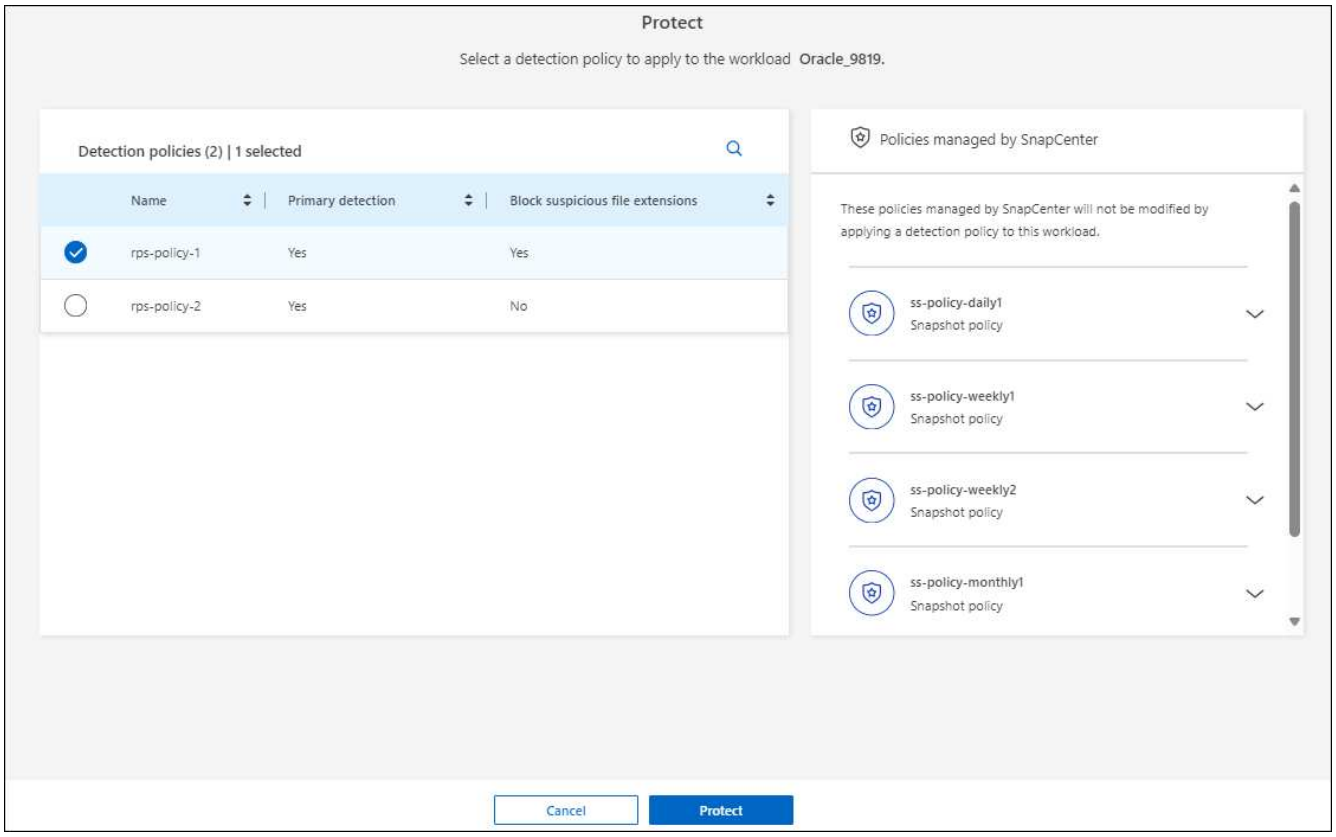
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



