Documentazione sulla protezione ransomware BlueXP

BlueXP ransomware protection

NetApp
October 07, 2024

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

Sommario

Documentazione sulla protezione ransomware BlueXP . . . 1
Note di release: Novità della protezione dal ransomware BlueXP . . . 2
30 settembre 2024 . . . 2
2 settembre 2024 . . . 2
5 agosto 2024 . . . 3
1 luglio 2024 . . . 3
10 giugno 2024 . . . 3
14 maggio 2024 . . . 4
5 marzo 2024 . . . 5
6 ottobre 2023 . . . 6
Inizia subito . . . 7
Scopri di più sulla protezione ransomware di BlueXP . . . 7
Prerequisiti della protezione dal ransomware di BlueXP . . . 12
Avvio rapido per la protezione dal ransomware di BlueXP . . . 14
Imposta la protezione dal ransomware BlueXP . . . 15
Accedi alla protezione dal ransomware di BlueXP . . . 16
Imposta una licenza per la protezione dal ransomware di BlueXP . . . 17
Rileva i carichi di lavoro nella protezione dal ransomware di BlueXP . . . 25
Configurare le impostazioni di protezione dal ransomware BlueXP . . . 27
Domande frequenti sulla protezione dal ransomware BlueXP . . . 37
Utilizzare la protezione ransomware BlueXP . . . 41
Utilizzare la protezione ransomware BlueXP . . . 41
Visualizza lo stato dei carichi di lavoro con un’occhiata utilizzando la dashboard . . . 41
Proteggere i carichi di lavoro . . . 46
Rispondi a un avviso ransomware rilevato . . . 62
Ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti) . . . 67
Scarica i report . . . 77
Conoscenza e supporto . . . 79
Registrati per ricevere assistenza . . . 79
Richiedi assistenza . . . 83
Riferimento . . . 89
Privileges per il controllo degli accessi in base al ruolo della protezione ransomware BlueXP . . . 89
Note legali . . . 91
Copyright . . . 91
Marchi . . . 91
Brevetti . . . 91
Direttiva sulla privacy . . . 91
Open source . . . 91

Documentazione sulla protezione ransomware BlueXP

Note di release: Novità della protezione dal ransomware BlueXP

Scopri le novità di BlueXP ransomware Protection.

30 settembre 2024

Questa versione della protezione ransomware di BlueXP include il seguente aggiornamento.

- **Raggruppamento personalizzato dei carichi di lavoro delle condivisioni di file**: Con questa versione, è ora possibile raggruppare le condivisioni di file in gruppi per semplificare la protezione del patrimonio dati. Il servizio può proteggere tutti i volumi in un gruppo allo stesso tempo. In precedenza, era necessario proteggere ciascun volume separatamente. "Scopri di più sul raggruppamento dei carichi di lavoro di condivisioni di file nelle strategie di protezione dal ransomware".

2 settembre 2024

Questa versione della protezione ransomware di BlueXP include i seguenti aggiornamenti.

- **Valutazione dei rischi di sicurezza di Digital Advisor**: La protezione anti-ransomware di BlueXP ora raccoglie informazioni sui rischi di sicurezza elevati e critici correlati a un cluster di NetApp Digital Advisor. Se viene rilevato un rischio, la protezione anti-ransomware di BlueXP fornisce una raccomandazione nel riquadro **azioni consigliate** della dashboard: "Correggere una vulnerabilità nota alla sicurezza nel <name> del cluster". Dal suggerimento sul dashboard, fare clic su **Rivedi e correggi** suggerisce di rivedere Digital Advisor e un articolo CVE (Common Vulnerability & Exposure) per risolvere il rischio per la protezione. In caso di più rischi per la protezione, consultare le informazioni in Digital Advisor.

  Fare riferimento alla "Documentazione di Digital Advisor".

- **Backup su Google Cloud Platform**: Con questa release, è possibile impostare una destinazione di backup su un bucket Google Cloud Platform. In precedenza, potevi aggiungere destinazioni di backup solo a NetApp StorageGRID, Amazon Web Services e Microsoft Azure.

  "Scopri di più sulla configurazione delle impostazioni di protezione dal ransomware BlueXP ".

- **Supporto per Google Cloud Platform**: Il servizio ora supporta Cloud Volumes ONTAP per Google Cloud Platform per la protezione dello storage. In precedenza, il servizio supportava solo Cloud Volumes ONTAP per Amazon Web Services e Microsoft Azure con NAS on-premise.

  "Scopri la protezione dal ransomware BlueXP e le origini dati supportate, le destinazioni di backup e gli ambienti di lavoro".

- **Role-based access control**: Ora puoi limitare l'accesso ad attività specifiche grazie al role-based access control (RBAC). La protezione ransomware BlueXP utilizza due ruoli di BlueXP : BlueXP account Admin e non-account Admin (Viewer).

  Per informazioni dettagliate sulle azioni che ogni ruolo può eseguire, vedere "Privileges per il controllo degli accessi in base al ruolo".

5 agosto 2024

Questa versione della protezione ransomware di BlueXP include il seguente aggiornamento.

- **Rilevamento delle minacce con Splunk Cloud**: Puoi inviare automaticamente i dati al tuo sistema di gestione degli eventi e della sicurezza (SIEM) per l'analisi e il rilevamento delle minacce. Con le release precedenti, puoi selezionare solo l'AWS Security Hub come tuo SIEM. Con questa release, puoi selezionare AWS Security Hub o Splunk Cloud come tuo SIEM.

  "Scopri di più sulla configurazione delle impostazioni di protezione dal ransomware BlueXP ".

1 luglio 2024

Questa versione della protezione dal ransomware di BlueXP include i seguenti aggiornamenti:

- **Bring Your Own License (BYOL)**: Con questa release, puoi utilizzare una licenza BYOL, che è un file di licenza NetApp (NLF) che ottieni dal tuo rappresentante di vendita NetApp

  "Ulteriori informazioni sull'impostazione delle licenze".

- **Ripristina il workload dell'applicazione a livello di file**: Prima di ripristinare il workload di un'applicazione a livello di file, è possibile visualizzare un elenco di file che potrebbero essere stati coinvolti da un attacco e identificare quelli che si desidera ripristinare. Puoi permettere alla protezione anti-ransomware di BlueXP di scegliere i file da ripristinare, caricare un file CSV che elenca tutti i file interessati da un avviso o identificare manualmente i file da ripristinare.

  > Con questa versione, se tutti i connettori BlueXP in un account non utilizzano Podman, la funzionalità di ripristino dei singoli file è attivata. In caso contrario, è disabilitato per quell'account.

  "Scopri di più sul ripristino in seguito a un attacco ransomware".

- **Scaricare un elenco dei file interessati** prima di ripristinare il carico di lavoro di un'applicazione a livello di file. È ora possibile accedere alla pagina Avvisi per scaricare un elenco di file interessati in un file CSV, quindi utilizzare la pagina di ripristino per caricare il file CSV.

  "Ulteriori informazioni sul download dei file interessati prima di ripristinare un'applicazione".

- **Elimina piano di protezione**: Con questa release, ora puoi eliminare una strategia di protezione dal ransomware.

  "Scopri di più su protezione dei carichi di lavoro e gestione delle strategie di protezione dal ransomware".

10 giugno 2024

Questa versione della protezione dal ransomware di BlueXP include i seguenti aggiornamenti:

- **Blocco delle copie Snapshot sullo storage primario**: Abilita questa opzione per bloccare le copie Snapshot sullo storage primario in modo che non possano essere modificate o eliminate per un certo periodo di tempo anche in caso di attacco ransomware che gestisca la destinazione storage di backup.

  "Scopri di più sulla protezione dei carichi di lavoro e sull'abilitazione del blocco del backup in una strategia

di protezione dal ransomware".

- **Questa versione supporta Cloud Volumes ONTAP per Microsoft Azure** come ambiente di lavoro oltre a Cloud Volumes ONTAP per AWS e ONTAP NAS on-premise.

  "Avvio rapido di Cloud Volumes ONTAP in Azure"

  "Scopri di più sulla protezione ransomware di BlueXP".

- **Microsoft Azure aggiunto come destinazione di backup**. Ora puoi aggiungere Microsoft Azure come destinazione di backup insieme ad AWS e NetApp StorageGRID.

  "Ulteriori informazioni su come configurare le impostazioni di protezione".

14 maggio 2024

Questa release è la release di disponibilità generale della protezione dal ransomware di BlueXP. Include i seguenti aggiornamenti:

- **Aggiornamenti sulle licenze**: Puoi iscriverti a una prova gratuita di 90 giorni. A breve sarai in grado di acquistare un abbonamento pay-as-you-go con Amazon Web Services Marketplace o Bring Your Own NetApp License.

  "Ulteriori informazioni sull'impostazione delle licenze".

- **Protocollo CIFS**: Il servizio ora supporta ONTAP e Cloud Volumes ONTAP on-premise negli ambienti di lavoro AWS utilizzando protocolli NFS e CIFS. La release precedente supportava solo il protocollo NFS.
- **Dettagli del carico di lavoro**: Questa versione fornisce maggiori dettagli sulle informazioni sul carico di lavoro dalle pagine protezione e altre pagine per una migliore valutazione della protezione del carico di lavoro. Dai dettagli del carico di lavoro, è possibile esaminare il criterio attualmente assegnato e le destinazioni di backup configurate.

  "Ulteriori informazioni sulla visualizzazione dei dettagli sul carico di lavoro sono disponibili nelle pagine protezione".

- **Protezione e ripristino coerenti con le applicazioni e con le VM**: È ora possibile eseguire una protezione coerente con le applicazioni con il software NetApp SnapCenter e una protezione coerente con le VM con il plug-in SnapCenter per VMware vSphere, ottenendo uno stato di inattività e coerente per evitare potenziali perdite di dati in un secondo momento se è necessario il ripristino. Se è necessario il ripristino, è possibile ripristinare l'applicazione o la VM in uno qualsiasi degli stati disponibili in precedenza.

  "Scopri di più sulla protezione dei carichi di lavoro".

- **Strategie di protezione dal ransomware**: Se le policy di backup o snapshot non esistono sul workload, puoi creare una strategia di protezione dal ransomware, che può includere le seguenti policy create in questo servizio:
  - Policy di Snapshot
  - Policy di backup
  - Policy di rilevamento

    "Scopri di più sulla protezione dei carichi di lavoro".

- **L'attivazione del rilevamento delle minacce** è ora disponibile utilizzando un sistema SIEM (Security and Event Management) di terze parti. Il dashboard ora mostra una nuova raccomandazione per "attivare il rilevamento delle minacce" che può essere configurata nella pagina Impostazioni.

  "Ulteriori informazioni sulla configurazione delle opzioni di impostazione".

- **Eliminare gli avvisi falsi positivi**: Dalla scheda Avvisi, è ora possibile eliminare i falsi positivi o decidere di recuperare immediatamente i dati.

  "Scopri di più su come rispondere a un avviso ransomware".

- **Nuovi stati di rilevamento** vengono visualizzati nella pagina protezione, che mostra lo stato del rilevamento ransomware applicato al carico di lavoro.

  "Scopri di più sulla protezione dei carichi di lavoro e sulla visualizzazione degli stati di protezione".

- **Scaricare i file CSV** dalle pagine protezione, Avvisi e Ripristino.

  "Ulteriori informazioni sul download di file CSV dal dashboard e da altre pagine".

- Il collegamento **Visualizza documentazione** è ora incluso nell'interfaccia utente. È possibile accedere a questa documentazione dal pannello verticale **azioni** opzione. Seleziona **Novità** per visualizzare i dettagli nelle Note sulla versione o **documentazione** per visualizzare la home page della documentazione relativa alla protezione dal ransomware di BlueXP.
- **Backup e recovery di BlueXP**: Il servizio di backup e recovery di BlueXP non deve più essere già abilitato nell'ambiente di lavoro. Vedere "prerequisiti". Il servizio di protezione dal ransomware di BlueXP aiuta a configurare una destinazione di backup tramite l'opzione Settings. Vedere "Configurare le impostazioni".
- **Opzione Impostazioni**: Ora puoi configurare le destinazioni di backup nelle impostazioni di protezione dal ransomware di BlueXP.

  "Ulteriori informazioni sulla configurazione delle opzioni di impostazione".

5 marzo 2024

Questa release di anteprima della protezione dal ransomware di BlueXP include i seguenti aggiornamenti:

- **Gestione dei criteri di protezione**: Oltre a utilizzare criteri predefiniti, è ora possibile creare criteri. "Ulteriori informazioni sulla gestione dei criteri".
- **Immutabilità nello storage secondario (DataLock)**: È ora possibile rendere immutabile il backup nello storage secondario utilizzando la tecnologia NetApp DataLock nell'archivio oggetti. "Ulteriori informazioni sulla creazione di criteri di protezione".
- **Backup automatico su NetApp StorageGRID**: Oltre a utilizzare AWS, è ora possibile scegliere StorageGRID come destinazione di backup. "Ulteriori informazioni sulla configurazione delle destinazioni di backup".
- **Caratteristiche aggiuntive per esaminare i potenziali attacchi**: Ora puoi visualizzare ulteriori dettagli forensi per analizzare il potenziale attacco rilevato. "Scopri di più sulla risposta a un avviso ransomware rilevato".
- **Processo di ripristino**. Il processo di ripristino è stato migliorato. Ora è possibile ripristinare volume per volume o tutti i volumi per un carico di lavoro. "Scopri di più sul ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti)".

"Scopri di più sulla protezione ransomware di BlueXP".

6 ottobre 2023

Il servizio di protezione dal ransomware BlueXP è una soluzione SaaS per la protezione dei dati, il rilevamento di potenziali attacchi e il recovery dei dati da un attacco ransomware.

Per la versione di anteprima, il servizio protegge i carichi di lavoro basati sull'applicazione dei datastore Oracle, MySQL, VM e file share nello storage NAS on-premise, oltre che in Cloud Volumes ONTAP su AWS (utilizzando il protocollo NFS) nelle singole organizzazioni BlueXP ed esegue il backup dei dati nel cloud storage Amazon Web Services.

Il servizio di protezione dal ransomware di BlueXP offre un utilizzo completo di diverse tecnologie NetApp per permettere all'amministratore della sicurezza dei dati o al Security Operations Engineer di raggiungere i seguenti obiettivi:

- Visualizza rapidamente la protezione dal ransomware su tutti i tuoi workload.
- Ottieni informazioni dettagliate sulle raccomandazioni relative alla protezione dal ransomware
- Migliora il livello di protezione in base alle raccomandazioni di protezione dal ransomware BlueXP.
- Assegna policy di protezione dal ransomware per proteggere i tuoi carichi di lavoro principali e i dati ad alto rischio dagli attacchi ransomware.
- Monitora la salute dei carichi di lavoro contro gli attacchi ransomware che cercano anomalie nei dati.
- Valutare rapidamente l'impatto degli incidenti ransomware sul carico di lavoro.
- Esegui il ripristino in maniera intelligente dai ransomware eseguendo il ripristino dei dati e garantendo che non si verifichi una nuova infezione da tali dati.

"Scopri di più sulla protezione ransomware di BlueXP".

Inizia subito

Scopri di più sulla protezione ransomware di BlueXP

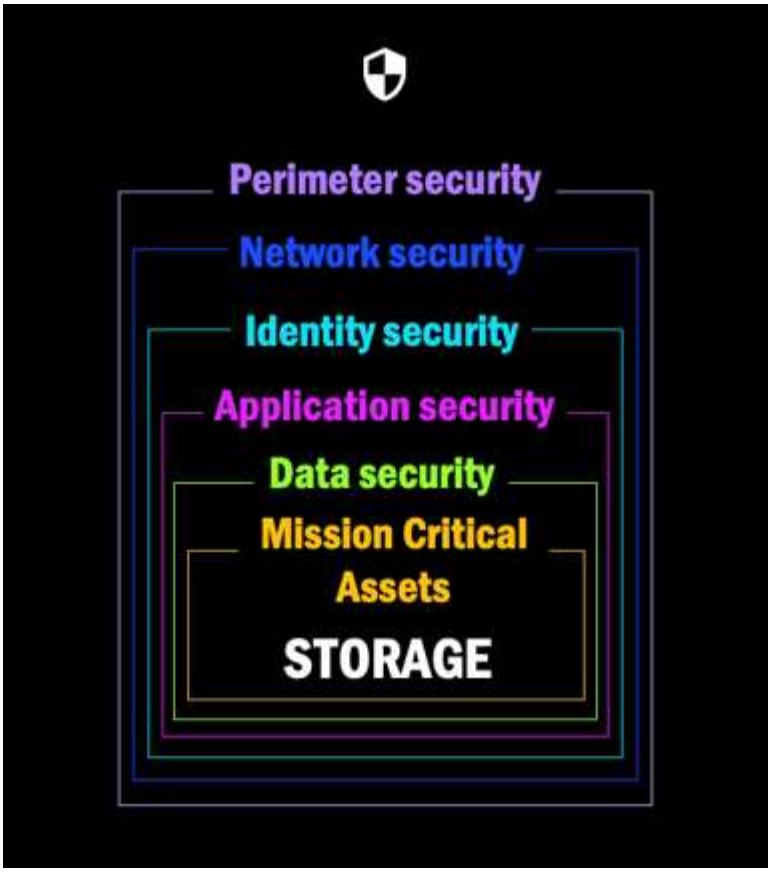
Gli attacchi ransomware possono bloccare l'accesso ai dati e gli hacker possono chiedere un riscatto in cambio del rilascio o della decrittografia dei dati. Secondo IDC, non è raro che le vittime del ransomware subiscano diversi attacchi ransomware. L'attacco può interrompere l'accesso ai tuoi dati tra un giorno e diverse settimane.

La protezione dal ransomware di BlueXP è un servizio per proteggere i tuoi dati dai ransomware. Il servizio protegge i carichi di lavoro basati su applicazioni dei datastore Oracle, MySQL, VM e file share su storage NAS on-premise (utilizzando i protocolli NFS e CIFS), oltre a Cloud Volumes ONTAP per Amazon Web Services, Cloud Volumes ONTAP per Google Cloud e Cloud Volumes ONTAP per Microsoft Azure nelle organizzazioni BlueXP . Il servizio esegue il backup dei dati su Amazon Web Services, Google Cloud, il cloud storage Microsoft Azure e NetApp StorageGRID.

Protezione dal ransomware ai layer di dati

La tua posizione di sicurezza generalmente comprende più livelli di difesa per proteggerti da una serie di minacce informatiche.

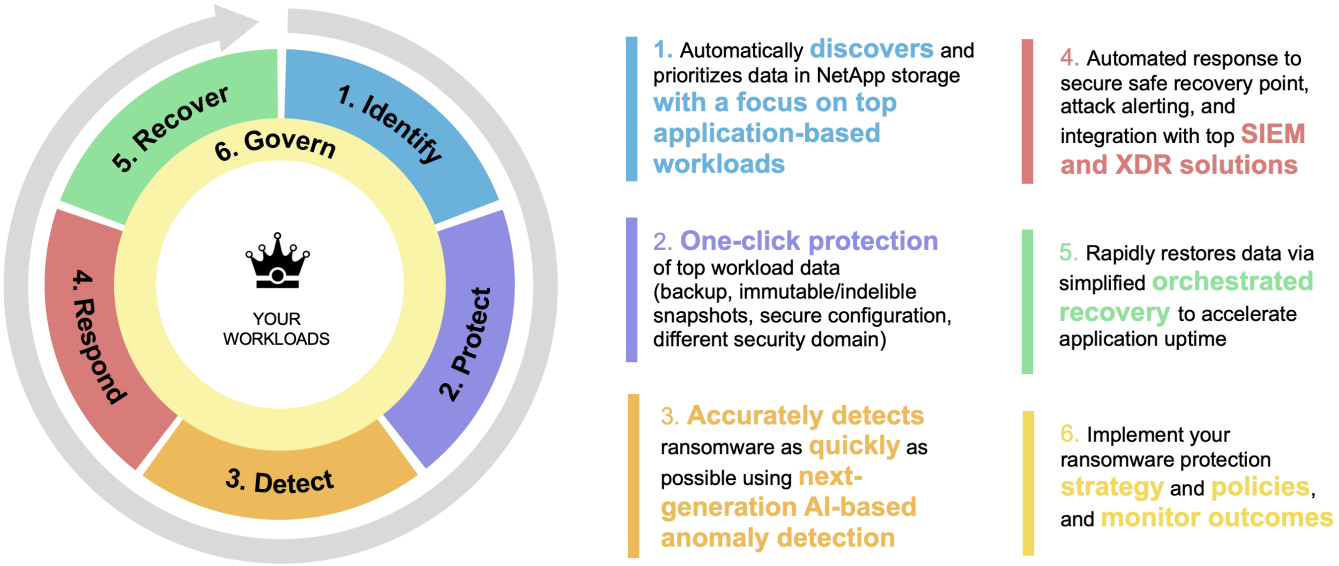
- **Livello più esterno**: Questa è la prima linea di difesa che utilizza firewall, sistemi di rilevamento delle intrusioni e reti private virtuali per salvaguardare i confini della rete.
- **Sicurezza della rete**: Questo livello si basa sulla segmentazione della rete, sul monitoraggio del traffico e sulla crittografia.
- **Sicurezza delle identità**: Utilizza metodi di autenticazione, controlli degli accessi e gestione delle identità per garantire che solo gli utenti autorizzati possano accedere a risorse riservate.
- **Protezione delle applicazioni**: Protegge le applicazioni software utilizzando procedure di codifica protetta, test di protezione e protezione automatica delle applicazioni runtime.
- **Sicurezza dei dati**: Protegge i tuoi dati con strategie di protezione, backup e recupero. La protezione ransomware BlueXP opera su questo livello.



Cosa puoi fare con la protezione dal ransomware di BlueXP

Il servizio di protezione dal ransomware di BlueXP offre un utilizzo completo di diverse tecnologie NetApp così che il tuo amministratore dello storage, amministratore della sicurezza dei dati o ingegnere delle operazioni di sicurezza possano raggiungere i seguenti obiettivi:

- **Identifica** tutti i workload basati su applicazioni, condivisioni di file o gestiti da VMware in NAS NetApp BlueXP on-premise con ambienti di lavoro NFS o CIFS in BlueXP , tra organizzazioni, progetti e connettori BlueXP . Quindi, il servizio categorizza la priorità dei dati e offre consigli per i miglioramenti alla protezione dal ransomware.
- **Proteggi** i tuoi workload abilitando backup, copie Snapshot e strategie di protezione dal ransomware sui tuoi dati.
- **Rileva** anomalie che potrebbero essere attacchi ransomware.nota a piè di pagina:[Nessun sistema di rilevamento o prevenzione del ransomware può garantire completamente la sicurezza da un attacco ransomware. Anche se è possibile che un attacco non venga rilevato, la tecnologia NetApp funge da importante livello di difesa aggiuntivo.]
- **Rispondi** ai potenziali attacchi ransomware avviando automaticamente una Snapshot NetApp ONTAP a prova di manomissione che è bloccata in modo che la copia non possa essere eliminata accidentalmente o malamente. I tuoi dati di backup rimarranno immutabili e protetti end-to-end dagli attacchi ransomware all'origine e alla destinazione.
- **Recupera** i tuoi workload che aiutano ad accelerare l'uptime dei workload orchestrando diverse tecnologie NetApp. È possibile scegliere di ripristinare volumi specifici. Il servizio fornisce consigli sulle opzioni migliori.
- **Governare**: Implementa la tua strategia di protezione dal ransomware e monitora i risultati.