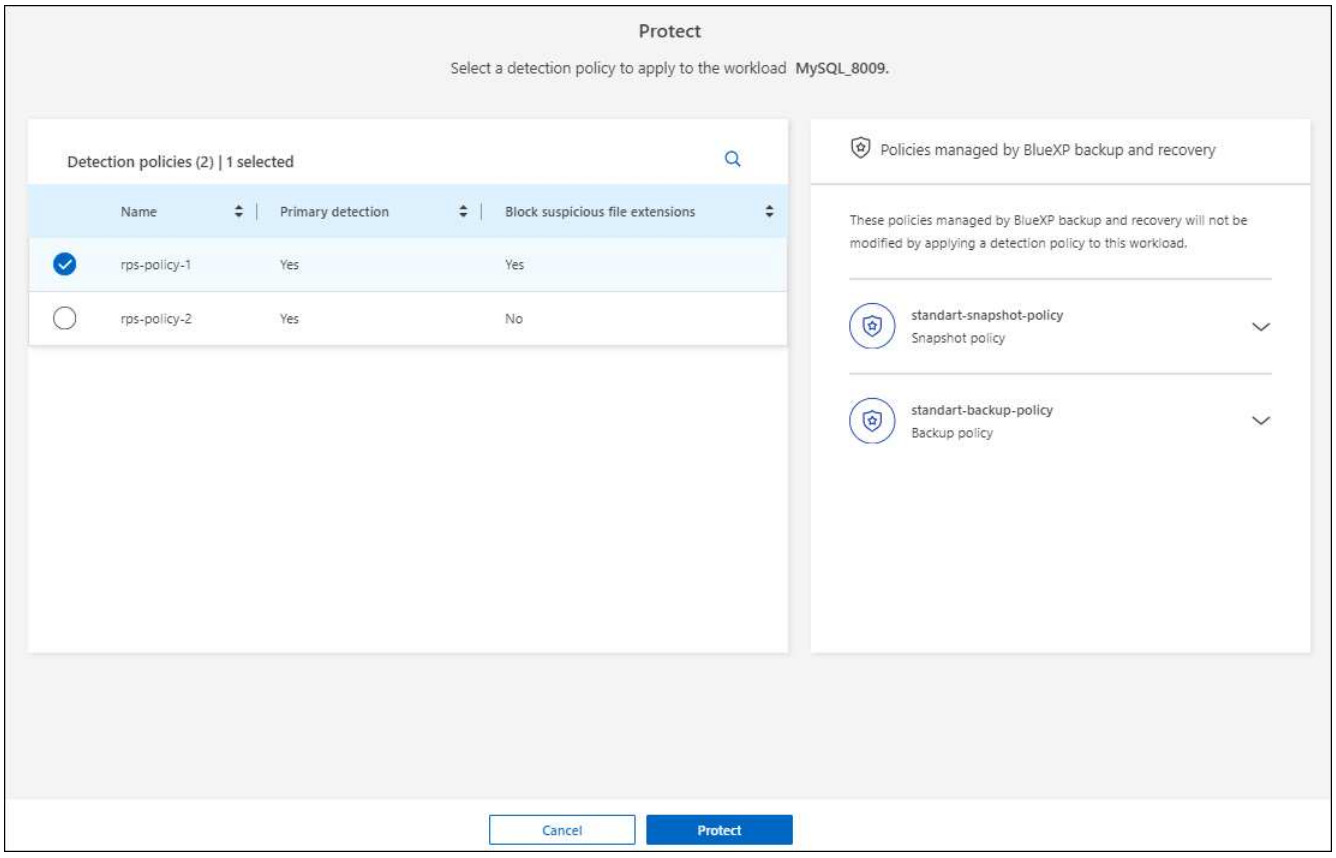
2. Nella pagina protezione, selezionare un carico di lavoro e selezionare **Proteggi**.