Vantaggi dell'utilizzo della protezione dal ransomware di BlueXP

La protezione dal ransomware BlueXP offre i seguenti benefici:

- Rileva i carichi di lavoro e le pianificazioni di backup e snapshot esistenti e classifica la relativa importanza.
- Valuta il livello di protezione ransomware e lo visualizza in un dashboard di facile comprensione.
- Fornisce consigli sulle fasi successive in base al rilevamento e all'analisi della postura di protezione.
- Applica raccomandazioni di data Protection ai/ML con un solo clic.
- Protegge i dati nei principali carichi di lavoro basati sull'applicazione, come i datastore e le condivisioni di file MySQL, Oracle e VMware.
- Rileva gli attacchi ransomware sui dati in tempo reale sullo storage primario utilizzando la tecnologia ai.
- Avvia azioni automatizzate in risposta ai potenziali attacchi rilevati creando copie Snapshot e avviando avvisi relativi ad attività anomale.
- Applica una recovery ridotta per soddisfare le policy di RPO. La protezione ransomware di BlueXP orchestra il recovery dagli incidenti ransomware utilizzando diversi servizi di recovery di NetApp, tra cui backup e recovery di BlueXP (in precedenza Cloud Backup) e SnapCenter.
- Utilizza RBAC (role-based access control) per gestire l'accesso a funzionalità e operazioni nel servizio, migliorando la sicurezza.

Costo

NetApp non ti addebita i costi per l'utilizzo della versione di prova della protezione dal ransomware di BlueXP.

Se disponi sia di backup e recovery di BlueXP che di protezione ransomware BlueXP , qualsiasi dato comune protetto da entrambi i prodotti verrà fatturato solo dalla protezione ransomware di BlueXP .

Dopo l'acquisto di una licenza o di un'iscrizione a PayGo, qualsiasi workload con una policy di rilevamento del ransomware (protezione autonoma da ransomware) abilitata (scoperta o impostata dalla protezione ransomware di BlueXP), e almeno una policy di backup o snapshot, la protezione ransomware di BlueXP la classifica "protetta" e conta sulla capacità acquistata o sull'iscrizione PayGo. Se un carico di lavoro viene rilevato senza una policy di rilevamento (ARP) anche se dispone di policy di backup o snapshot, viene classificato "a rischio" e *non* conta rispetto alla capacità acquistata.

I workload protetti contano rispetto alla capacità acquistata o all'iscrizione dopo la fine del periodo di prova di 90 giorni. La protezione dal ransomware BlueXP prevede addebiti per GB per i dati associati ai workload protetti prima dell'efficienza.

Licensing

Grazie alla protezione dal ransomware di BlueXP, puoi utilizzare diversi piani di licenza, tra cui una prova gratuita, un abbonamento pay-as-you-go a breve o il "Bring Your Own License".

Il servizio di protezione dal ransomware di BlueXP richiede una licenza NetApp ONTAP.

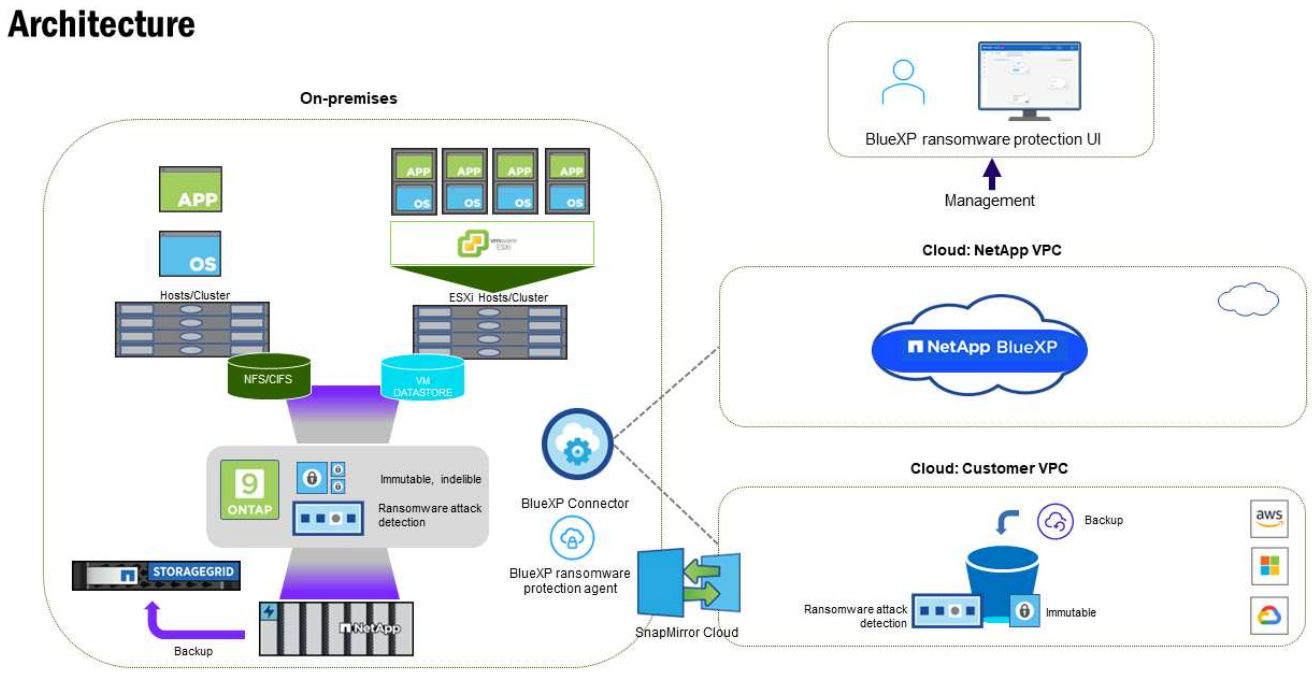
La licenza di protezione ransomware BlueXP non include prodotti NetApp aggiuntivi. La protezione dal ransomware di BlueXP può usare il backup e recovery di BlueXP anche se non disponi di una licenza per esso.

Per ulteriori informazioni, vedere "Impostare la licenza".

Come funziona la protezione ransomware di BlueXP

A un livello elevato, la protezione dal ransomware di BlueXP funziona in questo modo.

La protezione ransomware BlueXP utilizza il backup e il recovery di BlueXP per rilevare e impostare policy di backup e snapshot per i workload di condivisione di file e SnapCenter o SnapCenter per VMware per rilevare e impostare policy di backup e snapshot per applicazioni e workload delle macchine virtuali. Inoltre, la protezione dal ransomware BlueXP utilizza il backup e recovery di BlueXP e SnapCenter / SnapCenter per VMware per eseguire recovery coerente con file e carico di lavoro.



Funzione	Descrizione
IDENTIFICA	• Trova tutti i protocolli NAS on-premise del cliente (protocolli NFS e CIFS) e i dati Cloud Volumes ONTAP connessi ad BlueXP. • Identifica i dati dei clienti provenienti dalle API dei servizi ONTAP e SnapCenter e li associa ai workload. Scopri di più "ONTAP" e. "Software SnapCenter". • Rileva il livello di protezione corrente di ogni volume delle copie Snapshot NetApp e delle policy di backup, oltre a qualsiasi funzionalità di rilevamento on-box. Il servizio associa quindi questa postura di protezione ai workload utilizzando backup e recovery di BlueXP, i servizi ONTAP e le tecnologie NetApp come protezione autonoma da ransomware, FPolicy, policy di backup e policy Snapshot. Scopri di più "Protezione ransomware autonoma" e. "Backup e ripristino BlueXP", e. "FPolicy di ONTAP". • Assegna una priorità aziendale a ogni carico di lavoro in base ai livelli di protezione rilevati automaticamente e consiglia policy di protezione per i carichi di lavoro in base alla priorità aziendale. La priorità del carico di lavoro si basa sulle frequenze di Snapshot già applicate a ciascun volume associato al carico di lavoro.
PROTEGGI	• Monitora attivamente i workload e orchestra l'utilizzo di backup e recovery di BlueXP, le API SnapCenter e ONTAP applicando policy a ciascuno dei workload identificati.
RILEVA	• Rileva i potenziali attacchi con un modello di machine learning (ML) integrato che rileva crittografia e attività potenzialmente anomale. • Rilevamento a doppio livello che inizia con il rilevamento di potenziali attacchi ransomware nello storage primario e risponde ad attività anomale creando ulteriori copie Snapshot automatizzate per creare i punti di ripristino dei dati più vicini. Il servizio offre la possibilità di approfondire per identificare con maggiore precisione i potenziali attacchi, senza influire sulle performance dei carichi di lavoro primari. • Determina i file sospetti specifici e mappa gli attacchi ai carichi di lavoro associati, utilizzando le tecnologie ONTAP, protezione autonoma dal ransomware e FPolicy.
RISPONDI	• Mostra i dati pertinenti, come l'attività dei file, l'attività dell'utente e l'entropia, per aiutarti a completare revisioni forensi sull'attacco. • Avvia copie Snapshot rapide utilizzando tecnologie e prodotti NetApp come ONTAP, protezione autonoma da ransomware e FPolicy.
RECUPERA	• Determina la snapshot o il backup migliori e consiglia il recovery point effettivo (RPA) utilizzando backup e recovery di BlueXP, ONTAP, protezione autonoma da ransomware e tecnologie e servizi FPolicy. • Orchestra il recovery dei workload, tra cui VM, condivisioni di file e database, con coerenza delle applicazioni.
GOVERNARE	• Assegna le strategie di protezione dal ransomware • Aiuta a monitorare i risultati.

Destinazioni di backup, ambienti di lavoro e origini dati workload supportate

Utilizza la protezione ransomware BlueXP per scoprire quanto siano resilienti i tuoi dati rispetto a un attacco informatico sui seguenti tipi di destinazioni di backup, ambienti di lavoro e origini dati dei workload:

Target di backup supportati

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

Ambienti di lavoro supportati

- NAS ONTAP on-premise (con protocolli NFS e CIFS) con ONTAP versione 9.11.1 e successive
- Cloud Volumes ONTAP 9.11.1 o superiore per AWS (con protocolli NFS e CIFS)
- Cloud Volumes ONTAP 9.11.1 o versione successiva per Google Cloud Platform (con protocolli NFS e CIFS)
- Cloud Volumes ONTAP 9.11.1 o superiore per Microsoft Azure (con protocolli NFS e CIFS)

> Non sono supportati i seguenti elementi: Volumi FlexGroup, versioni di ONTAP precedenti a 9.11.1, volumi iSCSI, volumi punto di montaggio, volumi percorso di montaggio, volumi offline, e Data Protection (DP).

Origini dati workload supportate

Il servizio protegge i seguenti carichi di lavoro basati su applicazioni sui volumi di dati primari:

- Condivisioni di file NetApp
- Datastore VMware
- Database (MySQL e Oracle)
- Altre novità in arrivo

Inoltre, se stai utilizzando SnapCenter o SnapCenter per VMware, tutti i workload supportati da questi prodotti sono anche identificati nella protezione dal ransomware di BlueXP . La protezione ransomware di BlueXP può proteggere e ripristinare questi dati in modo coerente con il carico di lavoro.

Termini che potrebbero aiutarti con la protezione dal ransomware

Potresti trarre beneficio dalla comprensione di una certa terminologia relativa alla protezione dal ransomware.

- **Protezione**: La protezione in BlueXP consiste nel garantire che le snapshot e i backup immutabili vengano eseguiti regolarmente su un dominio di sicurezza diverso utilizzando criteri di protezione.
- **Carico di lavoro**: Un carico di lavoro nella protezione dal ransomware di BlueXP può includere database MySQL o Oracle, datastore VMware o condivisioni di file.

Prerequisiti della protezione dal ransomware di BlueXP

Inizia subito con la protezione dal ransomware di BlueXP verificando la preparazione del

tuo ambiente operativo, dell'accesso, dell'accesso alla rete e del browser web.

Per utilizzare la protezione dal ransomware BlueXP , hai bisogno di questi prerequisiti.

A BlueXP

- Un account utente BlueXP con Privileges amministratore organizzazione per la ricerca delle risorse.
- Un'organizzazione BlueXP con almeno un connettore BlueXP attivo che si connette ai cluster ONTAP on-premise o si connette a Cloud Volumes ONTAP in AWS o in Azure.
- Almeno un ambiente di lavoro BlueXP con un cluster ONTAP on-premise NetApp o Cloud Volume ONTAP in AWS o Azure (con protocolli NAS o CIFS).
  - Sono supportati i cluster ONTAP o Cloud Volume ONTAP con ONTAP OS versione 9.11.1 o superiore.
  - Se i tuoi cluster ONTAP on-premise o Cloud Volume ONTAP in AWS o nel cloud Azure non sono già integrati in BlueXP , ti servirà un BlueXP Connector.

    Fare riferimento a "Informazioni su come configurare un connettore BlueXP " e "Requisiti standard di BlueXP".

> Se disponi di più connettori BlueXP in una singola organizzazione BlueXP , il servizio di protezione dal ransomware BlueXP eseguirà la scansione delle risorse ONTAP su tutti i connettori oltre a quello attualmente selezionato nell'interfaccia utente di BlueXP .

In ONTAP 9.11.1 e versioni successive

- Una licenza per la protezione autonoma da ransomware NetApp, utilizzata dalla protezione BlueXP, abilitata sull'istanza ONTAP on-premise, a seconda della versione di ONTAP che stai utilizzando. Fare riferimento a. "Panoramica della protezione ransomware autonoma".

> La release generale della protezione ransomware di BlueXP, a differenza della release Preview, include una licenza per la tecnologia di protezione autonoma dal ransomware NetApp. Fare riferimento a. "Panoramica della protezione ransomware autonoma" per ulteriori informazioni.

  Per ulteriori informazioni sulle licenze, fare riferimento a. "Scopri di più sulla protezione ransomware di BlueXP".

- Per applicare configurazioni di protezione (come l'abilitazione della protezione autonoma da ransomware e altri), la protezione ransomware di BlueXP necessita di autorizzazioni amministrative sul cluster ONTAP. Il cluster ONTAP dovrebbe essere stato integrato utilizzando solo le credenziali dell'utente amministratore del cluster ONTAP.
- Se il cluster ONTAP è già integrato in BlueXP utilizzando credenziali utente non-admin, è necessario aggiornare le autorizzazioni utente non-admin con le autorizzazioni necessarie accedendo al cluster ONTAP, descritto in questa pagina.

Per il backup dei dati

- Un account in NetApp StorageGRID, AWS S3 o BLOB di Azure per le destinazioni di backup e il set di autorizzazioni di accesso.

  Per ulteriori informazioni, fare riferimento alla "Elenco dei permessi di AWS, Azure o S3" .

- Non è necessario attivare il servizio di backup e ripristino BlueXP nell'ambiente di lavoro.

  Il servizio di protezione dal ransomware di BlueXP aiuta a configurare una destinazione di backup tramite l'opzione Settings. Vedere "Configurare le impostazioni".

Aggiornare le autorizzazioni utente non amministrative in un ambiente di lavoro ONTAP

Se è necessario aggiornare le autorizzazioni utente non amministrative per un particolare ambiente di lavoro, completare questi passaggi.

1. Accedere a BlueXP e cercare l'ambiente di lavoro che richiede l'aggiornamento delle autorizzazioni utente ONTAP.
2. Fare doppio clic sull'ambiente di lavoro per visualizzare i dettagli.
3. Fare clic su **Visualizza informazioni aggiuntive** che mostrano il nome utente.
4. Accedere alla CLI del cluster di ONTAP usando l'utente di amministrazione.
5. Visualizza i ruoli esistenti per quell'utente. Inserire:

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

6. Modificare il ruolo dell'utente. Inserire:

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

7. Torna all'interfaccia utente di protezione ransomware di BlueXP per utilizzarla.

Avvio rapido per la protezione dal ransomware di BlueXP

Ecco una panoramica dei passaggi necessari per iniziare con la protezione dal ransomware di BlueXP. I collegamenti all'interno di ogni passaggio consentono di accedere a una pagina che fornisce ulteriori dettagli.

1 Esaminare i prerequisiti

"Assicurati che il tuo ambiente soddisfi questi requisiti".

2 Configurare il servizio di protezione dal ransomware

- "Preparare NetApp StorageGRID, Amazon Web Services o Microsoft Azure come destinazione di backup".
- "Configurare un connettore in BlueXP".
- "Configurare le destinazioni di backup".

- "Abilitare facoltativamente il rilevamento delle minacce".
- "Scopri i carichi di lavoro in BlueXP".

3 **Quali sono le prossime novità?**

Dopo aver configurato il servizio, ecco cosa fare in seguito.

- "Visualizza la salute della protezione dei carichi di lavoro sulla Dashboard".
- "Proteggere i carichi di lavoro".
- "Rispondi al rilevamento di potenziali attacchi ransomware".
- "Recupero da un attacco (dopo che gli incidenti sono neutralizzati)".

Imposta la protezione dal ransomware BlueXP

Per utilizzare la protezione dal ransomware di BlueXP, esegui alcuni passaggi per configurarla.

Prima di iniziare, rivedere "prerequisiti" per garantire che il tuo ambiente sia pronto.

Preparare la destinazione di backup

Preparare una delle seguenti destinazioni di backup:

- NetApp StorageGRID
- Amazon Web Services
- Microsoft Azure

Dopo aver configurato le opzioni nella destinazione di backup stessa, la configurerai in seguito come destinazione di backup nel servizio di protezione dal ransomware di BlueXP.

Preparare StorageGRID a diventare una destinazione di backup

Se si desidera utilizzare StorageGRID come destinazione di backup, fare riferimento alla sezione "Documentazione StorageGRID" Per ulteriori informazioni su StorageGRID.

Prepara AWS a diventare una destinazione di backup

- Configurare un account in AWS.
- Configurare "Autorizzazioni AWS" In AWS.

Per informazioni sulla gestione dello storage AWS in BlueXP, fare riferimento a. "Gestisci i bucket Amazon S3".

Preparare Azure a diventare una destinazione di backup

- Configurare un account in Azure.
- Configurare "Autorizzazioni Azure" In Azure.

Per informazioni sulla gestione dello storage Azure in BlueXP, fare riferimento a. "Gestione degli account storage Azure".

Configurare BlueXP

Il passo successivo è la configurazione di BlueXP e del servizio di protezione dal ransomware di BlueXP.

Revisione "Requisiti standard di BlueXP".

Creare un connettore in BlueXP

Contattare il rappresentante di vendita NetApp per provare o utilizzare questo servizio. Quindi, quando usi il connettore BlueXP, includerai le funzionalità appropriate per il servizio di protezione dal ransomware.

Per creare un connettore in BlueXP prima di utilizzare il servizio, consultare la documentazione di BlueXP che descrive "Come creare un connettore BlueXP".

> Se disponi di più connettori BlueXP, il servizio scansionerà i dati su tutti i connettori oltre a quello attualmente visualizzato nell'interfaccia utente di BlueXP. Questo servizio rileva tutti i progetti e tutti i connettori associati a questa organizzazione.

Accedi alla protezione dal ransomware di BlueXP

USA NetApp BlueXP per accedere al servizio di protezione dal ransomware di BlueXP.

La protezione anti-ransomware BlueXP utilizza il role-based access control (RBAC) per gestire l'accesso che ogni utente ha ad azioni specifiche. Per informazioni dettagliate sulle azioni che ogni ruolo può eseguire, vedere "Privileges per il controllo degli accessi in base al ruolo della protezione ransomware BlueXP ".

Per accedere a BlueXP, puoi utilizzare le credenziali del sito di supporto NetApp oppure iscriverti per un login cloud NetApp utilizzando la tua email e una password. "Scopri di più sull'accesso".

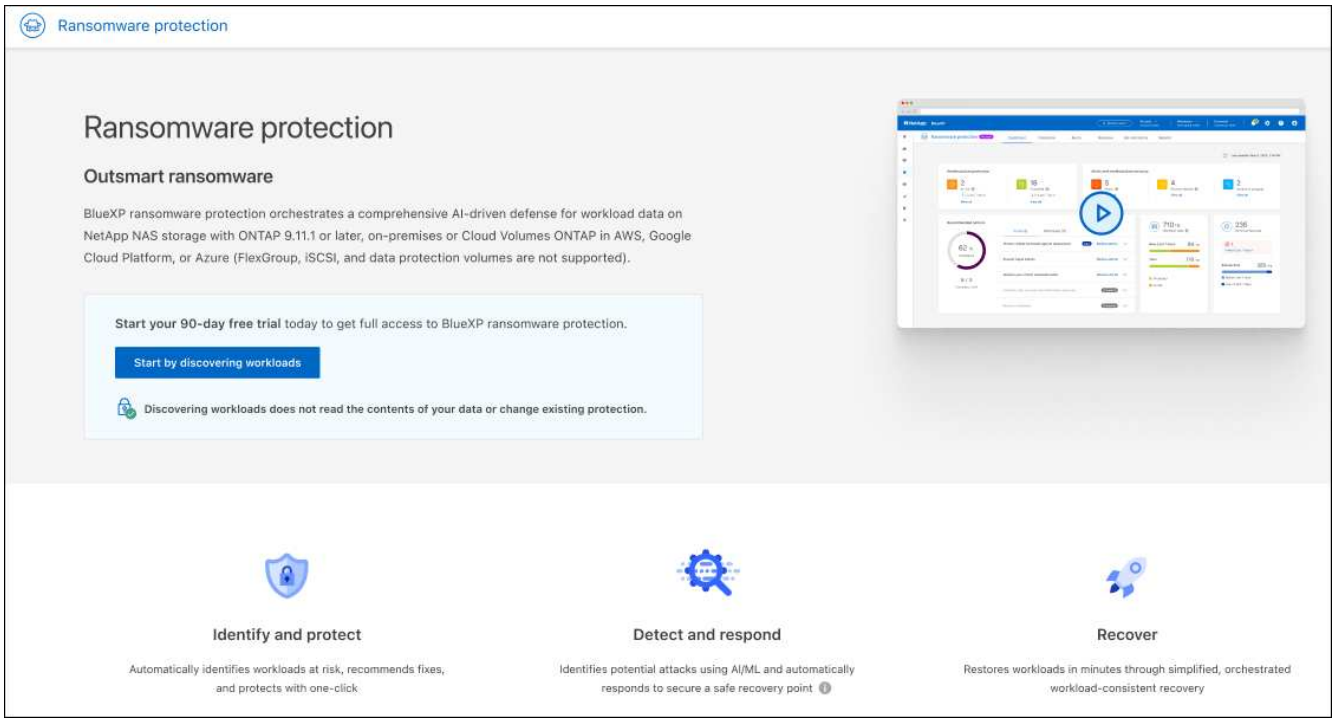
Fasi

1. Aprire un browser Web e accedere a. "Console BlueXP".

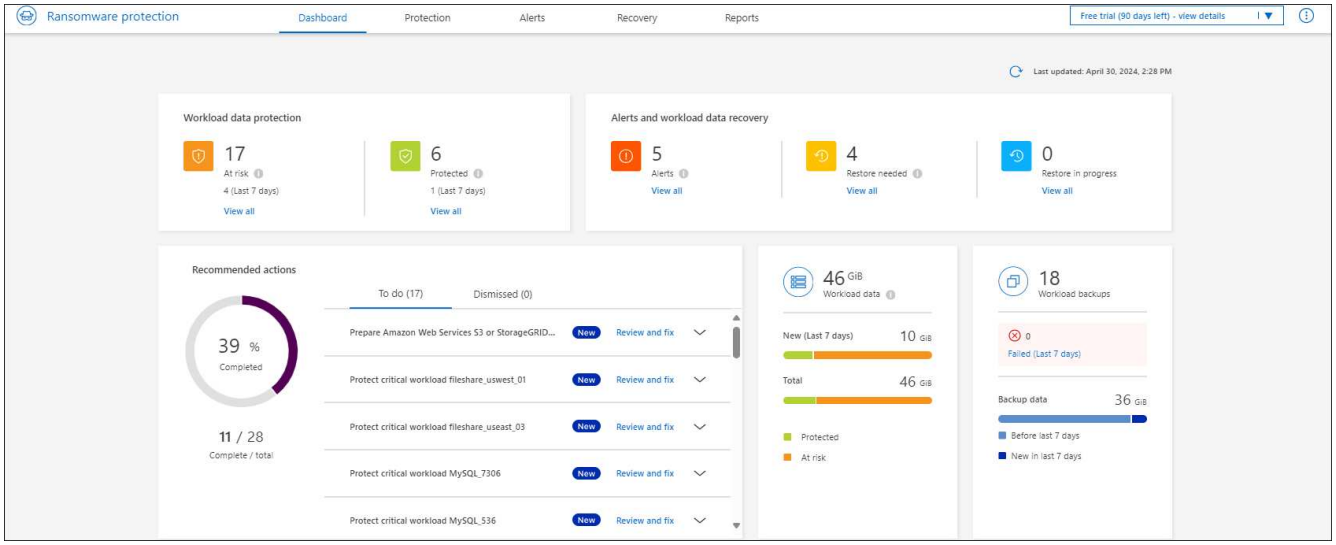
   Viene visualizzata la pagina di accesso a NetApp BlueXP.

2. Accedere a BlueXP.
3. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

   Se è la prima volta che accedi a questo servizio, viene visualizzata la pagina iniziale.



In caso contrario, verrà visualizzata la dashboard di protezione dal ransomware BlueXP.



> Se non disponi di un connettore BlueXP o non è quello per questo servizio, potrebbe essere necessario contattare il supporto NetApp.

4. Se non l'hai già fatto, seleziona l'opzione **rileva carichi di lavoro**.

   Fare riferimento a. "Rileva i carichi di lavoro".

Imposta una licenza per la protezione dal ransomware di BlueXP

Con la protezione dal ransomware di BlueXP, puoi usare piani di licenza diversi.

È possibile utilizzare i seguenti tipi di licenza:

- Iscriviti per una prova gratuita di 90 giorni.
- Acquista un abbonamento pay-as-you-go (PAYGO) con Amazon Web Services (AWS) Marketplace o Azure Marketplace (presto disponibile).
- BYOL (Bring Your Own License), ovvero un file di licenza NetApp (NLF) ottenuto dal rappresentante vendite NetApp Puoi utilizzare il numero di serie della licenza per attivare il BYOL nel Digital Wallet di BlueXP.

La licenza di protezione ransomware BlueXP non include prodotti NetApp aggiuntivi. La protezione dal ransomware di BlueXP può usare il backup e recovery di BlueXP anche se non disponi di una licenza per esso.

> Se disponi sia di backup e recovery di BlueXP che di protezione ransomware BlueXP , qualsiasi dato comune protetto da entrambi i prodotti verrà fatturato solo dalla protezione ransomware di BlueXP .

Dopo aver impostato il proprio BYOL o aver acquistato un abbonamento a PAYGO, è possibile visualizzare la licenza nella scheda portafoglio digitale BlueXP **licenze servizio dati** o l'abbonamento attivo nella scheda portafoglio digitale BlueXP **Sottoscrizioni**.

Al termine della prova gratuita o alla scadenza della licenza o dell'abbonamento, è comunque possibile effettuare le seguenti operazioni nel servizio:

- Visualizzare la salute dei carichi di lavoro e dei carichi di lavoro.
- Eliminare qualsiasi risorsa, ad esempio un carico di lavoro o una policy.
- Eseguire tutte le operazioni pianificate create durante il periodo di prova o sotto la licenza.

Provalo con una prova gratuita di 90 giorni

Puoi provare la protezione dal ransomware BlueXP utilizzando una prova gratuita di 90 giorni. Per avviare la prova gratuita, è necessario essere un amministratore dell'organizzazione BlueXP .

> Durante la prova non vengono applicati limiti di capacità.

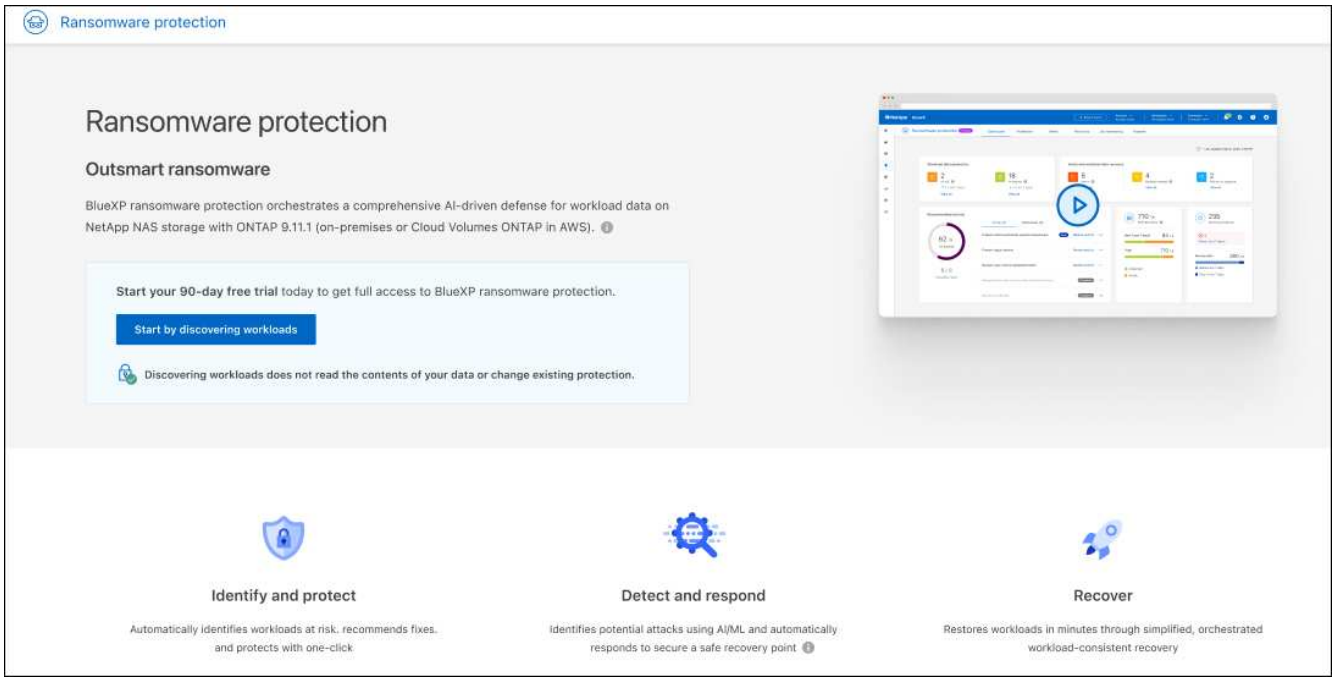
È possibile ottenere una licenza o sottoscrivere l'abbonamento in qualsiasi momento e non verrà addebitato alcun costo fino al termine della prova di 90 giorni. Per continuare dopo la prova di 90 giorni, dovrai acquistare una licenza BYOL o un abbonamento PAYGO.

Durante la prova, si dispone di tutte le funzionalità.

Fasi

1. Accedere a. "Console BlueXP".
2. Accedere a BlueXP.
3. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

   Se è la prima volta che accedi a questo servizio, viene visualizzata la pagina iniziale.



4. Se non è già stato aggiunto un connettore per altri servizi, aggiungerne uno.

   Per aggiungere un connettore, fare riferimento a. "Scopri di più sui connettori".

5. Dopo aver configurato un connettore, nella landing page della protezione dal ransomware BlueXP, il pulsante per aggiungere un connettore diventa un pulsante per rilevare i workload. Selezionare **inizia rilevando i carichi di lavoro**.
6. Per rivedere le informazioni sulla prova gratuita, selezionare l'opzione a discesa in alto a destra.

Al termine della prova, richiedere un abbonamento o una licenza

Al termine della prova gratuita, puoi iscriverti tramite AWS Marketplace o acquistare una licenza da NetApp.

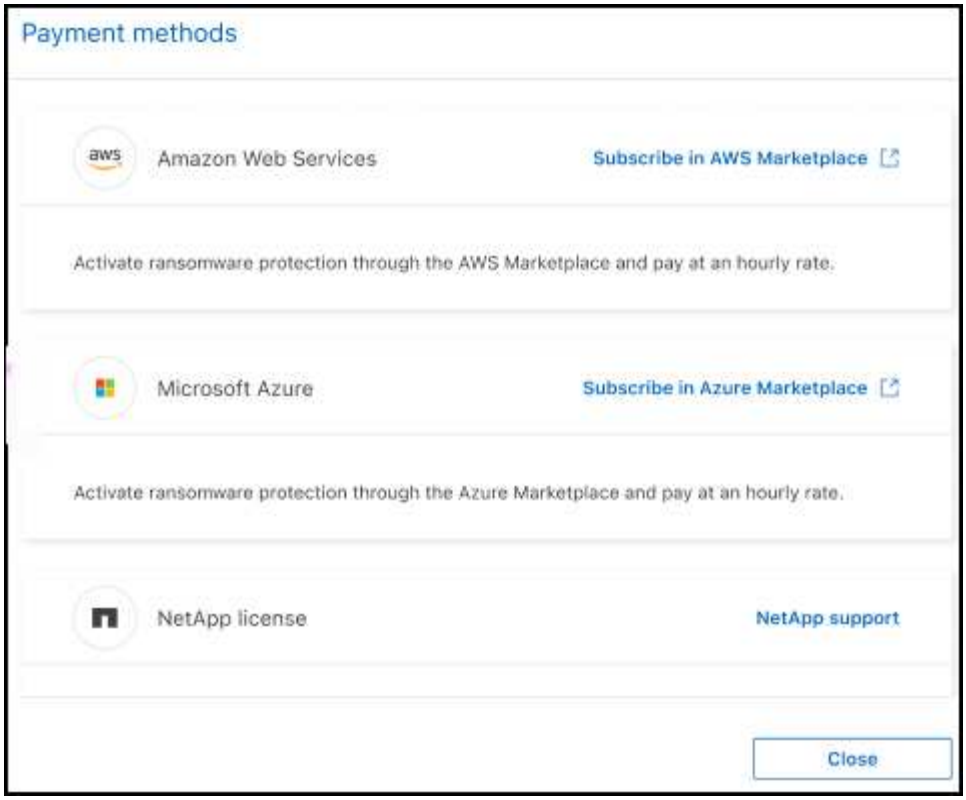
Iscriviti tramite AWS Marketplace Iscriviti tramite Microsoft Azure Marketplace BYOL

Iscriviti tramite AWS Marketplace

Questa procedura offre una panoramica di alto livello su come iscriversi direttamente in AWS Marketplace.

Fasi

1. Nella protezione dal ransomware di BlueXP, esegui una delle seguenti operazioni:
   - Viene visualizzato un messaggio che informa che la versione di prova gratuita sta per scadere. Nel messaggio, selezionare **Visualizza metodi di pagamento**.
   - Fare clic sull'avviso **prova gratuita** in alto a destra e selezionare **Visualizza metodi di pagamento**.

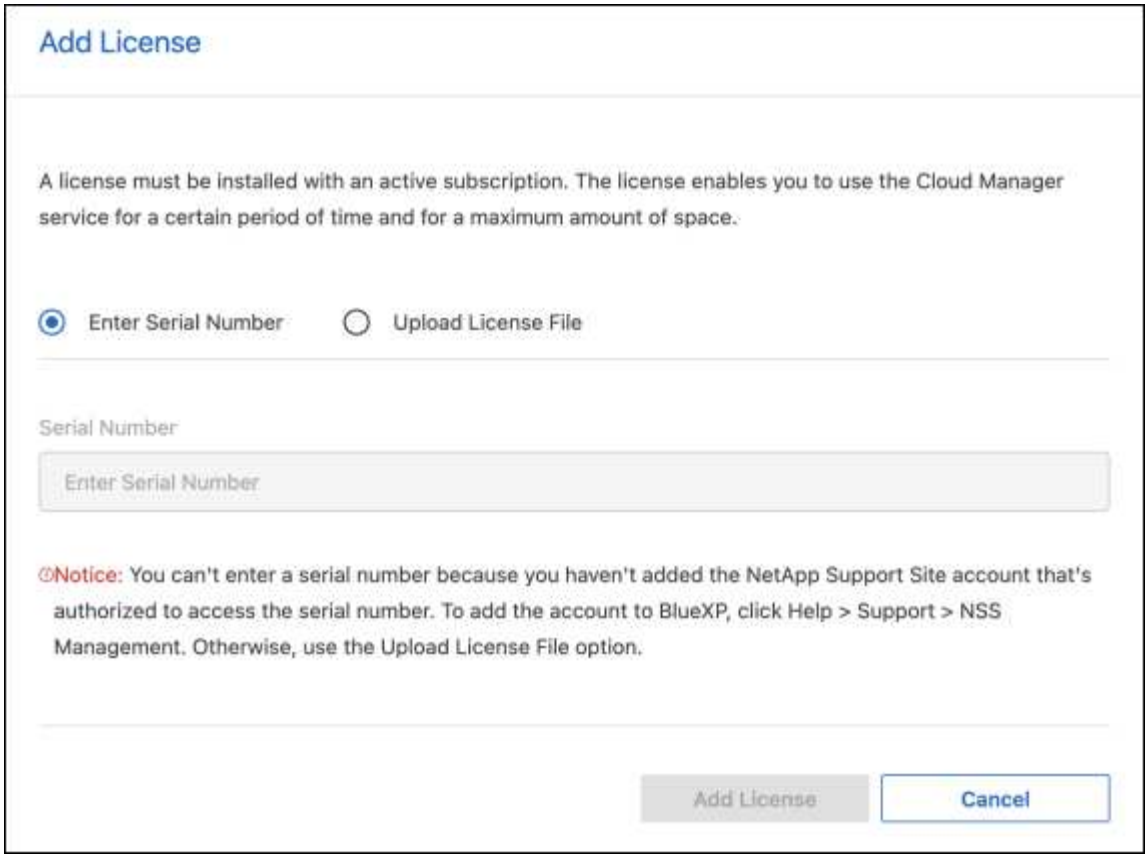


2. Nella pagina metodi di pagamento, seleziona **Iscriviti in AWS Marketplace**.
3. In AWS Marketplace, selezionare **Visualizza opzioni di acquisto**.
4. USA AWS Marketplace per sottoscrivere il servizio di protezione dal ransomware BlueXP.
5. Quando torni alla protezione ransomware di BlueXP, un messaggio indica che sei iscritto.

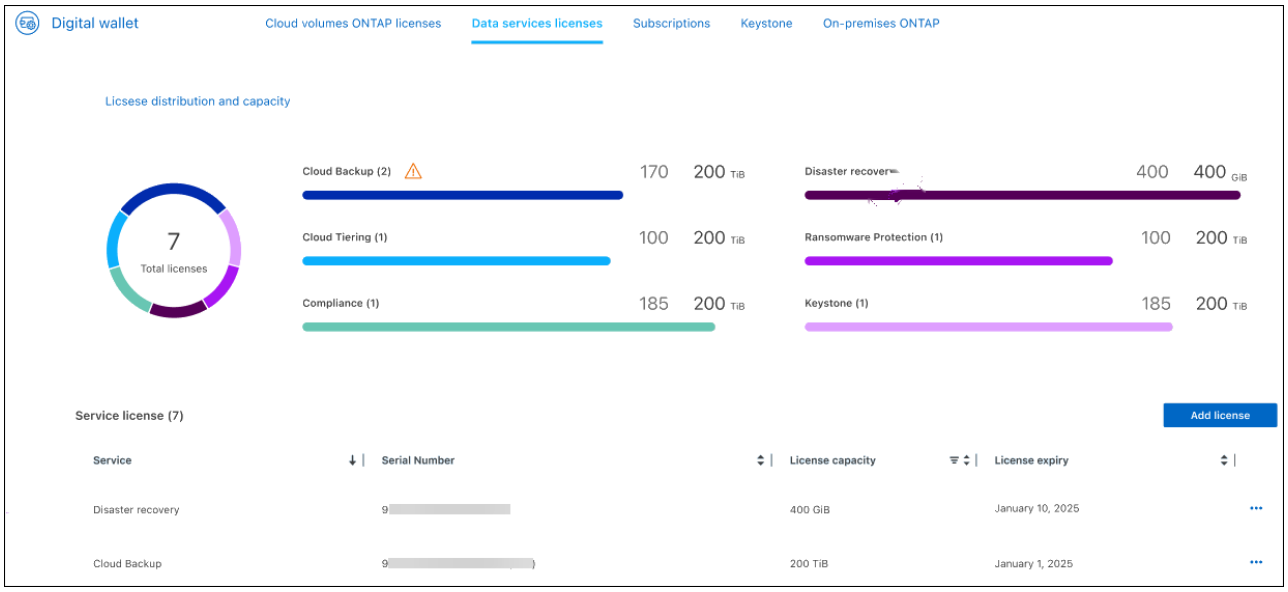
> Ti viene inviata un'email che include il numero di serie della protezione dal ransomware di BlueXP e che indica che la protezione dal ransomware di BlueXP è sottoscritta in AWS Marketplace.

6. Torna alla pagina dei metodi di pagamento per la protezione dal ransomware di BlueXP.
7. Aggiungere la licenza a BlueXP selezionando **Aggiungi licenza a BlueXP**.

   Il servizio di Digital Wallet di BlueXP mostra la pagina Add License (Aggiungi licenza).



8. Nella pagina Aggiungi licenza del Digital Wallet di BlueXP, seleziona **Inserisci numero di serie**, inserisci il numero di serie incluso nell'e-mail inviata e seleziona **Aggiungi licenza**.
9. Per visualizzare i dettagli della licenza nel Digital Wallet di BlueXP, dal menu di navigazione a sinistra di BlueXP, seleziona **Governance** > **Digital Wallet**.
   - Per visualizzare le informazioni sulla sottoscrizione, selezionare **Abbonamenti**.
   - Per visualizzare le licenze BYOL, selezionare **licenze servizi dati**.



10. Torna alla protezione dal ransomware di BlueXP. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

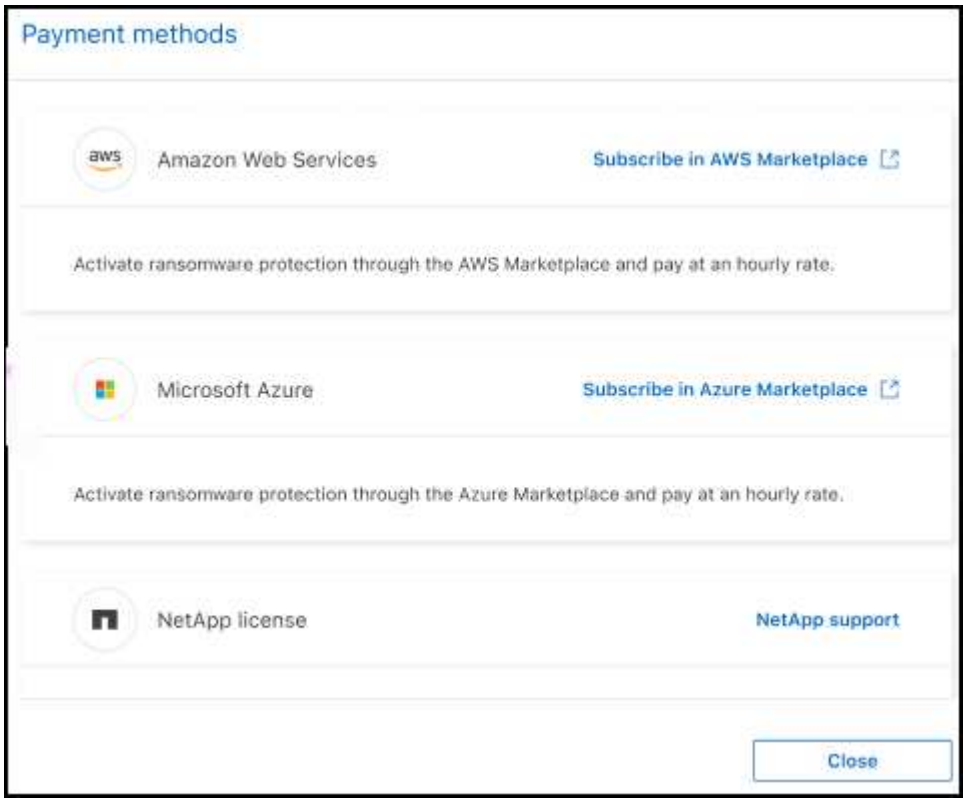
Viene visualizzato un messaggio che indica che è stata aggiunta una licenza.

Iscriviti tramite Microsoft Azure Marketplace

Questa procedura fornisce una panoramica di alto livello su come iscriversi direttamente in Azure Marketplace.

Fasi

1. Nella protezione dal ransomware di BlueXP, esegui una delle seguenti operazioni:
   - Viene visualizzato un messaggio che informa che la versione di prova gratuita sta per scadere. Nel messaggio, selezionare **Visualizza metodi di pagamento**.
   - Fare clic sull'avviso **prova gratuita** in alto a destra e selezionare **Visualizza metodi di pagamento**.

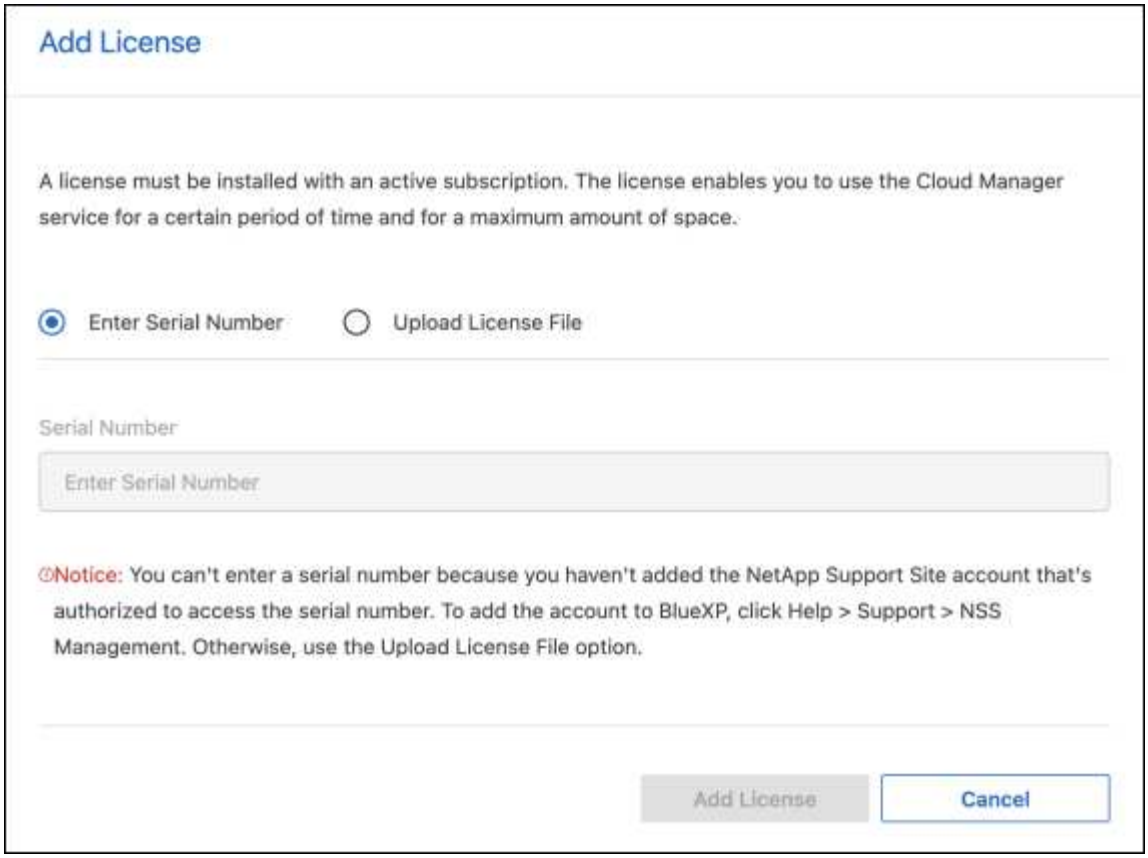


2. Nella pagina metodi di pagamento, seleziona **Sottoscrivi in Azure Marketplace**.
3. In Azure Marketplace, selezionare **Visualizza opzioni di acquisto**.
4. USA Azure Marketplace per sottoscrivere la protezione dal ransomware BlueXP.
5. Quando torni alla protezione ransomware di BlueXP, un messaggio indica che sei iscritto.