   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

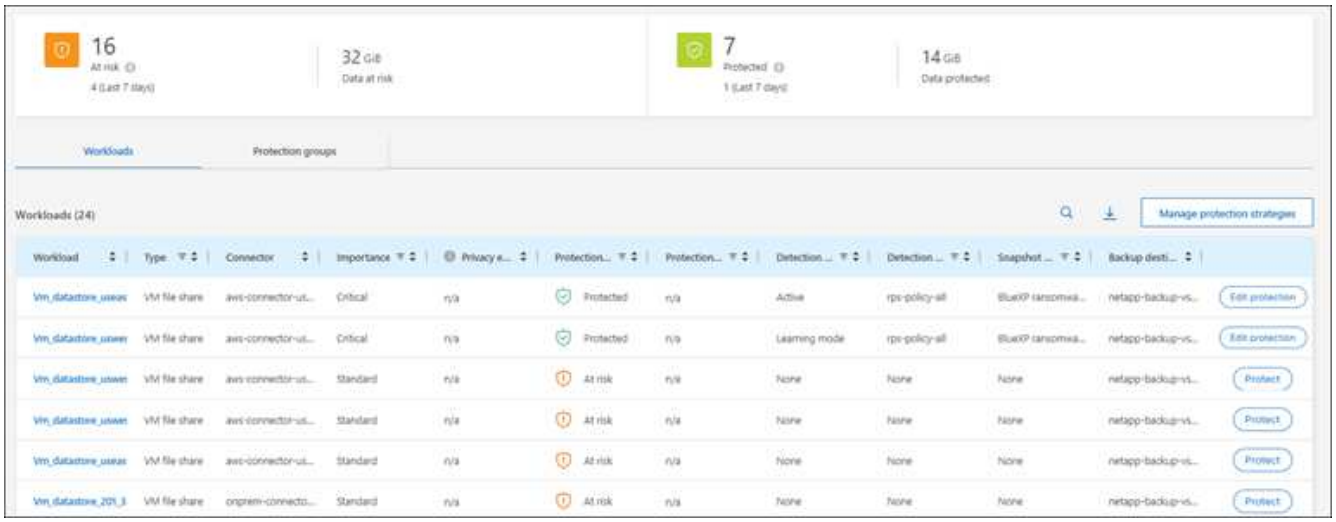
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, nella riga del carico di lavoro, selezionare **Modifica protezione**.
3. Nella pagina Criteri, fare clic sulla freccia verso il basso relativa al criterio che si desidera assegnare per rivedere i dettagli.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