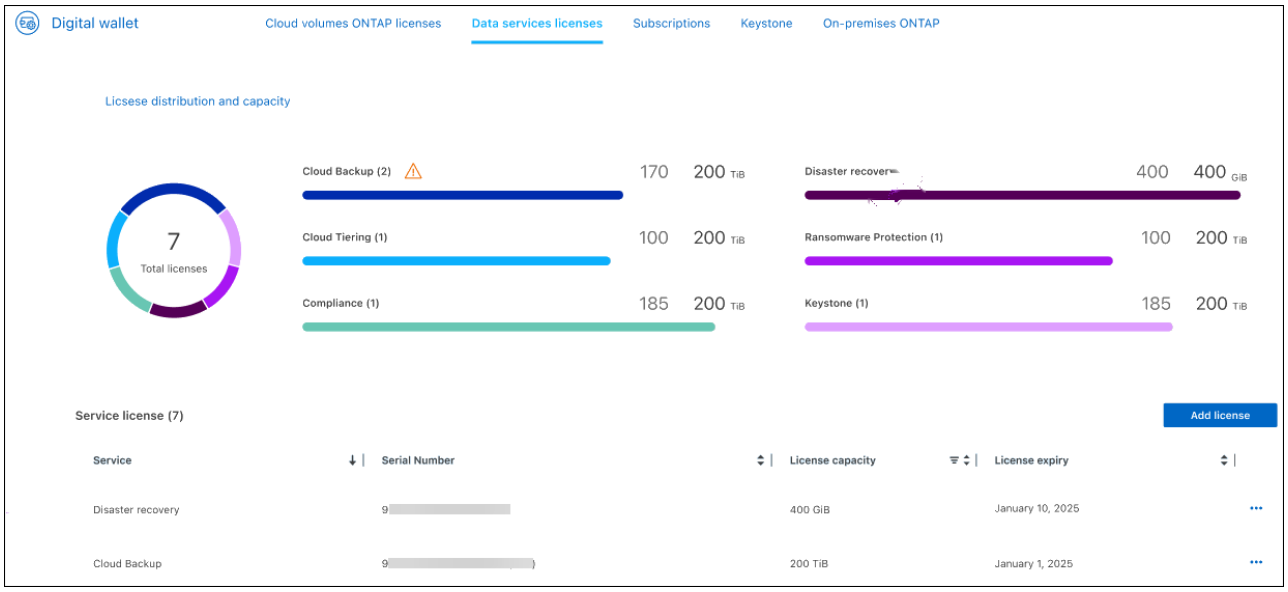
> Ti viene inviata un'email che include il numero di serie della protezione dal ransomware di BlueXP e che indica che la protezione dal ransomware di BlueXP è sottoscritta in Azure Marketplace.

6. Torna alla pagina dei metodi di pagamento per la protezione dal ransomware di BlueXP.
7. Aggiungere la licenza a BlueXP selezionando **Aggiungi licenza a BlueXP**.

   Il servizio di Digital Wallet di BlueXP mostra la pagina Add License (Aggiungi licenza).



8. Nella pagina Aggiungi licenza del Digital Wallet di BlueXP, seleziona **Inserisci numero di serie**, inserisci il numero di serie incluso nell'e-mail inviata e seleziona **Aggiungi licenza**.
9. Per visualizzare i dettagli della licenza nel Digital Wallet di BlueXP, dal menu di navigazione a sinistra di BlueXP, seleziona **Governance** > **Digital Wallet**.
   - Per visualizzare le informazioni sulla sottoscrizione, selezionare **Abbonamenti**.
   - Per visualizzare le licenze BYOL, selezionare **licenze servizi dati**.



10. Torna alla protezione dal ransomware di BlueXP. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

Viene visualizzato un messaggio che indica che è stata aggiunta una licenza.

BYOL

Per ottenere la tua licenza BYOL, dovrai acquistare la licenza, ottenere il file di licenza NetApp (NLF) e aggiungere la licenza al portafoglio digitale di BlueXP.

Aggiungi il file di licenza al Digital Wallet di BlueXP

Dopo aver acquistato la licenza di protezione ransomware BlueXP dal rappresentante di vendita NetApp, attivi la licenza inserendo il numero di serie della protezione ransomware di BlueXP e le informazioni dell'account del sito di supporto NetApp (NSS).

Prima di iniziare

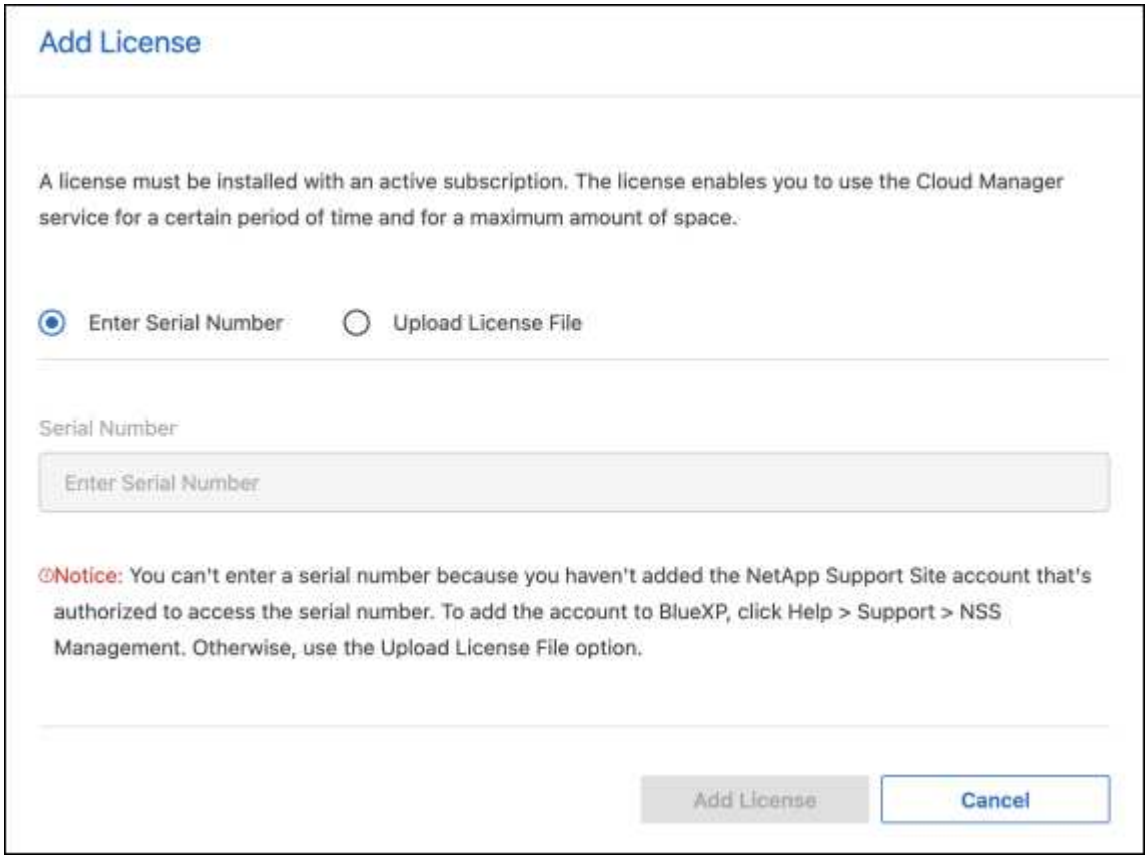
Avrai bisogno del numero di serie della protezione ransomware di BlueXP . Individua questo numero nell'ordine di vendita o contatta l'account team per ottenere queste informazioni.

Fasi

1. Una volta ottenuta la licenza, torna alla protezione dal ransomware di BlueXP. Seleziona l'opzione **Visualizza metodi di pagamento** in alto a destra. Oppure, nel messaggio che la prova gratuita sta per scadere, seleziona **Sottoscrivi o acquista una licenza**.
2. Selezionare **Aggiungi licenza ad BlueXP**.

   Verrai indirizzato al Digital Wallet di BlueXP.

3. Nel Digital Wallet di BlueXP, dalla scheda **licenze servizi dati**, selezionare **Aggiungi licenza**.



4. Nella pagina Aggiungi licenza, immettere il numero di serie e le informazioni sull'account del sito di assistenza NetApp.
   - Se si dispone del numero di serie della licenza BlueXP e si conosce il proprio account NSS, selezionare l'opzione **Inserisci numero di serie** e inserire le informazioni.

     Se il tuo account NetApp Support Site non è disponibile nell'elenco a discesa, "Aggiungere l'account NSS a BlueXP".

   - Se si dispone del file di licenza BlueXP (richiesto quando installato in un sito scuro), selezionare l'opzione **carica file di licenza** e seguire le istruzioni per allegare il file.
5. Selezionare **Aggiungi licenza**.

Risultato

Ora il Digital Wallet di BlueXP mostra la protezione dal ransomware di BlueXP con una licenza.

Aggiorna la tua licenza BlueXP alla scadenza

Se il termine in licenza si avvicina alla data di scadenza o se la tua capacità concessa in licenza sta raggiungendo il limite, riceverai una notifica nell'interfaccia utente di protezione dal ransomware di BlueXP. Puoi aggiornare la licenza di protezione dal ransomware BlueXP prima che scada, in modo che non ci siano interruzioni nella capacità di accesso ai dati sottoposti a scansione.

Questo messaggio viene visualizzato anche nel Digital Wallet di BlueXP e in "Notifiche".

Fasi

1. Seleziona l'icona della chat in basso a destra di BlueXP per richiedere un'estensione del termine o capacità aggiuntiva alla licenza per il numero di serie specifico. È anche possibile inviare un'e-mail per richiedere un aggiornamento della licenza.

   Dopo aver pagato la licenza e averla registrata nel NetApp Support Site, BlueXP aggiorna automaticamente la licenza nel portafoglio digitale BlueXP e la pagina licenze servizi dati rifletterà la modifica tra 5 e 10 minuti.

2. Se BlueXP non riesce ad aggiornare automaticamente la licenza (ad esempio, se installata in un sito buio), sarà necessario caricare manualmente il file di licenza.
   a. È possibile ottenere il file di licenza dal sito di assistenza NetApp.
   b. Accedi al Digital Wallet di BlueXP.
   c. Selezionare la scheda **licenze servizi dati**, selezionare l'icona **azioni …** per il numero di serie del servizio che si sta aggiornando, quindi selezionare **Aggiorna licenza**.

Rileva i carichi di lavoro nella protezione dal ransomware di BlueXP

Per utilizzare la protezione dal ransomware di BlueXP, il servizio deve prima rilevare i dati. Durante la scoperta, la protezione anti-ransomware BlueXP analizza tutti i volumi e i file negli ambienti di lavoro su tutti i connettori BlueXP e i progetti all'interno di un'organizzazione.

La protezione dal ransomware di BlueXP valuta applicazioni MySQL, applicazioni Oracle, datastore VMware e

condivisioni di file.

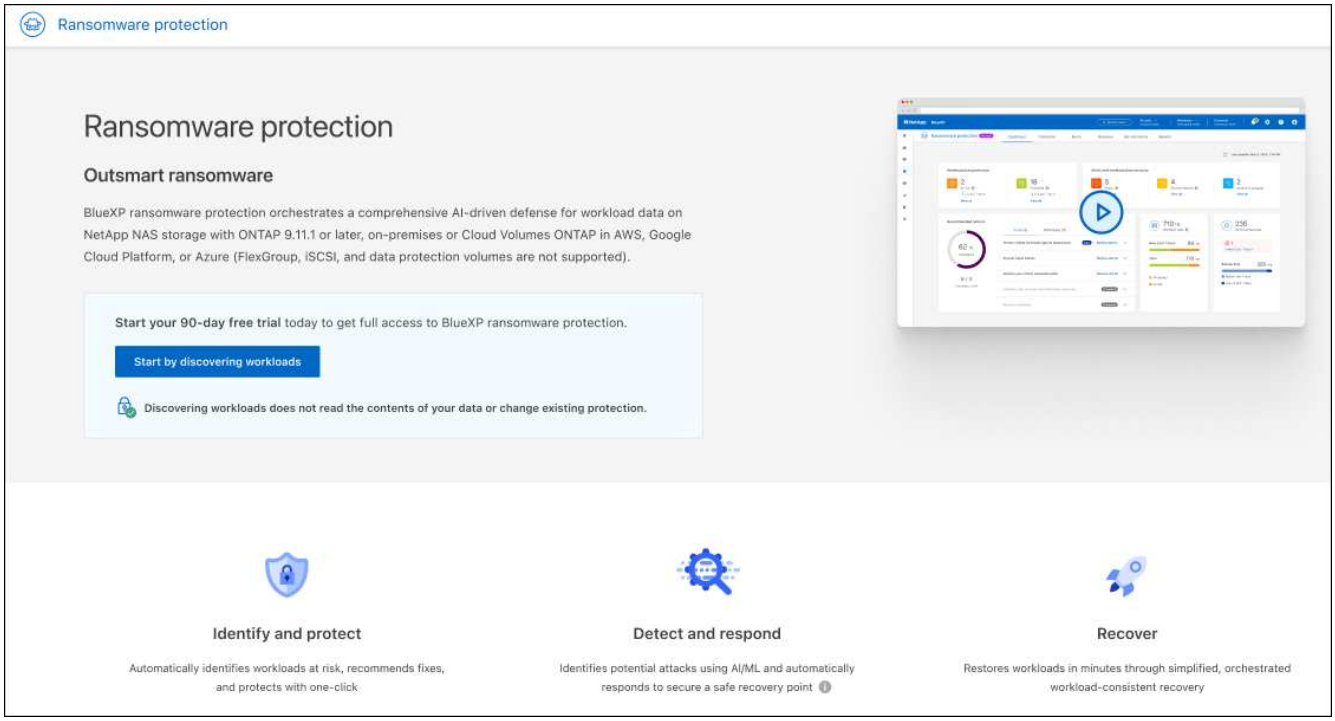
> Non verranno rilevati carichi di lavoro con volumi che utilizzano FlexGroup o iSCSI.

Il servizio valuta il livello di protezione esistente, incluse le opzioni di protezione di backup correnti, le copie Snapshot e le opzioni di protezione autonoma da ransomware NetApp. In base alla valutazione, il servizio consiglia quindi come migliorare la tua protezione dal ransomware.

Fasi

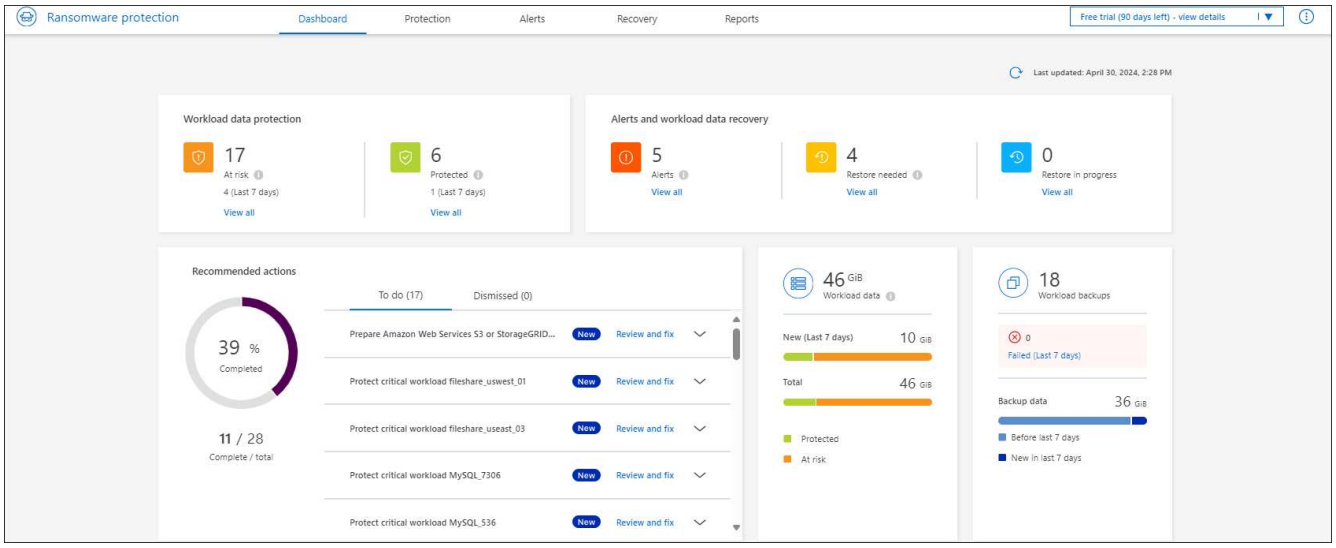
1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

   Se è la prima volta che accedi a questo servizio, viene visualizzata la pagina iniziale.



2. Dalla pagina iniziale, selezionare **inizia rilevando i carichi di lavoro**.

   Il servizio rileva i dati del carico di lavoro e mostra lo stato di salute della protezione dei dati nella Dashboard.



"Scopri cosa ti mostra il dashboard."

Configurare le impostazioni di protezione dal ransomware BlueXP

È possibile configurare una destinazione di backup o abilitare il rilevamento delle minacce consultando i suggerimenti sul dashboard o accedendo all'opzione **Impostazioni**.

L'attivazione del rilevamento delle minacce invia automaticamente i dati al sistema di gestione degli eventi e della sicurezza (SIEM) per l'analisi delle minacce.

Accedere direttamente alla pagina Impostazioni

È possibile accedere facilmente alla pagina Impostazioni dall'opzione azioni accanto al menu principale.

1. Dal menu di protezione dal ransomware BlueXP, seleziona il menu Vertical (verticale) … opzione in alto a destra.
2. Dal menu a discesa, selezionare **Impostazioni**.
3. Dalla pagina Impostazioni, è possibile effettuare le seguenti operazioni:
   - Aggiungere una destinazione di backup.
   - Collega il tuo sistema di gestione degli eventi e della sicurezza (SIEM) per l'analisi e il rilevamento delle minacce.

Aggiungere una destinazione di backup

La protezione dal ransomware di BlueXP identifica i workload che non hanno ancora backup e anche quelli che non hanno ancora destinazioni di backup assegnate.

Per proteggere questi workload, è necessario aggiungere una destinazione di backup. È possibile scegliere una delle seguenti destinazioni di backup:

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

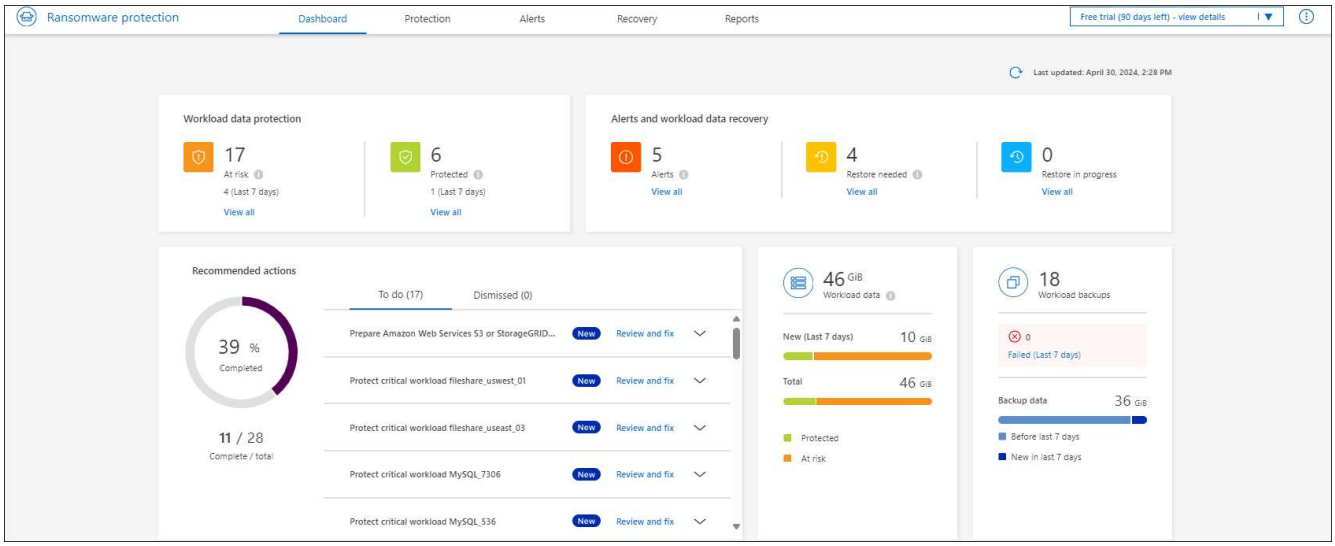
È possibile aggiungere una destinazione di backup in base all'azione consigliata dal Dashboard.

Accedere alle opzioni destinazione backup dalle azioni consigliate del dashboard

Il Dashboard fornisce molti consigli. Si consiglia di configurare una destinazione di backup.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Esaminare il riquadro delle azioni consigliate del dashboard.



3. Dal dashboard, selezionare **Rivedi e correggi** per la raccomandazione "prepara <backup provider> come destinazione di backup".
4. Continuare con le istruzioni a seconda del provider di backup.

Accedere alle opzioni destinazione di backup dal menu a discesa azioni

È possibile accedere facilmente alla pagina Impostazioni dall'opzione azioni accanto al menu principale.

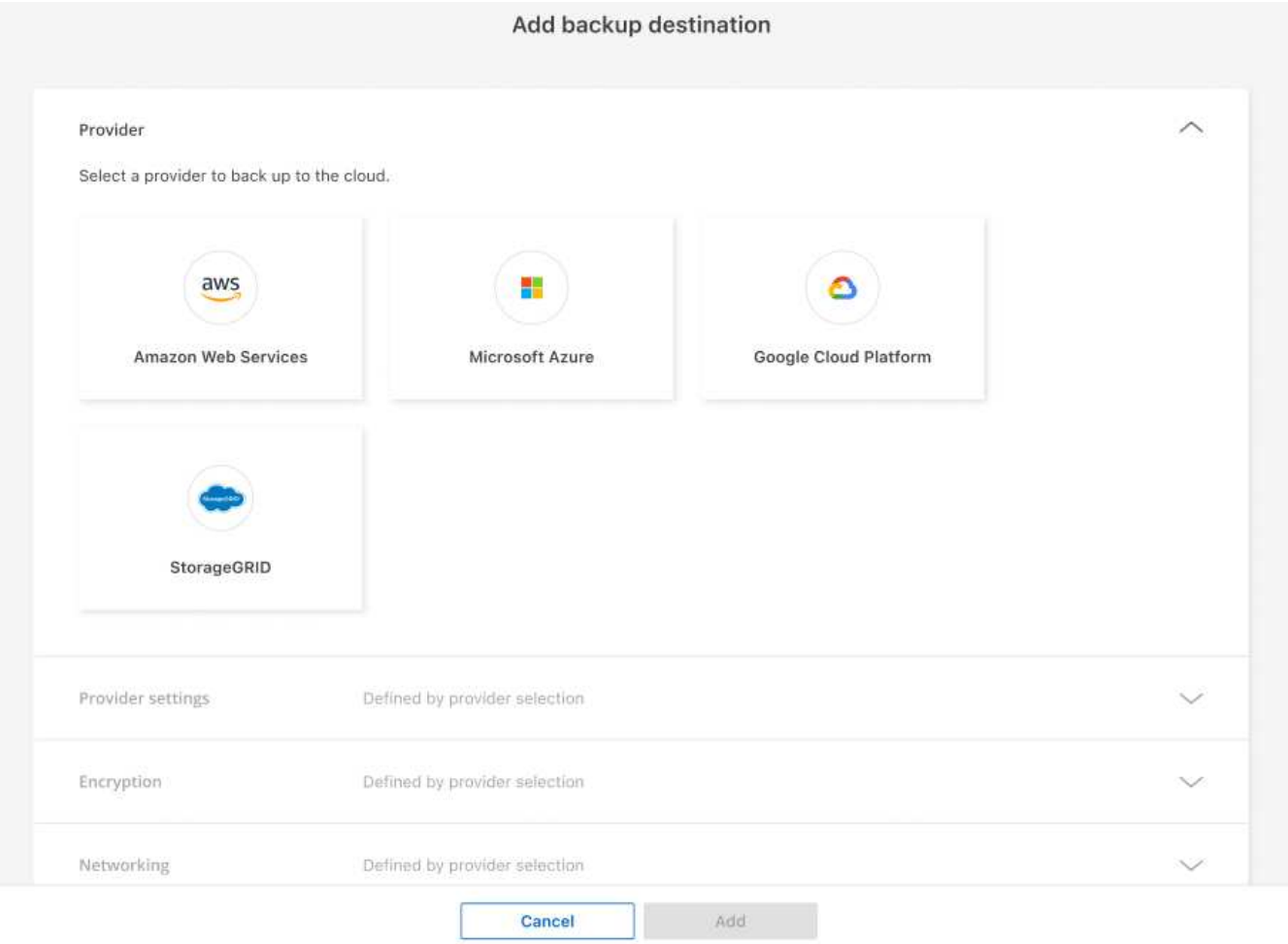
1. Dal menu di protezione dal ransomware BlueXP, seleziona il menu Vertical (verticale) … opzione in alto a destra.
2. Dal menu a discesa, selezionare **Impostazioni**.
3. Per aggiungere una destinazione di backup, selezionare **Aggiungi**.

Aggiungere StorageGRID come destinazione di backup

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

1. Nella pagina **Impostazioni > Destinazioni di backup**, selezionare **Aggiungi**.

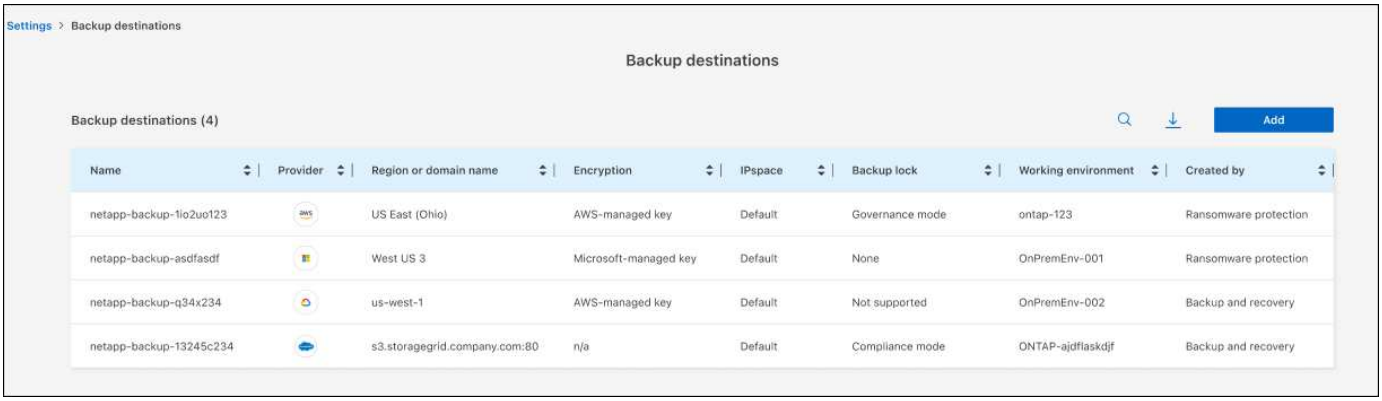
2. Immettere un nome per la destinazione di backup.



3. Selezionare **StorageGRID**.
4. Selezionare la freccia verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni provider**:
     - Creare un nuovo bucket o portare il proprio bucket che memorizzerà i backup.
     - Nodo gateway StorageGRID Nome di dominio, porta, chiave di accesso StorageGRID e credenziali chiave segreta completi.
   - **Networking**: Scegliere IPSpace.
     - IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
5. Selezionare **Aggiungi**.

Risultato

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

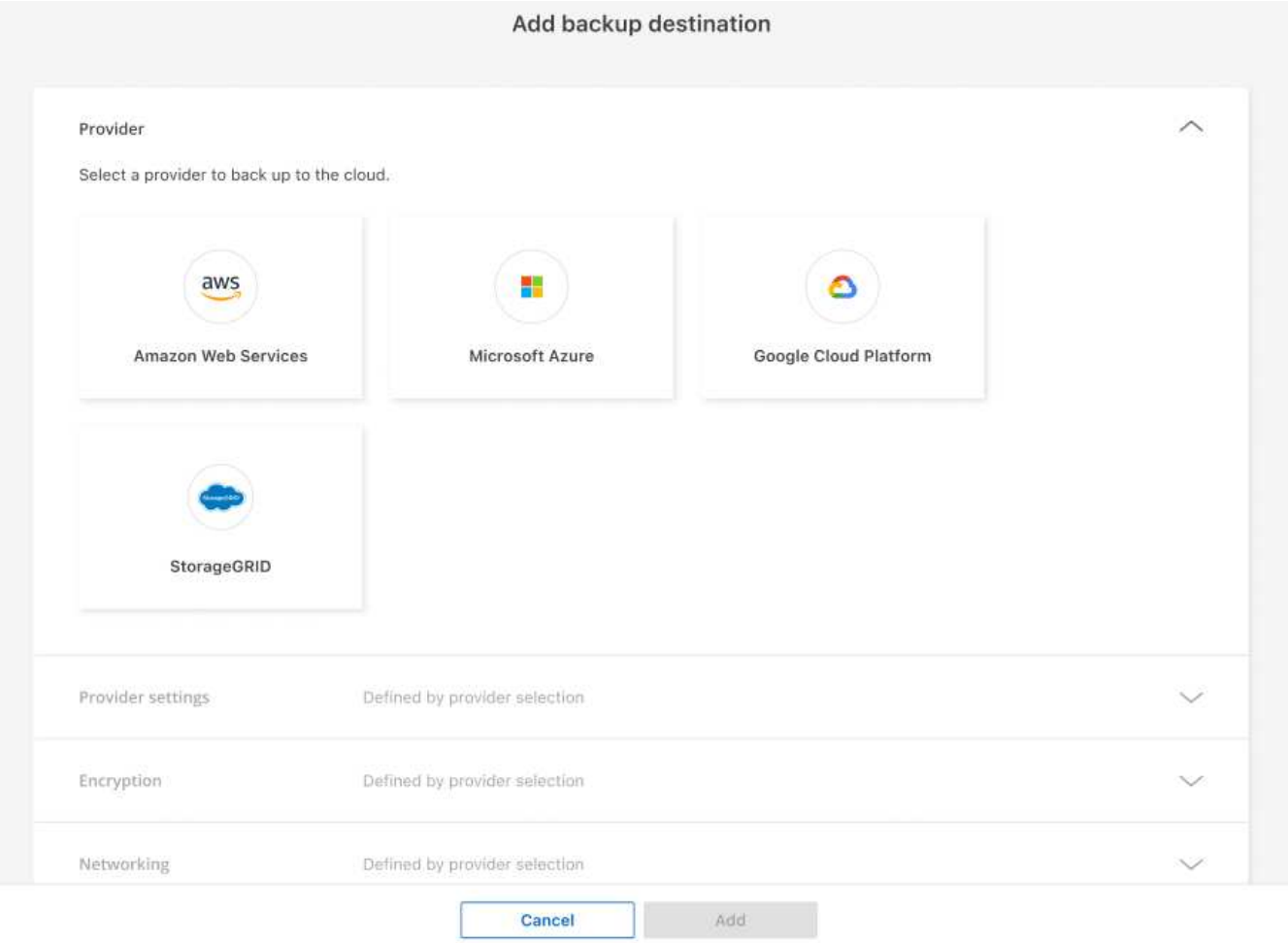


Aggiungere Amazon Web Services come destinazione di backup

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

Per informazioni sulla gestione dello storage AWS in BlueXP, fare riferimento a. "Gestisci i bucket Amazon S3".

1. Nella pagina **Impostazioni > Destinazioni di backup**, selezionare **Aggiungi**.
2. Immettere un nome per la destinazione di backup.



3. Selezionare **Amazon Web Services**.
4. Selezionare la freccia verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:

- **Impostazioni provider**:
  - Crea un nuovo bucket, seleziona un bucket esistente se già esistente in BlueXP o porta il tuo bucket in cui archiviare i backup.
  - Account AWS, regione, chiave di accesso e chiave segreta per le credenziali AWS

    "Se si desidera portare il proprio secchio, fare riferimento a Aggiungi S3 secchielli".

- **Crittografia**: Se si sta creando un nuovo bucket S3, immettere le informazioni sulla chiave di crittografia fornite dal provider. Se si sceglie un bucket esistente, le informazioni di crittografia sono già disponibili.

  I dati nel bucket sono criptati con chiavi gestite da AWS per impostazione predefinita. Puoi continuare a utilizzare le chiavi gestite da AWS oppure gestire la crittografia dei tuoi dati con le tue chiavi.

- **Rete**: Scegliere IPSpace e se si utilizza un endpoint privato.
  - IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
  - In alternativa, è possibile scegliere se utilizzare un endpoint privato AWS (PrivateLink) precedentemente configurato.

    Per utilizzare AWS PrivateLink, consultare la sezione "AWS PrivateLink per Amazon S3".

- **Blocco di backup**: Scegliere se si desidera che il servizio protegga i backup dalla modifica o dall'eliminazione. Questa opzione utilizza la tecnologia DataLock di NetApp. Ciascun backup verrà bloccato durante il periodo di conservazione o per un minimo di 30 giorni, più un periodo di buffer massimo di 14 giorni.

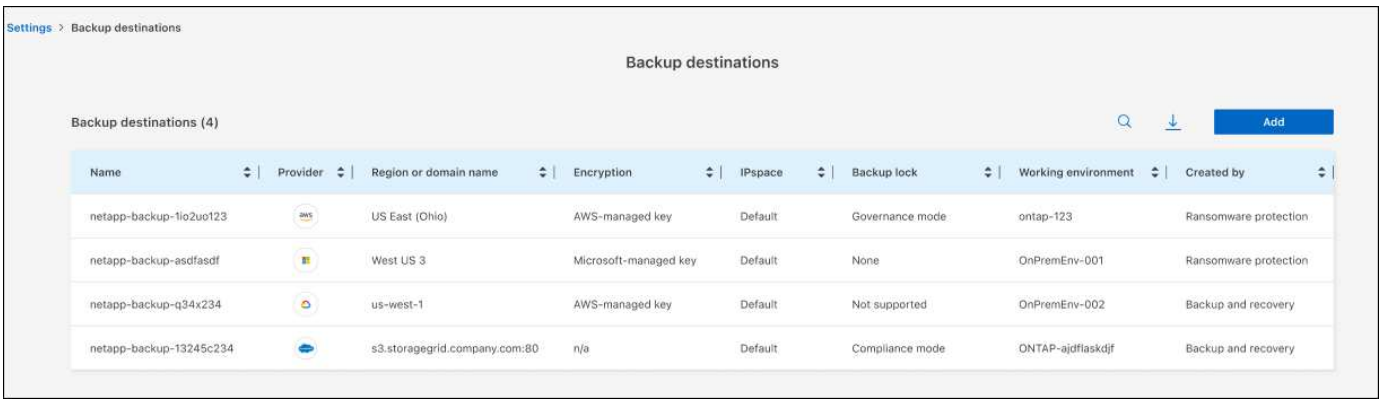
  > Se si configura ora l'impostazione del blocco di backup, non sarà possibile modificarla in un secondo momento dopo la configurazione della destinazione di backup.

  - **Governance mode**: Utenti specifici (con autorizzazione S3:BypassGovernanceRetention) possono sovrascrivere o eliminare i file protetti durante il periodo di conservazione.
  - **Modalità conformità**: Gli utenti non possono sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.

5. Selezionare **Aggiungi**.

Risultato

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

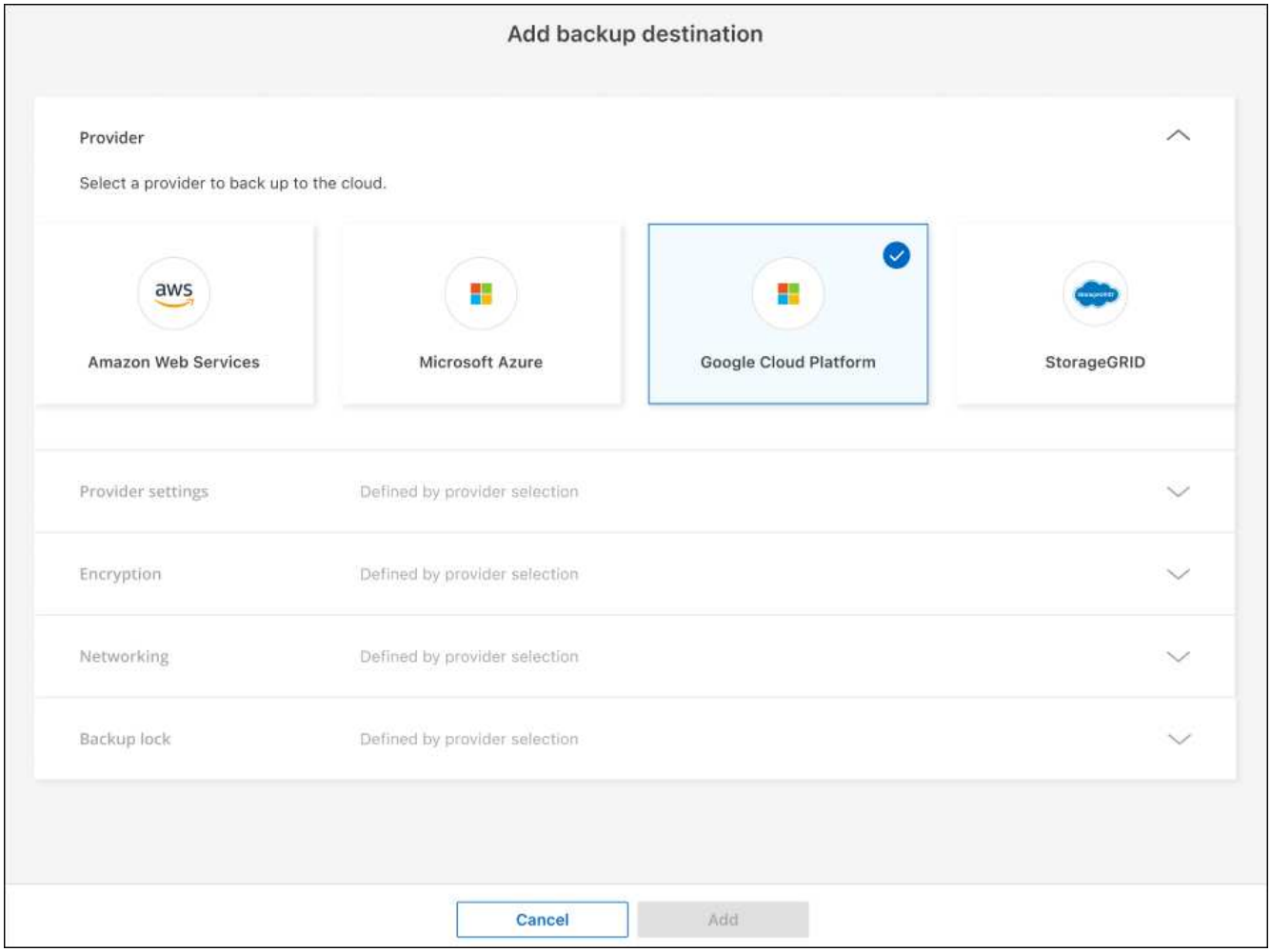


Aggiungi Google Cloud Platform come destinazione di backup

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

Per informazioni dettagliate sulla gestione dello storage GCP in BlueXP , fare riferimento alla "Opzioni di installazione del connettore in Google Cloud".

1. Nella pagina **Impostazioni > Destinazioni di backup**, selezionare **Aggiungi**.
2. Immettere un nome per la destinazione di backup.



3. Selezionare **Google Cloud Platform**.
4. Selezionare la freccia verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni provider**:
     - Creare un nuovo bucket. Immettere la chiave di accesso e la chiave segreta.
     - Immettere o selezionare il progetto e la regione di Google Cloud Platform.
   - **Crittografia**: Se si sta creando un nuovo bucket, immettere le informazioni sulla chiave di crittografia fornite dal provider. Se si sceglie un bucket esistente, le informazioni di crittografia sono già disponibili.

     Per impostazione predefinita, i dati nel bucket sono crittografati con chiavi gestite da Google. È possibile continuare a utilizzare le chiavi gestite da Google.

   - **Rete**: Scegliere IPSpace e se si utilizza un endpoint privato.

- IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
- In alternativa, è possibile scegliere se utilizzare un endpoint privato GCP (PrivateLink) precedentemente configurato.

5. Selezionare **Aggiungi**.

Risultato

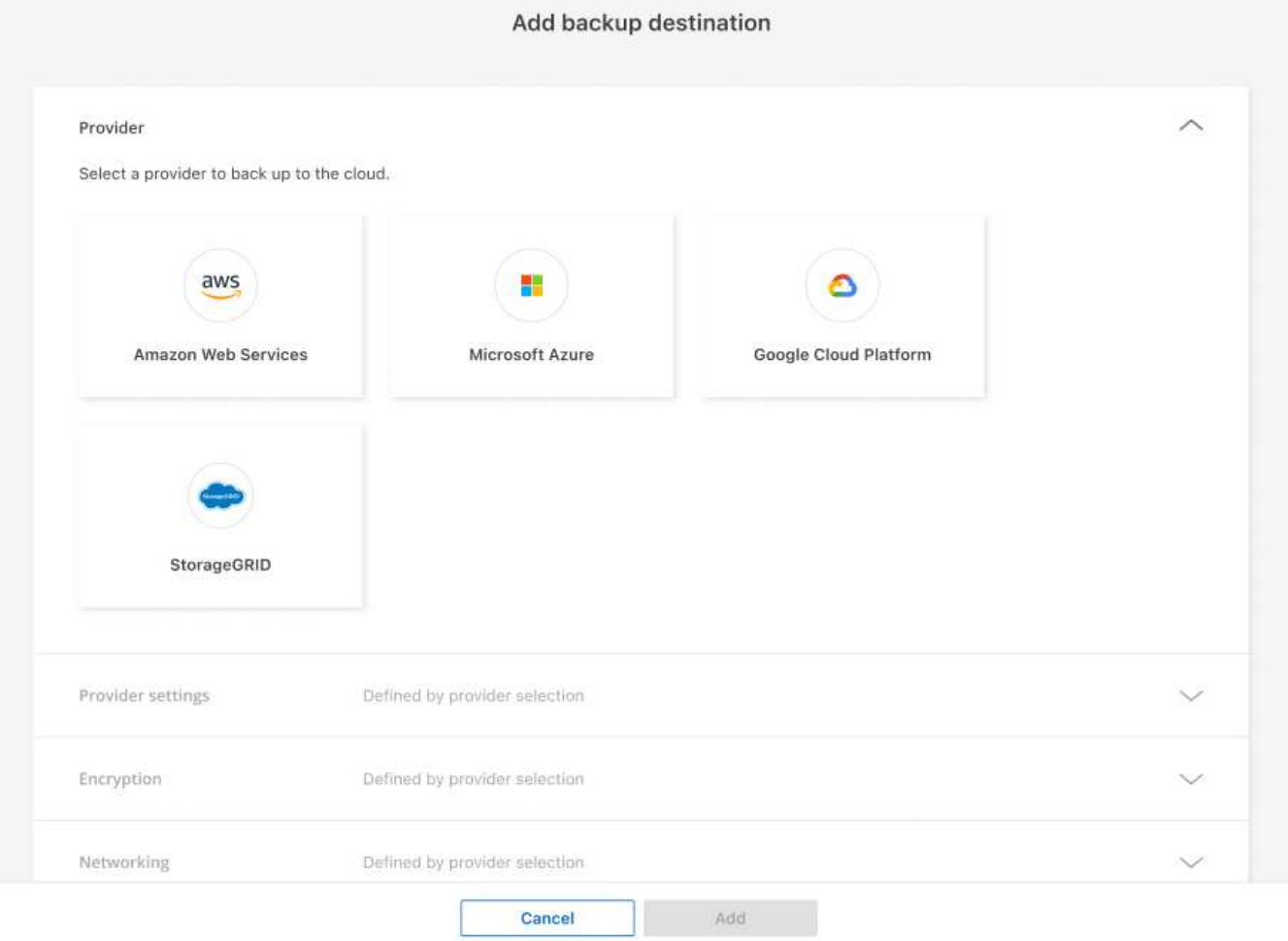
La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.

Aggiungere Microsoft Azure come destinazione di backup

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

Per informazioni sulla gestione delle credenziali di Azure e delle iscrizioni al marketplace in BlueXP, fare riferimento a. "Gestire le tue credenziali Azure e le iscrizioni al marketplace".

1. Nella pagina **Impostazioni > Destinazioni di backup**, selezionare **Aggiungi**.
2. Immettere un nome per la destinazione di backup.



3. Selezionare **Azure**.
4. Selezionare la freccia verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni provider**:

    - Crea un nuovo account storage, selezionane uno esistente (se già esistente) in BlueXP o crea un account storage proprietario che memorizzerà i backup.
    - Iscrizione, regione e gruppo di risorse di Azure per le credenziali Azure

      "Per trasferire il proprio account di storage, fare riferimento a Add Azure Blob storage accounts".

  - **Crittografia**: Se si crea un nuovo account di archiviazione, immettere le informazioni sulla chiave di crittografia fornite dal provider. Se si sceglie un account esistente, le informazioni sulla crittografia sono già disponibili.

    Per impostazione predefinita, i dati dell'account sono crittografati con chiavi gestite da Microsoft. Puoi continuare a utilizzare le chiavi gestite da Microsoft o gestire la crittografia dei tuoi dati con le tue chiavi.