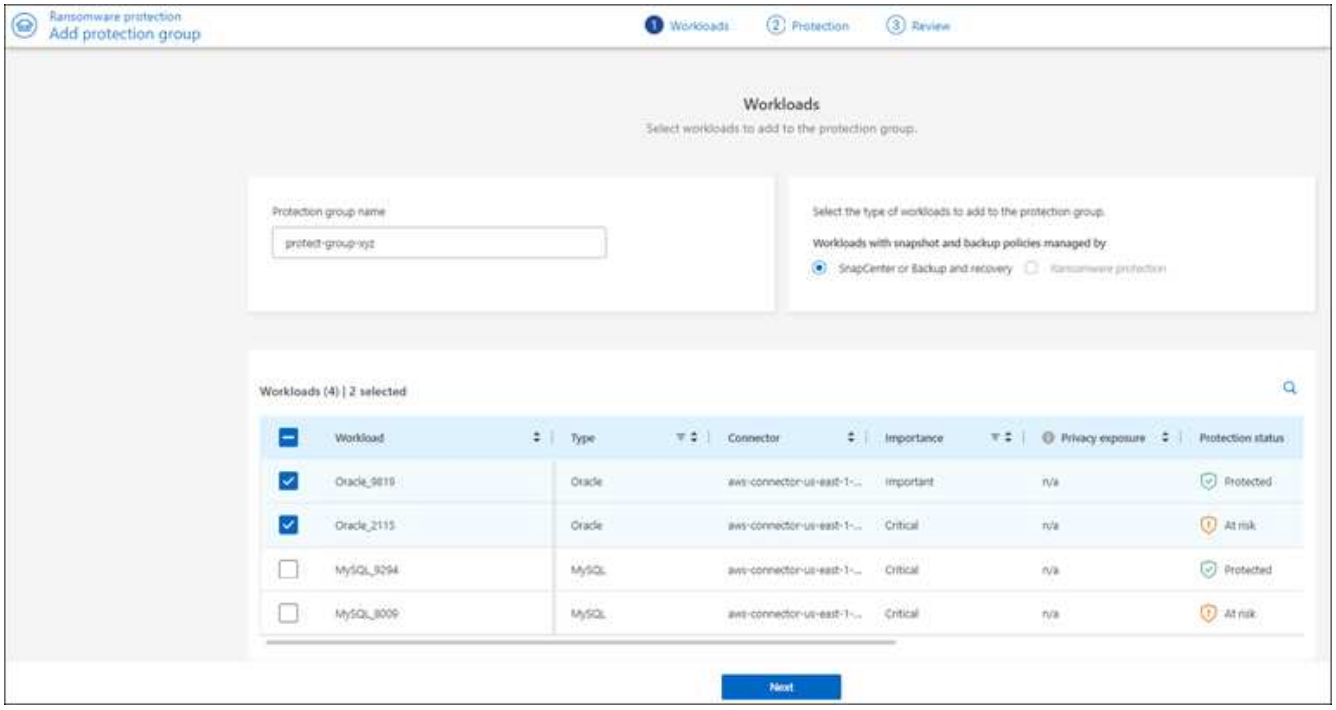
Fasi

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



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

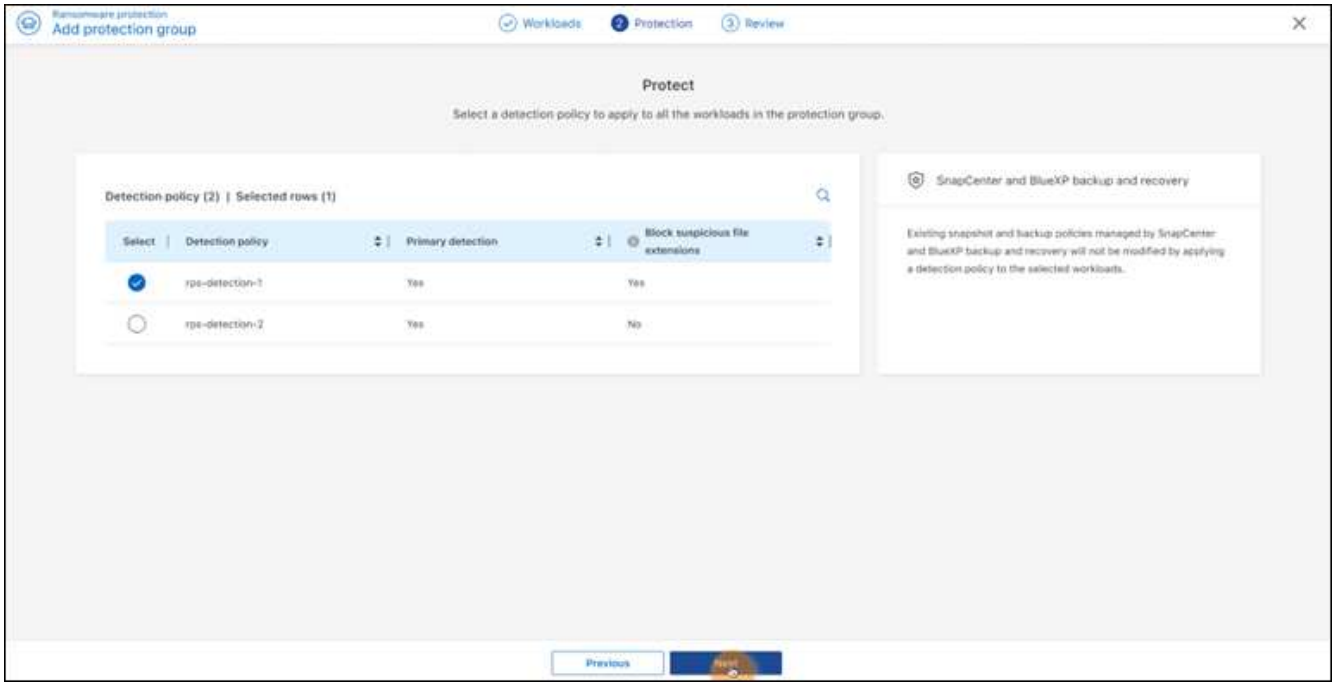
3. Selezionare **Aggiungi**.