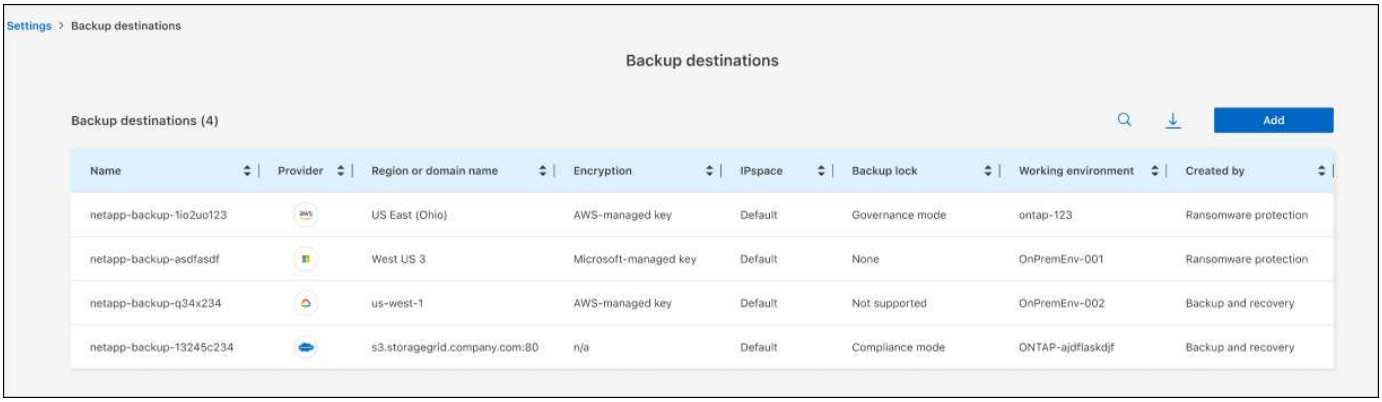
  - **Rete**: Scegliere IPSpace e se si utilizza un endpoint privato.
    - IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
    - Facoltativamente, scegliere se utilizzare un endpoint privato Azure precedentemente configurato.

      Se si desidera utilizzare Azure PrivateLink, consultare la sezione "Azure PrivateLink".

5. Selezionare **Aggiungi**.

Risultato

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



Attivare il rilevamento delle minacce

Puoi inviare automaticamente i dati al tuo sistema di gestione degli eventi e della sicurezza (SIEM) per l'analisi e il rilevamento delle minacce. Puoi selezionare AWS Security Hub o Splunk Cloud come tuo SIEM.

Prima di abilitare SIEM nella protezione dal ransomware BlueXP , devi configurare il tuo sistema SIEM.

Configurare AWS Security Hub per il rilevamento delle minacce

Prima di abilitare la protezione dal ransomware di AWS Security Hub in BlueXP , devi eseguire i seguenti passaggi generali nell'AWS Security Hub:

- Impostare le autorizzazioni in AWS Security Hub.
- Configurare la chiave di accesso e la chiave segreta di autenticazione nell'AWS Security Hub. (Questi

passaggi non sono forniti qui).

Procedura per impostare le autorizzazioni in AWS Security Hub

1. Vai a **Console IAM AWS**.
2. Selezionare **Criteri**.
3. Creare un criterio utilizzando il seguente codice in formato JSON:

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

Configura Splunk Cloud per il rilevamento delle minacce

Prima di abilitare la protezione dal ransomware Splunk Cloud in BlueXP , dovrai eseguire le seguenti operazioni di alto livello in Splunk Cloud:

- Abilitare un servizio di raccolta eventi HTTP in Splunk Cloud per ricevere dati degli eventi tramite HTTP o HTTPS da BlueXP .
- Creare un token di raccolta eventi in Splunk Cloud.

Procedura per attivare un agente di raccolta eventi HTTP in Splunk

1. Vai a Splunk Cloud.
2. Selezionare **Impostazioni** > **ingressi dati**.
3. Selezionare **HTTP Event Collector** > **Impostazioni globali**.
4. Nell'interruttore tutti i token, selezionare **abilitato**.
5. Per fare in modo che Event Collector ascolti e comunichi su HTTPS piuttosto che su HTTP, selezionare **Abilita SSL**.
6. Immettere una porta in **numero porta HTTP** per il modulo di raccolta eventi HTTP.

Procedura per creare un token di raccolta eventi in Splunk

1. Vai a Splunk Cloud.

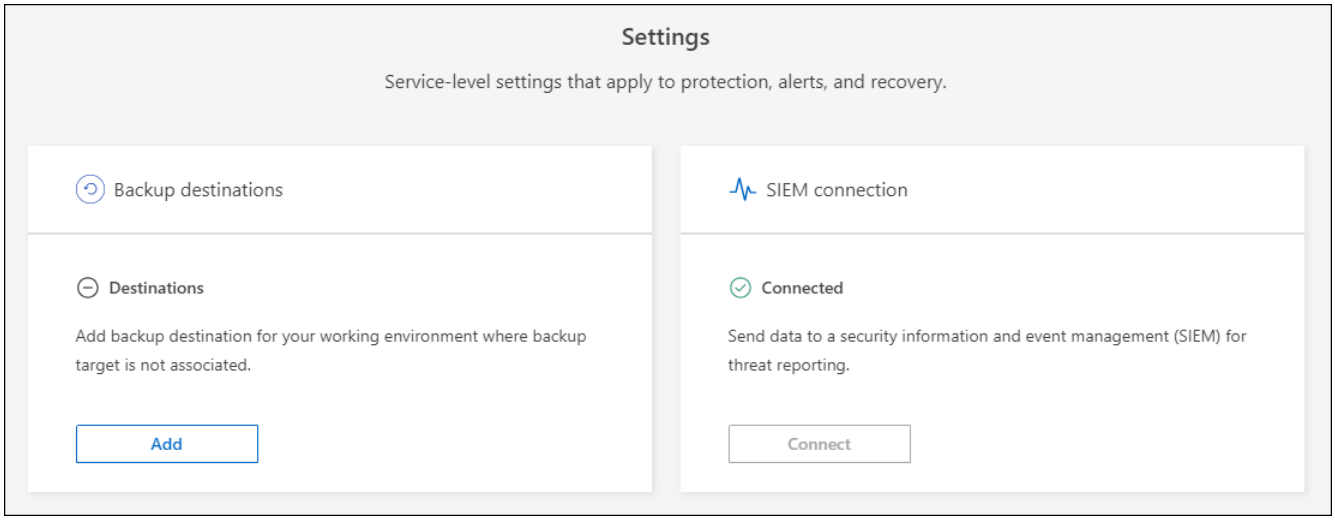
2. Selezionare **Impostazioni** > **Aggiungi dati**.
3. Selezionare **Monitor** > **HTTP Event Collector**.
4. Immettere un nome per il token e selezionare **Avanti**.
5. Selezionare un **Indice predefinito** in cui verranno inviati gli eventi, quindi selezionare **Rivedi**.
6. Verificare che tutte le impostazioni per l'endpoint siano corrette, quindi selezionare **Invia**.
7. Copiare il token e incollarlo in un altro documento per prepararlo all'operazione di autenticazione.

Connetti SIEM alla protezione dal ransomware BlueXP

Attivando SIEM, i dati dalla protezione anti-ransomware BlueXP vengono inviati al server SIEM per l'analisi e il reporting delle minacce.

1. Dal menu BlueXP , seleziona **protezione** > **protezione anti-ransomware**.
2. Dal menu di protezione dal ransomware BlueXP, seleziona il menu Vertical (verticale) … opzione in alto a destra.
3. Selezionare **Impostazioni**.

   Viene visualizzata la pagina Impostazioni.



4. Nella pagina Impostazioni, selezionare **Connetti** nel riquadro di connessione SIEM.
5. Scegliere uno dei sistemi SIEM.
6. Inserisci il token e i dettagli di autenticazione configurati in AWS Security Hub o Splunk Cloud.

   Le informazioni immesse dipendono dal SIEM selezionato.

7. Selezionare **Abilita**.

   Nella pagina Impostazioni viene visualizzato "connesso".

Scollegare SIEM

La disconnessione di SIEM impedisce al servizio di inviare dati al server SIEM.

Fasi

1. Dal menu BlueXP , seleziona **protezione** > **protezione anti-ransomware**.
2. Dal menu di protezione dal ransomware BlueXP, seleziona il menu Vertical (verticale) … opzione in alto a destra.
3. Selezionare **Impostazioni**.
4. Nel riquadro di connessione SIEM, selezionare **Disconnetti**.
5. Nella pagina di conferma, selezionare **Disconnetti**.

Domande frequenti sulla protezione dal ransomware BlueXP

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Implementazione

Ti serve una licenza per usare la protezione da ransomware di BlueXP?

È possibile utilizzare i seguenti tipi di licenza:

- Iscriviti per una prova gratuita di 90 giorni.
- A breve potrai acquistare un abbonamento pay-as-you-go (PAYGO) con Amazon Web Services (AWS) Marketplace.
- Presto sarà possibile portare la propria licenza (BYOL), ovvero un file di licenza NetApp (NLF) che si ottiene dal proprio rappresentante di vendita NetApp Puoi utilizzare il numero di serie della licenza per attivare il BYOL nel Digital Wallet di BlueXP.

In che modo abiliti la protezione dal ransomware BlueXP?
La protezione dal ransomware di BlueXP non richiede alcuna abilitazione. L'opzione di protezione dal ransomware viene automaticamente abilitata nel sistema di navigazione BlueXP a sinistra.

Per iniziare, devi iscriverti o contattare il tuo rappresentante commerciale NetApp per provare questo servizio. Quindi, quando si utilizza il connettore BlueXP, esso includerà le funzionalità appropriate per il servizio.

Per iniziare con la protezione ransomware di BlueXP , fai clic su "inizia a rilevare i workload" nella sua landing page iniziale.

La protezione anti-ransomware BlueXP è disponibile in modalità standard, limitata e privata? Al momento, la protezione dal ransomware di BlueXP è disponibile solo in modalità standard. Continua a seguirci per saperne di più.

Per una spiegazione di queste modalità in tutti i servizi BlueXP, fare riferimento a. "Modalità di implementazione di BlueXP".

Accesso

Qual è l'URL di protezione dal ransomware BlueXP?
Per l'URL, in un browser, immettere: "https://console.bluexp.netapp.com/" Per accedere alla console BlueXP.

Come vengono gestite le autorizzazioni di accesso? Solo gli amministratori dell'organizzazione possono

avviare il servizio e rilevare i carichi di lavoro (perché comporta l'utilizzo di una risorsa). Le interazioni successive possono essere effettuate da qualsiasi ruolo.

Qual è la migliore risoluzione del dispositivo? La risoluzione consigliata del dispositivo per la protezione dal ransomware BlueXP è di 1920x1080 o superiore.

Quale browser devo utilizzare? Qualsiasi browser moderno funzionerà.

Interazione con altri servizi

La protezione dal ransomware di BlueXP è a conoscenza delle impostazioni di protezione di NetApp ONTAP?
Sì, la protezione dal ransomware BlueXP rileva le pianificazioni Snapshot impostate in ONTAP.

Se imposti una policy utilizzando la protezione dal ransomware di BlueXP, devi apportare modifiche future solo in questo servizio?
Ti consigliamo di apportare modifiche alla policy dal servizio di protezione dal ransomware di BlueXP.

In che modo la protezione ransomware BlueXP interagisce con il backup e il ripristino di BlueXP e con SnapCenter?

La protezione dal ransomware di BlueXP utilizza i seguenti prodotti e servizi:

- Backup e recovery di BlueXP per rilevare e impostare policy di backup e snapshot per i carichi di lavoro di condivisioni di file
- SnapCenter o SnapCenter per VMware per rilevare e impostare policy di backup e snapshot per applicazioni e carichi di lavoro delle VM.

Inoltre, la protezione dal ransomware BlueXP utilizza il backup e recovery di BlueXP e SnapCenter / SnapCenter per VMware per eseguire recovery coerente con file e carico di lavoro.

Carichi di lavoro

Che cosa costituisce un carico di lavoro? Un carico di lavoro è un'applicazione, una macchina virtuale o una condivisione di file. Un carico di lavoro include tutti i volumi utilizzati da una singola istanza dell'applicazione. Ad esempio, un'istanza di Oracle DB implementata in ora3.host.com può avere vol1 GB e vol2 GB rispettivamente per dati e registri. Questi volumi costituiscono insieme il carico di lavoro per quella specifica istanza dell'istanza del database Oracle.

In che modo la protezione dal ransomware di BlueXP assegna la priorità ai dati del carico di lavoro?
La priorità dei dati è determinata dalle copie Snapshot create e dai backup pianificati.

La priorità del carico di lavoro (critico, standard, importante) è determinata dalle frequenze di Snapshot già applicate a ciascun volume associato al carico di lavoro.

"Scopri la priorità o l'importanza del carico di lavoro".

Quali workload supporta la protezione ransomware BlueXP ?

La protezione ransomware di BlueXP è in grado di identificare i seguenti workload: Oracle, MySQL, file share, VM e datastore VM.

Inoltre, se il cliente utilizza SnapCenter o SnapCenter per VMware, tutti i workload supportati da questi prodotti sono anche identificati nella protezione dal ransomware BlueXP e nella protezione dal ransomware BlueXP

possono proteggere e ripristinare i dati in modo coerente con il carico di lavoro.

Come si associano i dati a un carico di lavoro?

La protezione ransomware BlueXP associa i dati a un carico di lavoro nei seguenti modi:

- La protezione ransomware BlueXP rileva i volumi e le estensioni dei file e li associa al carico di lavoro appropriato.
- Inoltre, se disponi di SnapCenter o SnapCenter per VMware e hai configurato i workload nel backup e recovery di BlueXP , la protezione dal ransomware BlueXP scopre i workload gestiti da SnapCenter e SnapCenter per VMware e i loro volumi associati.

Che cos'è un carico di lavoro "protetto"? Nella protezione ransomware di BlueXP , un carico di lavoro mostra uno stato "protetto" quando ha una policy di rilevamento principale abilitata. Per ora, ciò significa che ARP è abilitato su tutti i volumi correlati al carico di lavoro.

Che cos'è un carico di lavoro "a rischio"? Se un carico di lavoro non ha abilitata una policy di rilevamento primaria, è "a rischio" anche se ha abilitata una policy di backup e snapshot.

Nuovo volume aggiunto, ma non ancora visualizzato se è stato aggiunto un nuovo volume all'ambiente, avviare nuovamente il rilevamento e applicare i criteri di protezione per proteggere il nuovo volume.

Il Dashboard non mostra tutti i miei workload. Che cosa potrebbe essere sbagliato? Al momento sono supportati solo volumi NFS e CIFS. I volumi iSCSI e altre configurazioni non supportate vengono filtrati e non vengono visualizzati nella dashboard.

Policy di protezione

Le policy ransomware di BlueXP coesistono con altri tipi di policy dei workload?
Al momento, il backup e recovery di BlueXP (Cloud Backup) supporta una policy di backup per ogni volume. Pertanto, il backup e recovery di BlueXP e la protezione dal ransomware di BlueXP condividono le policy di backup.

Le copie Snapshot non sono limitate e possono essere aggiunte separatamente da ciascun servizio.

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.

La protezione dal ransomware di BlueXP è a conoscenza delle impostazioni di protezione di NetApp ONTAP?

Sì, la protezione ransomware BlueXP rileva le pianificazioni delle snapshot impostate in ONTAP e se ARP e FPolicy sono abilitati in tutti i volumi di un carico di lavoro rilevato. Le informazioni visualizzate inizialmente nella dashboard sono aggregate da altre soluzioni e prodotti NetApp.

La protezione dal ransomware BlueXP è consapevole delle policy già adottate in backup e recovery di BlueXP e SnapCenter?

Sì, se hai workload gestiti in backup e recovery di BlueXP o SnapCenter, le policy gestite da questi prodotti sono integrate nella protezione dal ransomware di BlueXP .

È possibile modificare i criteri riportati dal backup e ripristino di BlueXP e/o da SnapCenter?

No, non puoi modificare le policy gestite dal backup e recovery di BlueXP o dal SnapCenter all'interno della protezione dal ransomware di BlueXP . Eventuali modifiche a tali criteri vengono gestite in backup e ripristino di BlueXP o SnapCenter.

Se esistono policy di ONTAP (già attivate in Gestione sistema come ARP, FPolicy e snapshot), sono state modificate quelle nella protezione ransomware di BlueXP ?

1. La protezione dal ransomware BlueXP non modifica alcuna policy di rilevamento esistente (ARP, impostazioni FPolicy) da ONTAP.

Cosa succede se Aggiungi nuove policy nel backup e ripristino di BlueXP o in SnapCenter dopo aver effettuato la registrazione alla protezione dal ransomware di BlueXP ?

La protezione dal ransomware BlueXP riconosce qualsiasi nuova policy creata in backup e recovery di BlueXP o SnapCenter.

È possibile modificare le policy da ONTAP?

Sì, puoi modificare le policy di ONTAP nella protezione dal ransomware BlueXP . Puoi anche creare nuove policy nella protezione dal ransomware di BlueXP e applicarle ai carichi di lavoro. Questa azione sostituisce le policy ONTAP esistenti con quelle create nella protezione dal ransomware BlueXP .

È possibile disabilitare i criteri?

È possibile disattivare ARP nei criteri di rilevamento utilizzando l'interfaccia utente, le API o la CLI di System Manager.

È possibile disattivare FPolicy e i criteri di backup applicando un criterio diverso che non li include.

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.

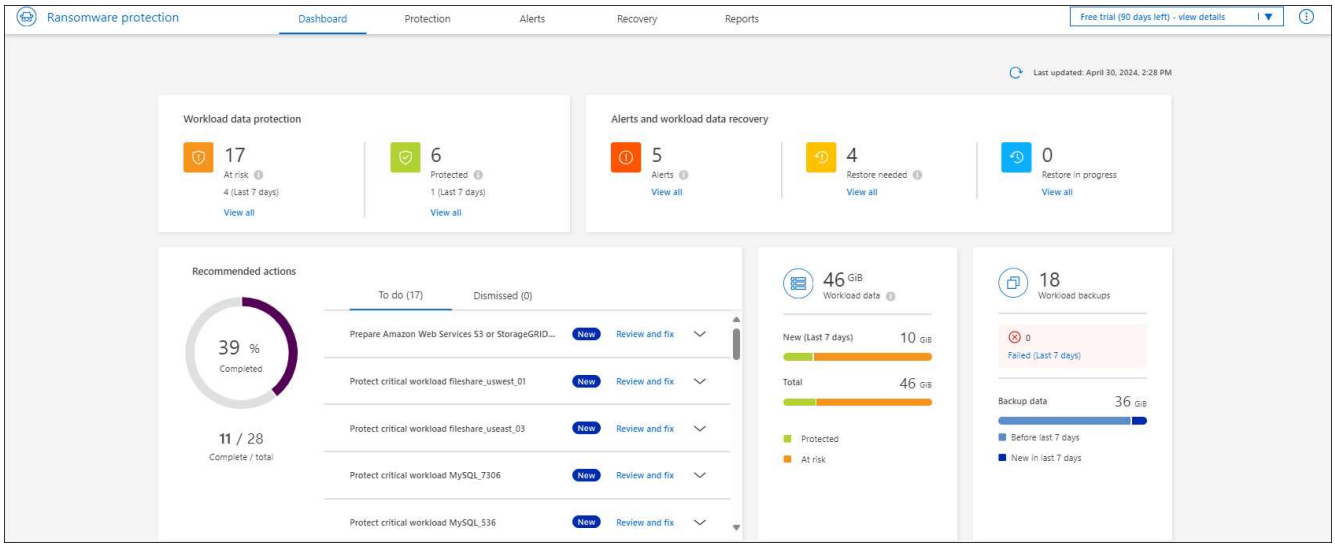
Puoi anche utilizzare la dashboard per esaminare e agire in base ai consigli sulla protezione, accedere alle impostazioni globali, scaricare i report e accedere a questa documentazione tecnica.

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:

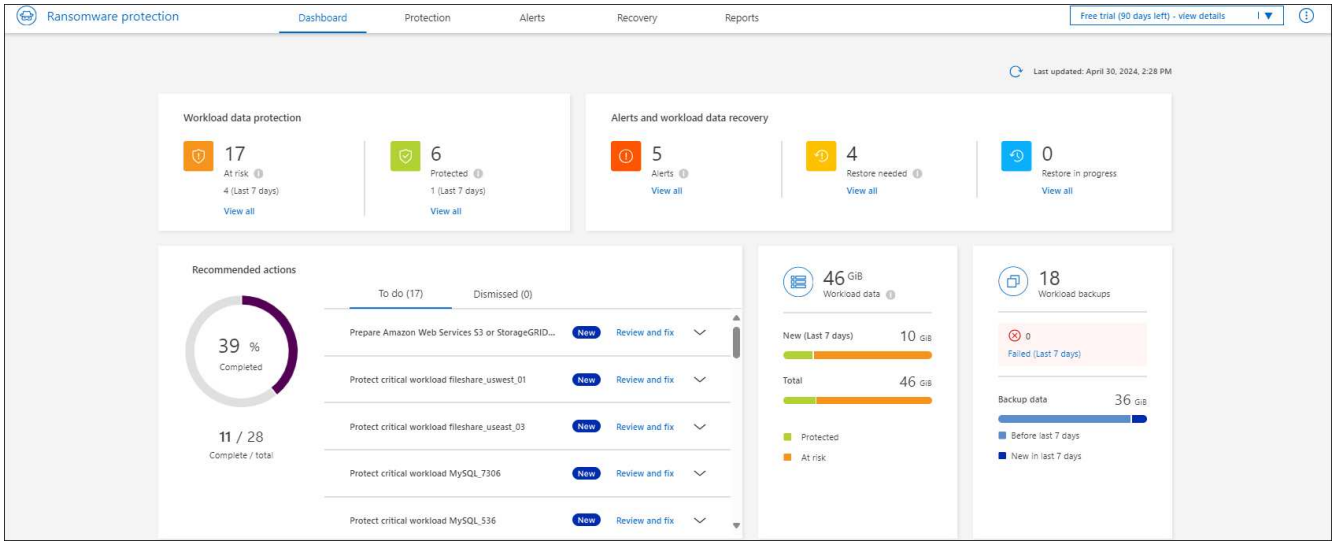
- **Protezione**: Contiene lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale protetto e a rischio.
- **Avvisi**: Include lo stato e i dettagli di tutti gli avvisi, compreso il numero totale di avvisi e istantanee automatiche.
- **Recovery**: Include lo stato e i dettagli di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

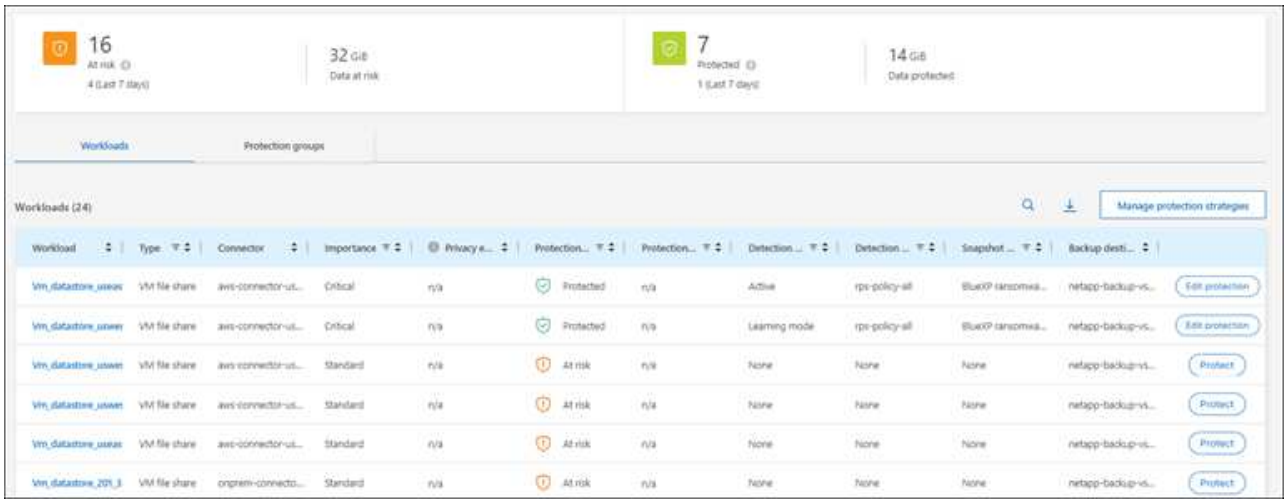
Visualizza la protezione dal ransomware su un carico di lavoro

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.