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

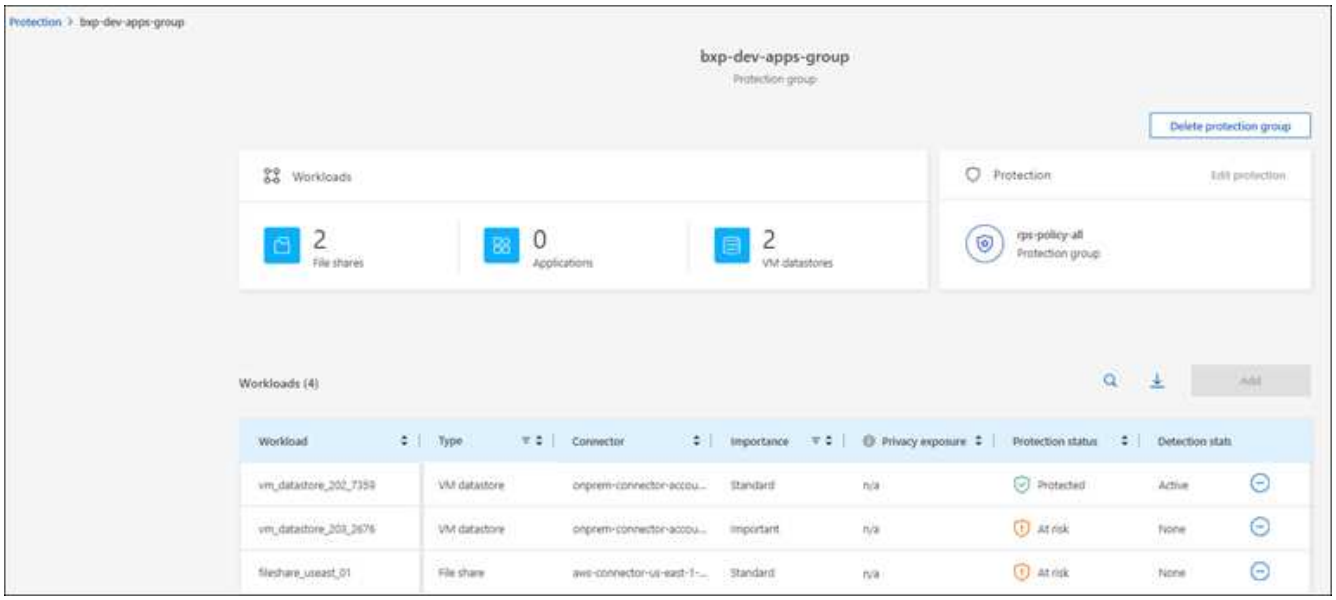
In seguito, potrebbe essere necessario aggiungere altri carichi di lavoro a un gruppo esistente.

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.