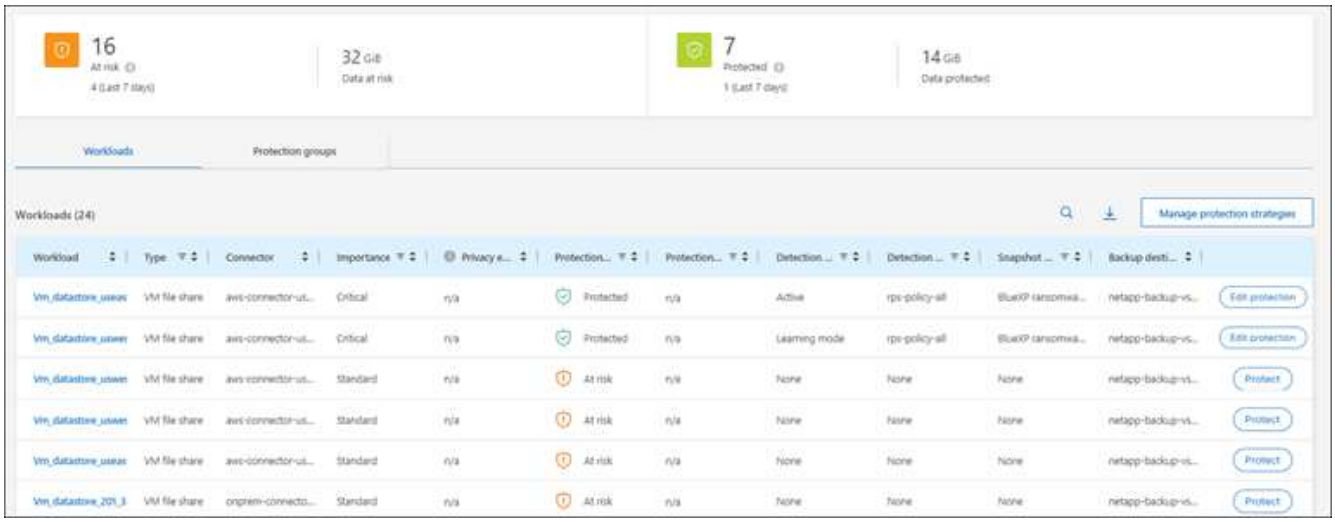
Creare una strategia di protezione dal ransomware (se non disponi di policy di backup o snapshot)

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

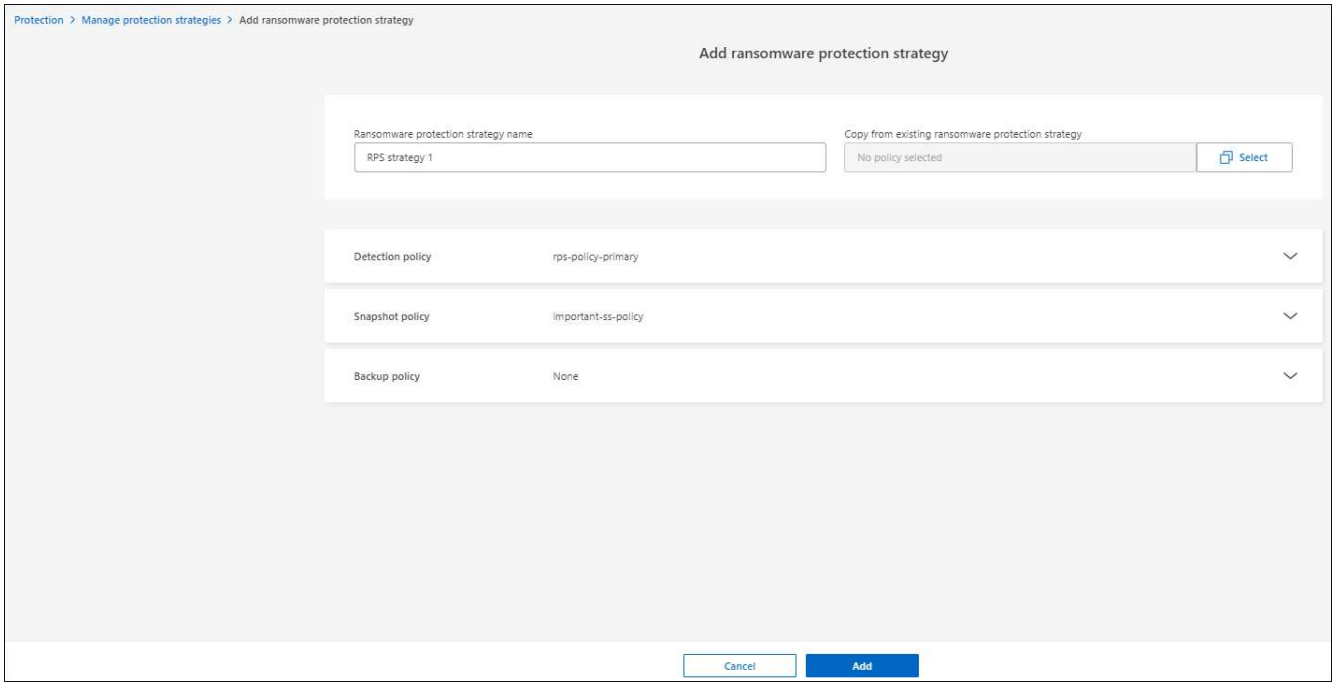
Passaggi per creare una strategia di protezione dal ransomware

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

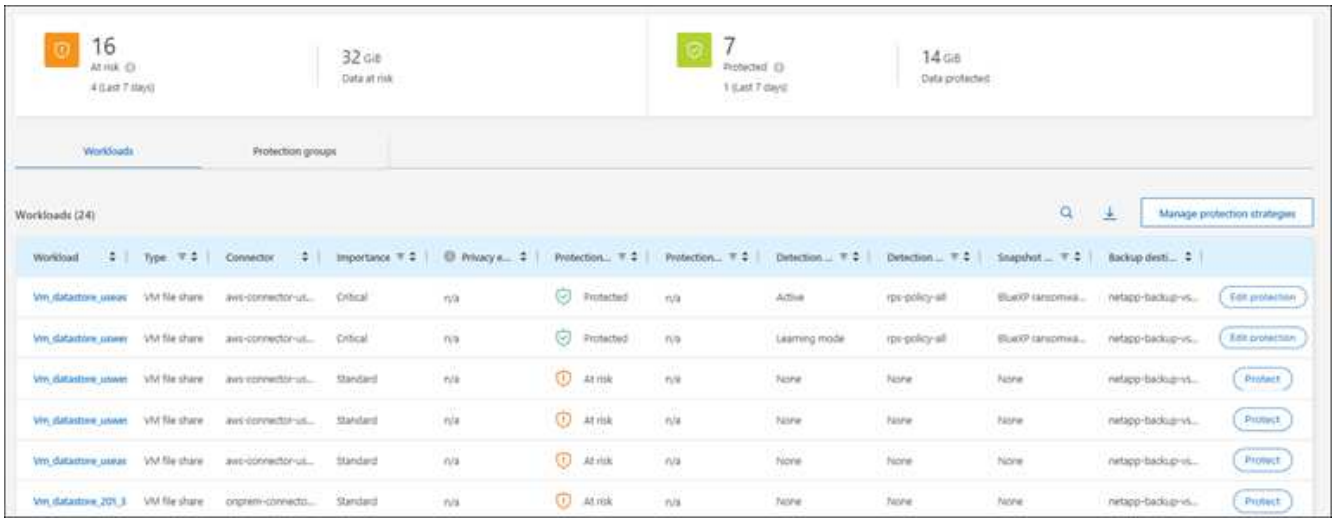
Con la protezione dal ransomware di BlueXP puoi assegnare una policy di rilevamento del ransomware a workload che dispongono già di policy di backup e snapshot, gestite in altri prodotti o servizi NetApp. Il criterio di rilevamento non modifica i criteri gestiti in altri prodotti.

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

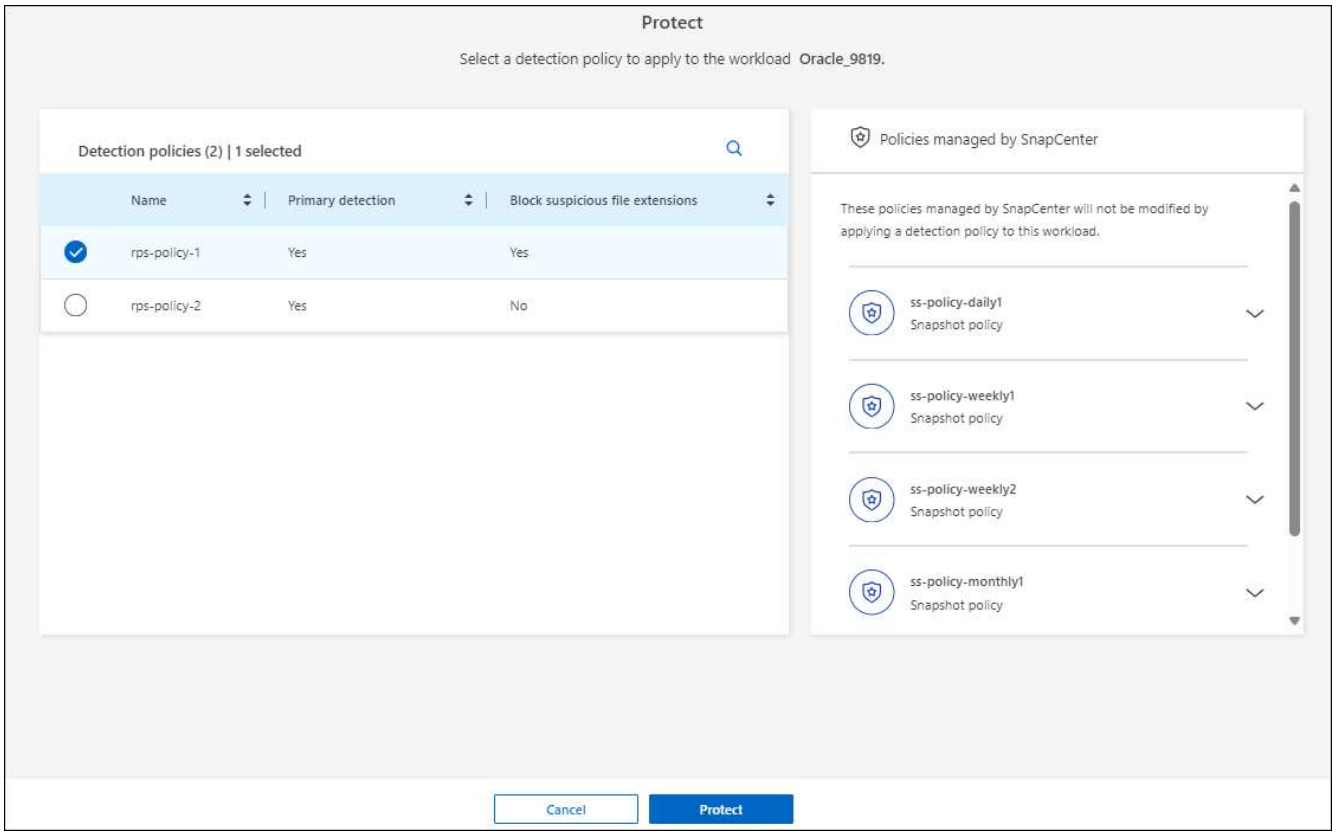
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



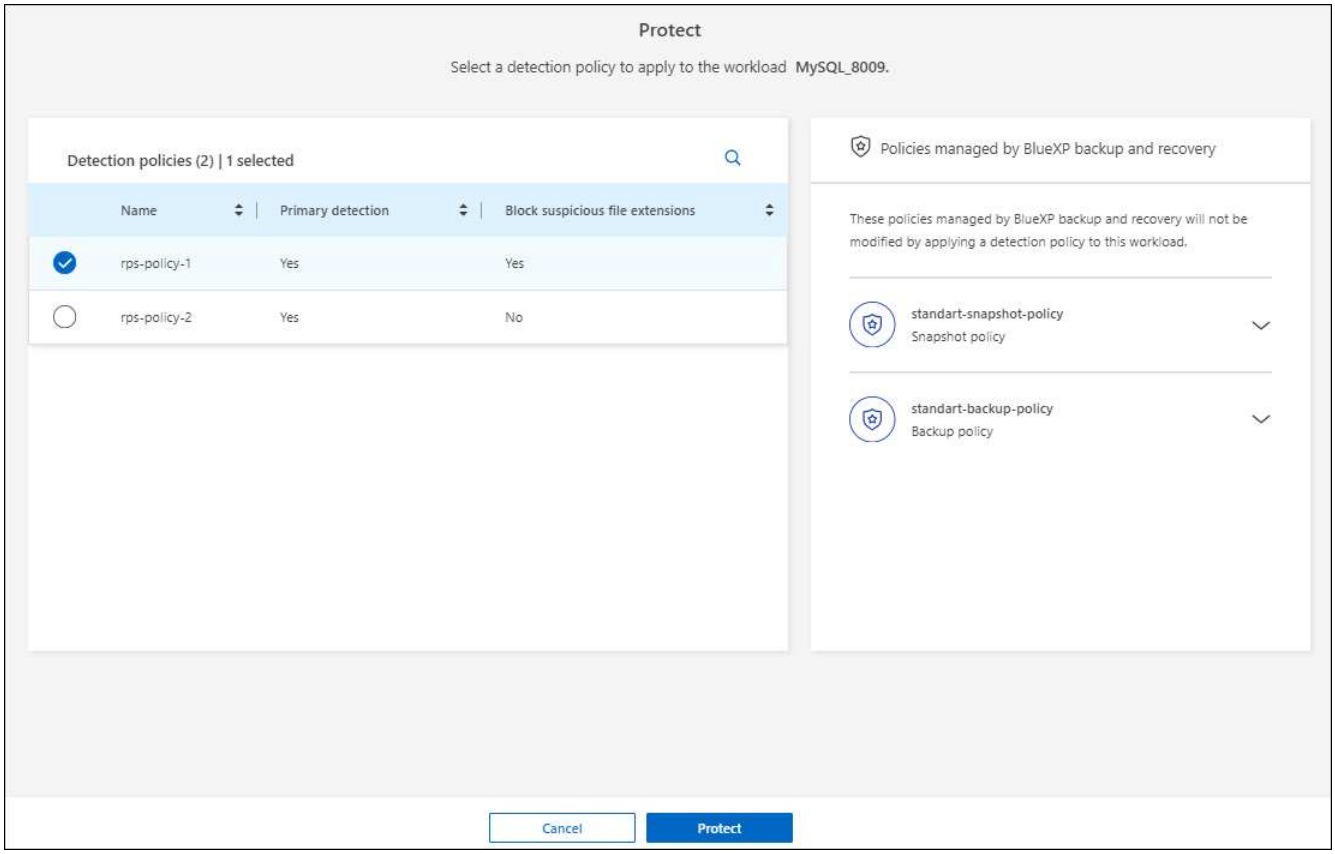
2. Nella pagina protezione, selezionare un carico di lavoro e selezionare **Proteggi**.

   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

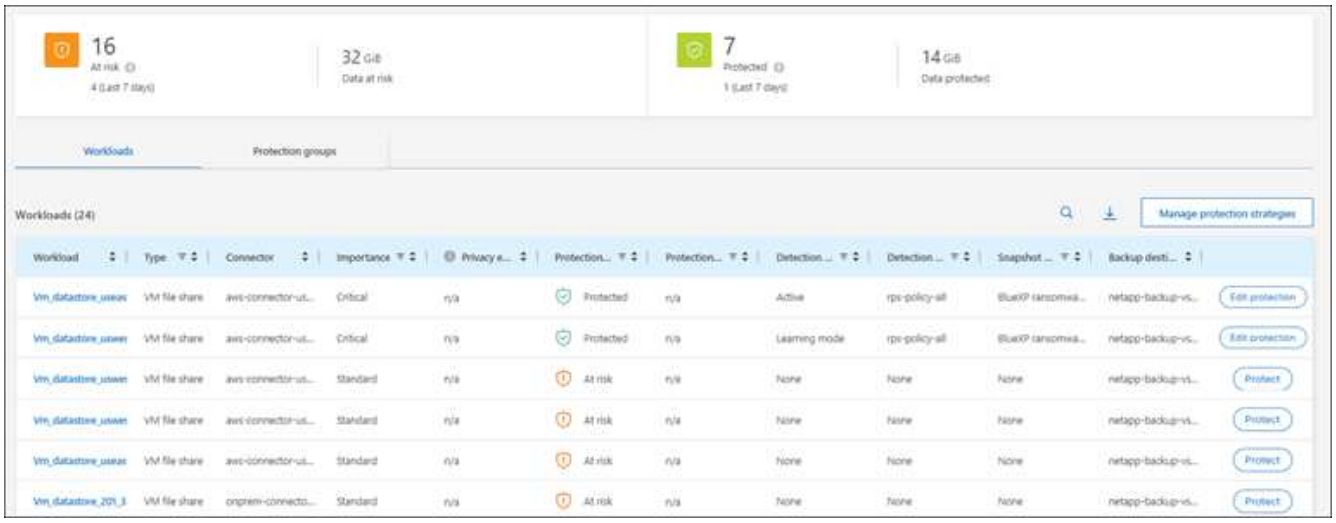
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, nella riga del carico di lavoro, selezionare **Modifica protezione**.
3. Nella pagina Criteri, fare clic sulla freccia verso il basso relativa al criterio che si desidera assegnare per rivedere i dettagli.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

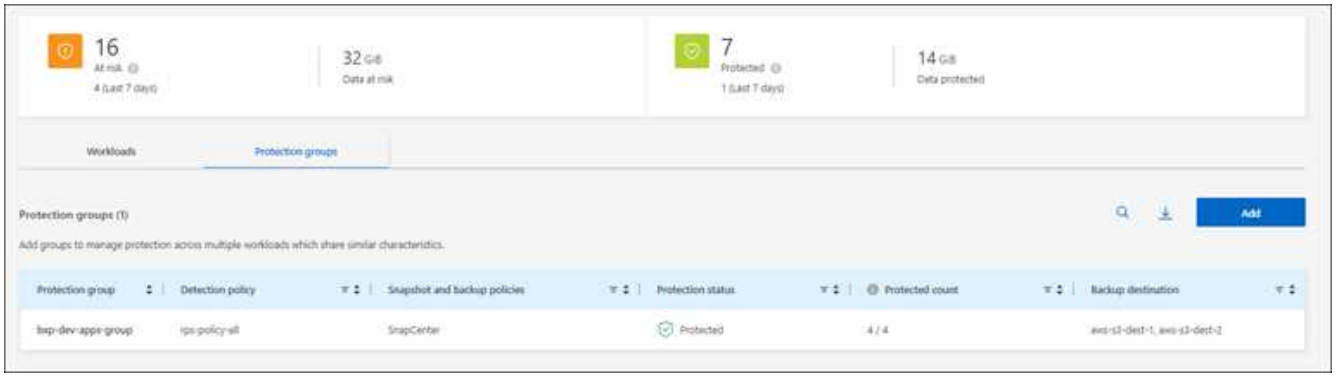
Il raggruppamento delle condivisioni dei file semplifica la protezione dell'ambiente dati. Il servizio consente di proteggere contemporaneamente tutti i volumi di un gruppo piuttosto che proteggere ogni volume separatamente.

Fasi

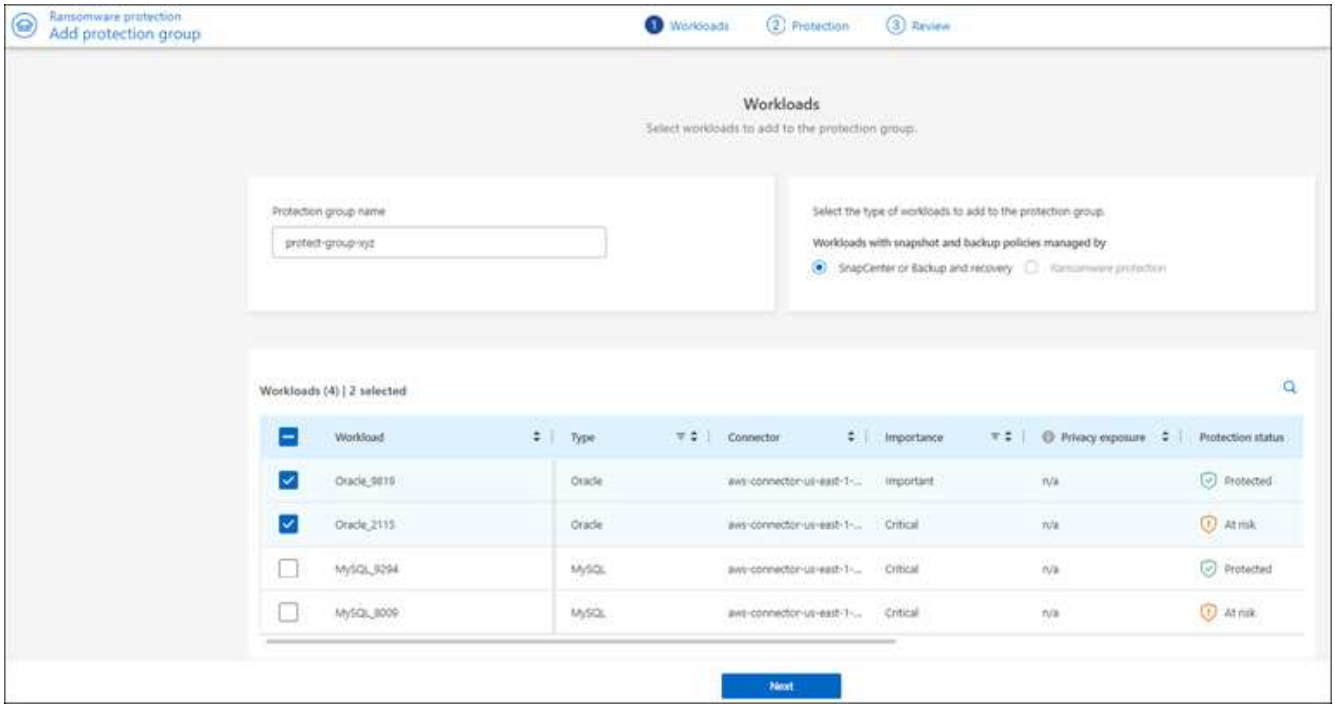
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



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



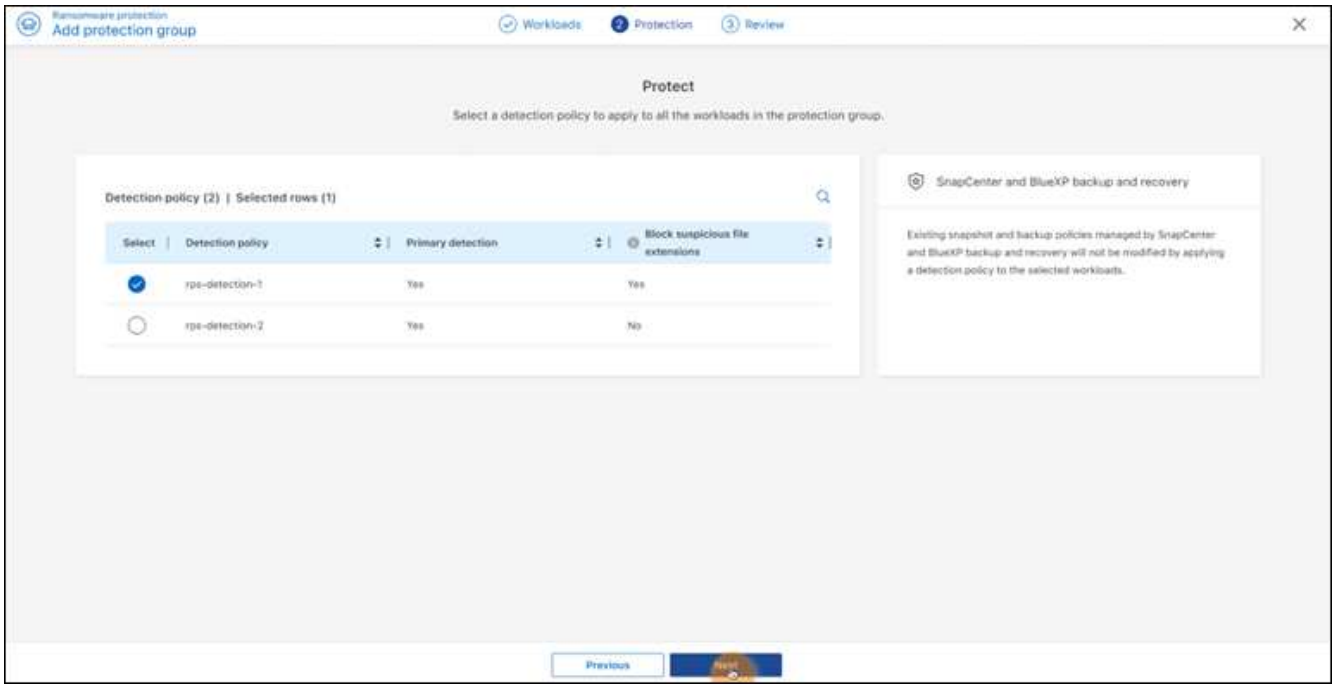
3. Selezionare **Aggiungi**.