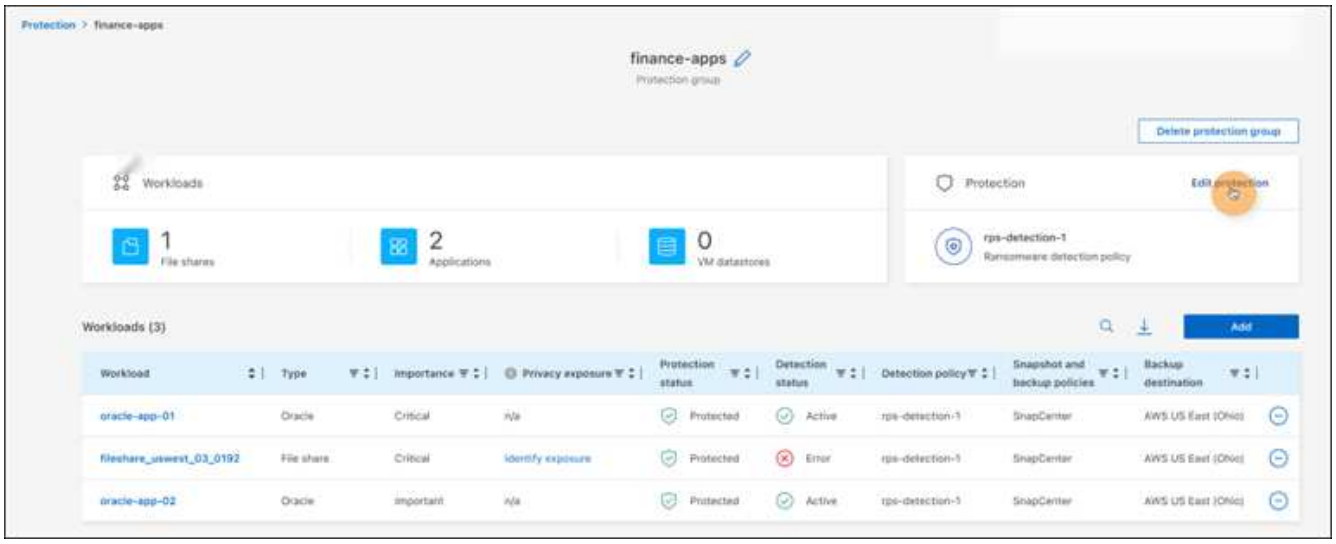
5. Selezionare i carichi di lavoro aggiuntivi da aggiungere al gruppo.
6. Selezionare **Salva**.

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**.



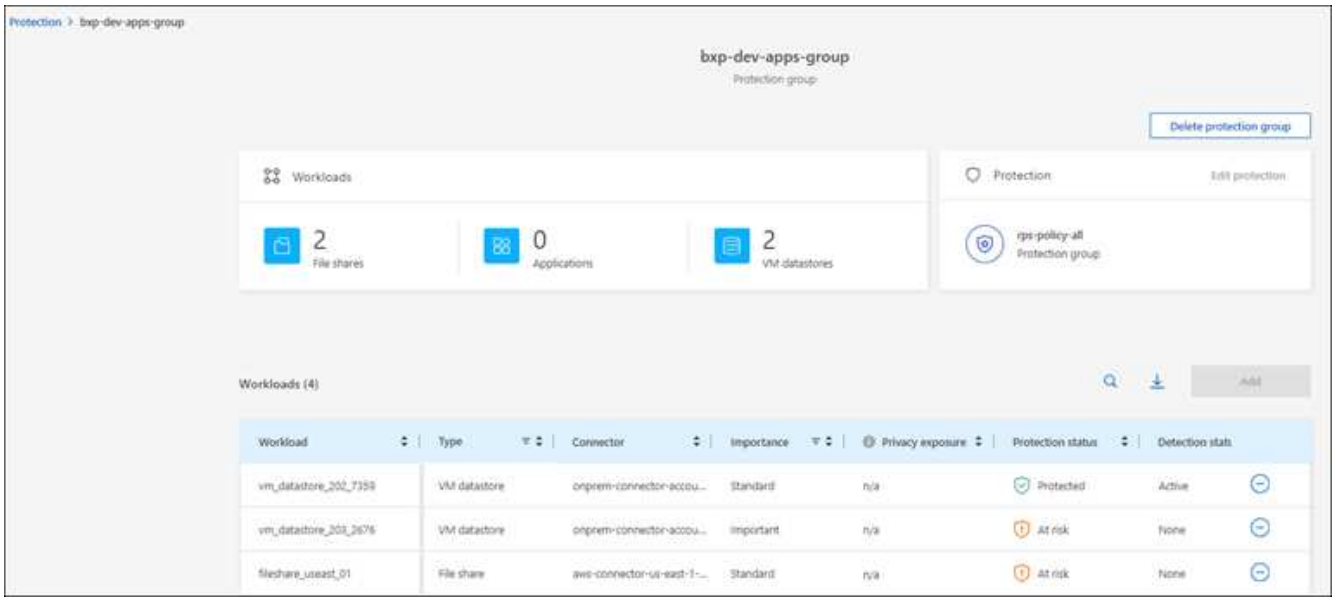
3. Dal riquadro protezione, selezionare **Modifica protezione**.
4. Selezionare o aggiungere un criterio di rilevamento a questo gruppo.

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.



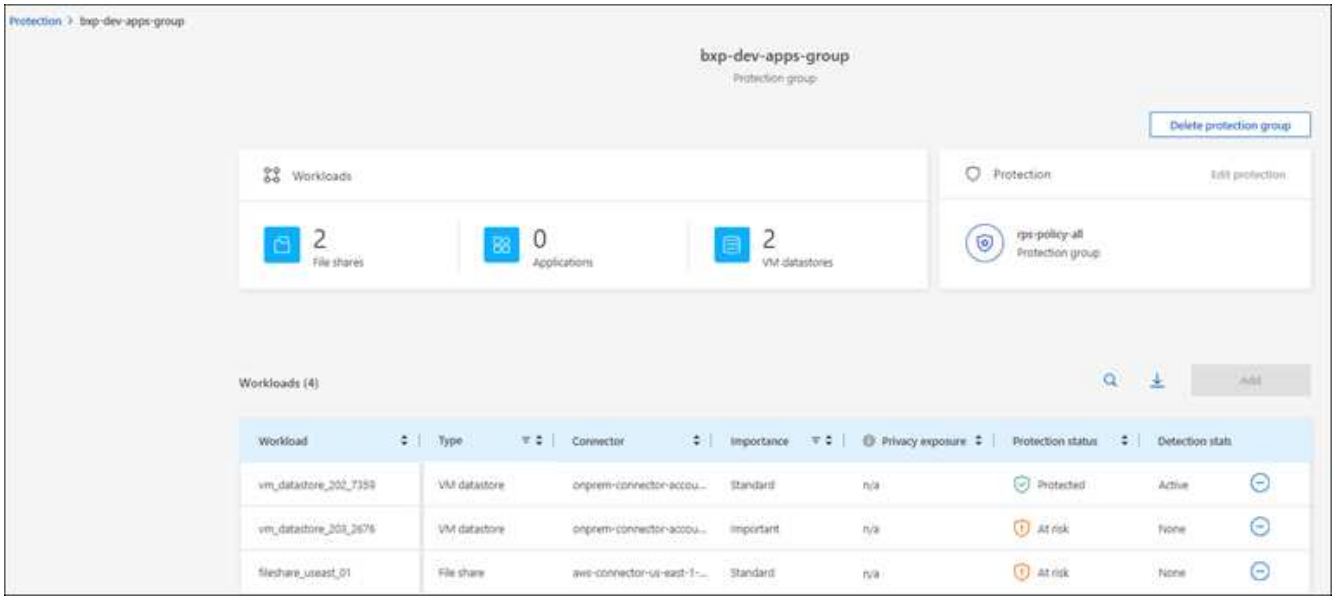
4. Dalla pagina Gruppo protezione selezionato, selezionare il carico di lavoro che si desidera rimuovere dal gruppo e selezionare l'opzione *azioni*•••.
5. Dal menu azioni, selezionare **Rimuovi carico di lavoro**.
6. Confermare che si desidera rimuovere il carico di lavoro e selezionare **Rimuovi**.

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**.

Informazioni sul copyright

Informazioni sul marchio commerciale