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**.

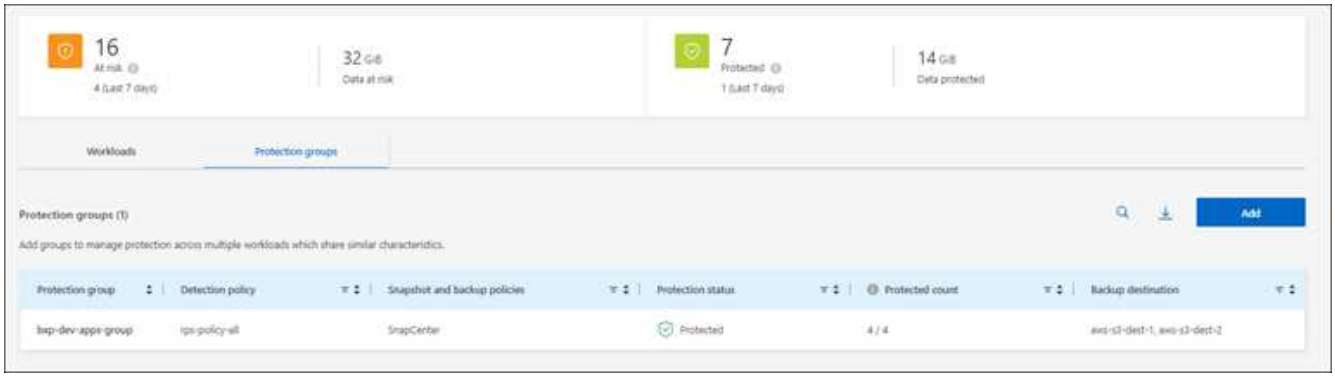
Aggiungere altri carichi di lavoro a un gruppo

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

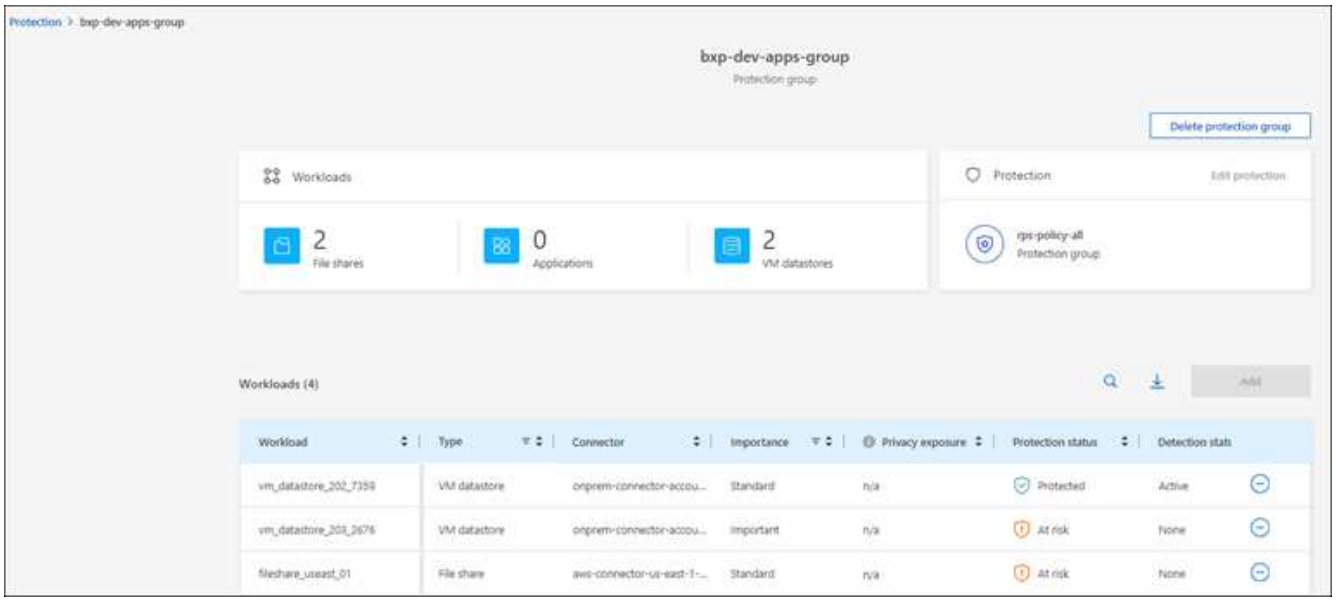
Se il gruppo include carichi di lavoro gestiti solo dalla protezione anti-ransomware BlueXP (e non dal backup e recovery di SnapCenter o BlueXP), dovresti utilizzare gruppi separati per i carichi di lavoro gestiti solo dalla protezione anti-ransomware BlueXP e un altro gruppo per i carichi di lavoro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

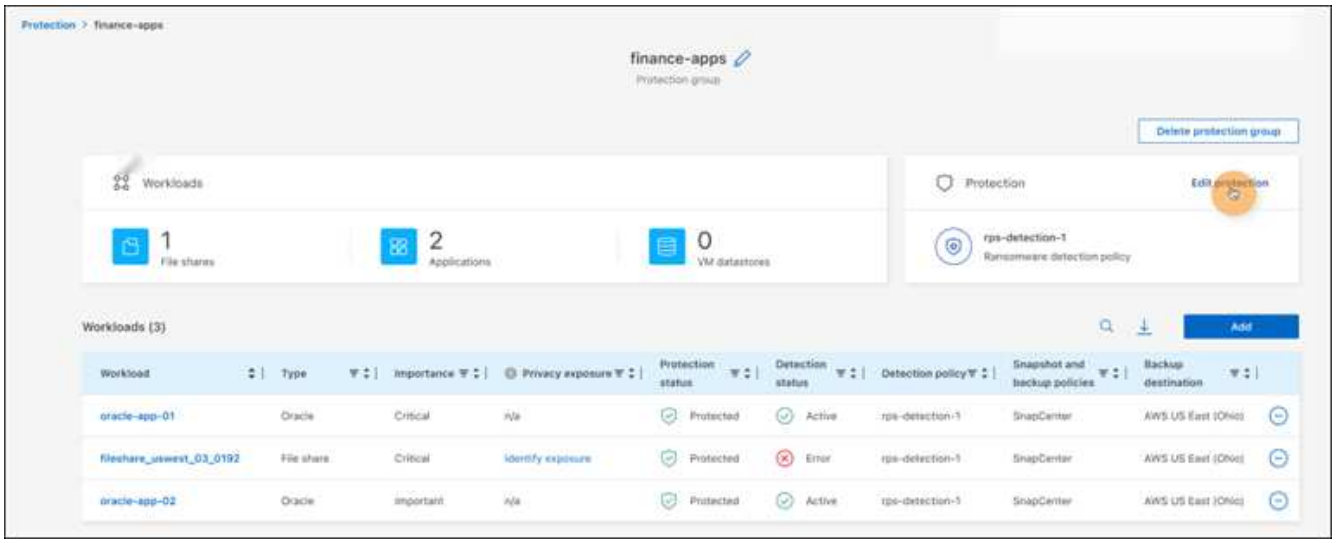
5. Selezionare i carichi di lavoro aggiuntivi da aggiungere al gruppo.
6. Selezionare **Salva**.

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**.



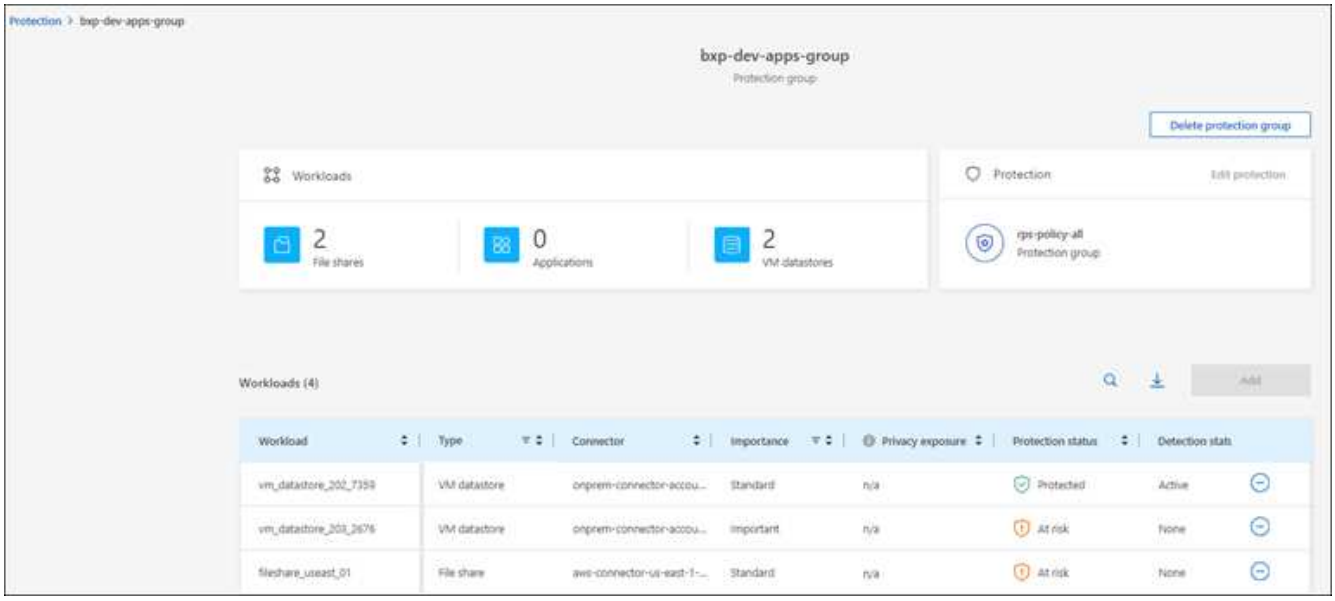
3. Dal riquadro protezione, selezionare **Modifica protezione**.
4. Selezionare o aggiungere un criterio di rilevamento a questo gruppo.

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.



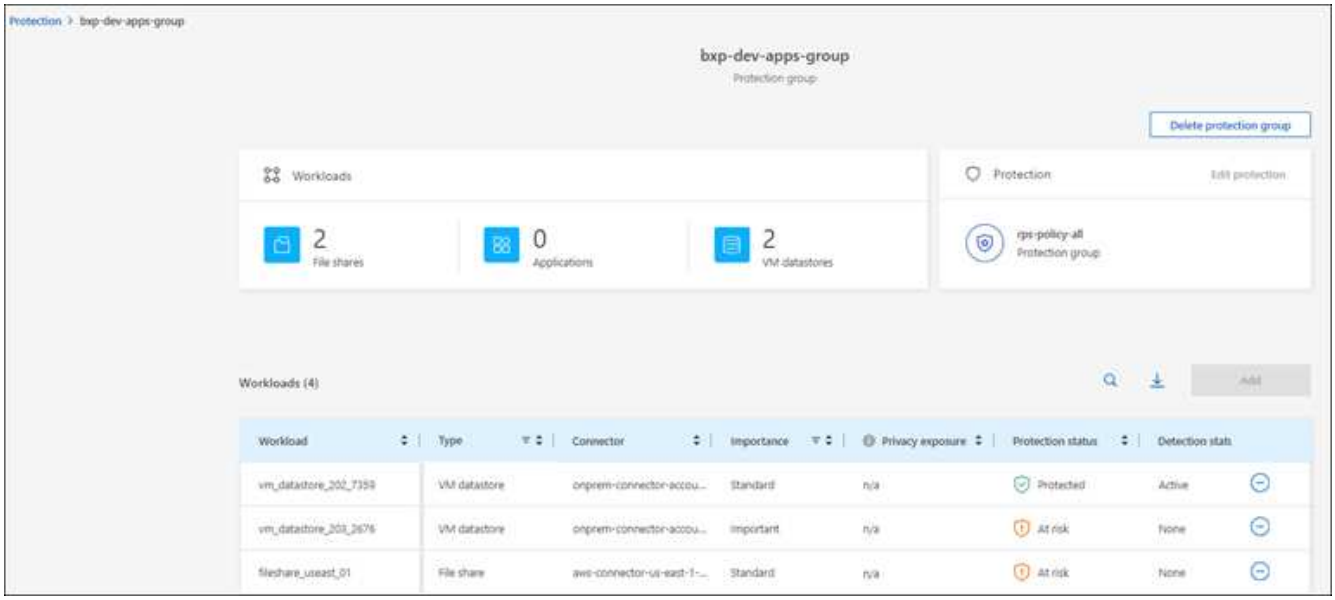
4. Dalla pagina Gruppo protezione selezionato, selezionare il carico di lavoro che si desidera rimuovere dal gruppo e selezionare l'opzione *azioni*•••.
5. Dal menu azioni, selezionare **Rimuovi carico di lavoro**.
6. Confermare che si desidera rimuovere il carico di lavoro e selezionare **Rimuovi**.

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.

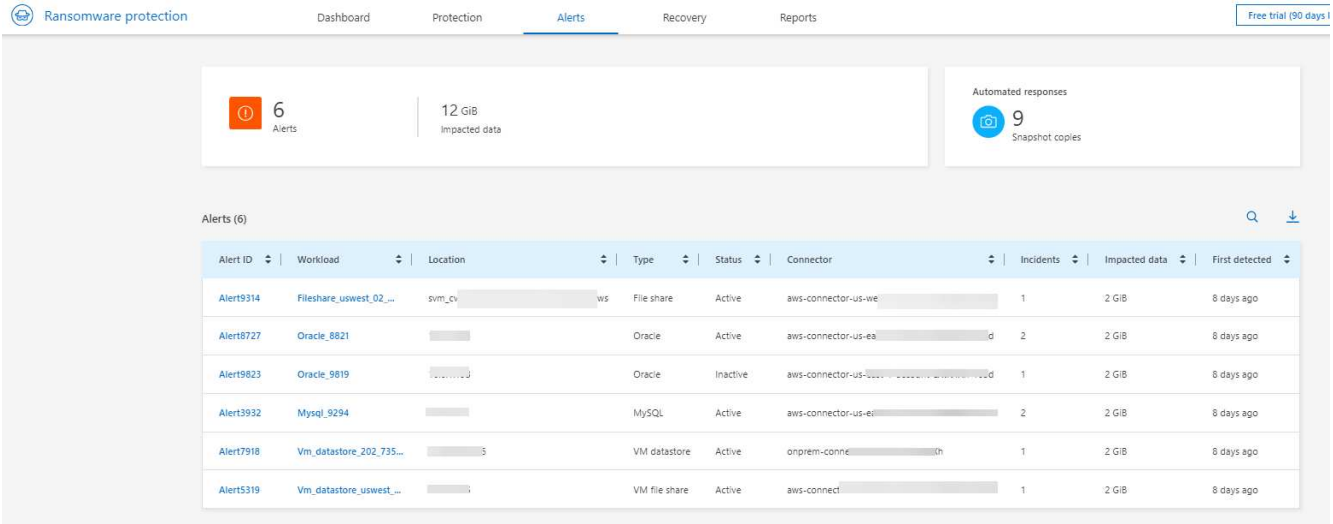
- **Licenziamento**: L'incidente è in fase di licenziamento.
- **Risolto**: L'incidente è stato mitigato.

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.



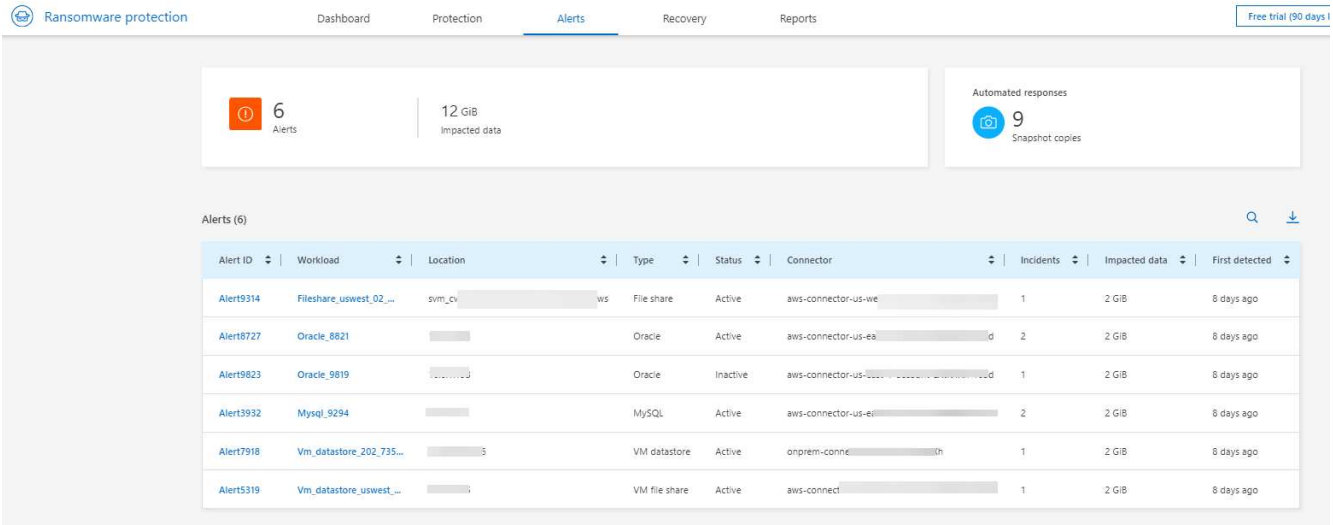
6. Continua:
   - Contrassegna gli incidenti ransomware come pronti per il recovery (dopo la neutralizzazione degli incidenti).
   - Elimina gli incidenti che non sono potenziali attacchi.

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

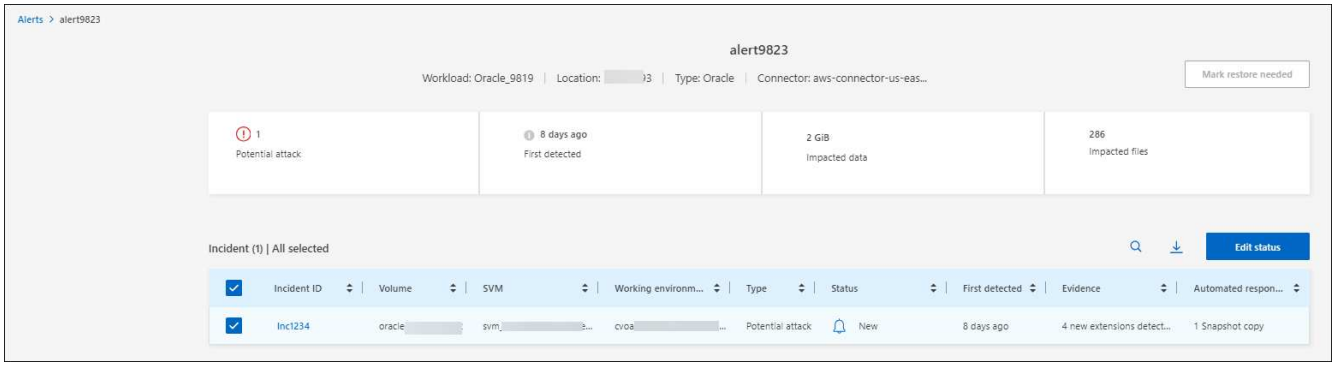
Una volta mitigato l'attacco e sei pronto a ripristinare i carichi di lavoro, dovresti comunicare con il tuo team di amministrazione dello storage che i dati sono pronti per il recovery, in modo che possano avviare il processo di recovery.

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.

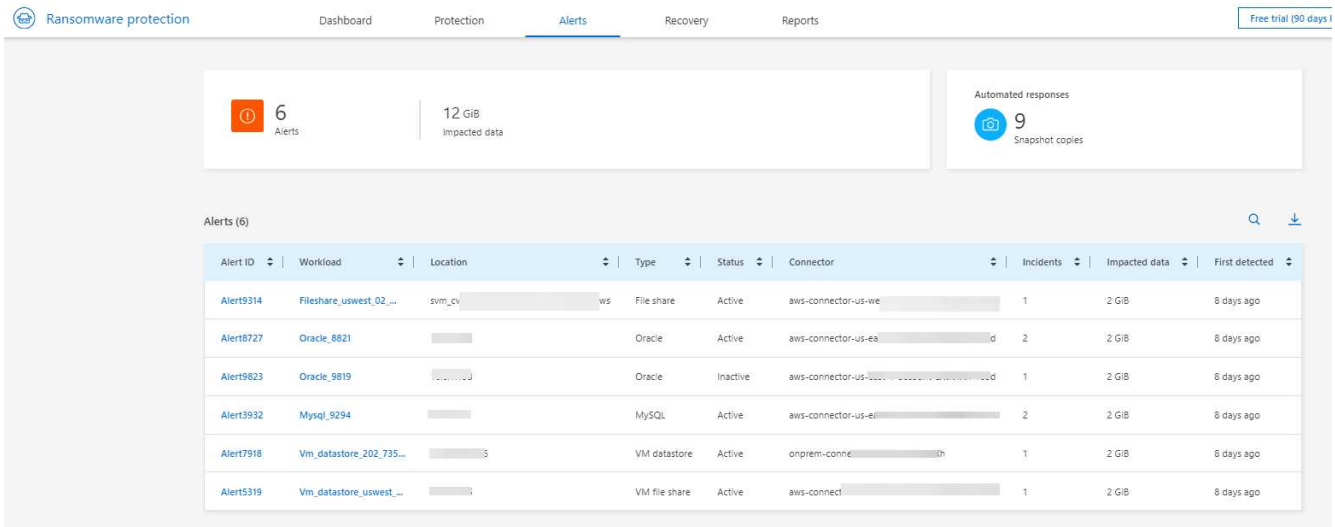
Puoi liquidare i falsi positivi o decidere di recuperare immediatamente i tuoi dati. Se si decide di ignorare l'avviso, il servizio apprenderà questo comportamento e lo assocerà alle normali operazioni e non avvierà nuovamente un avviso su tale comportamento.

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

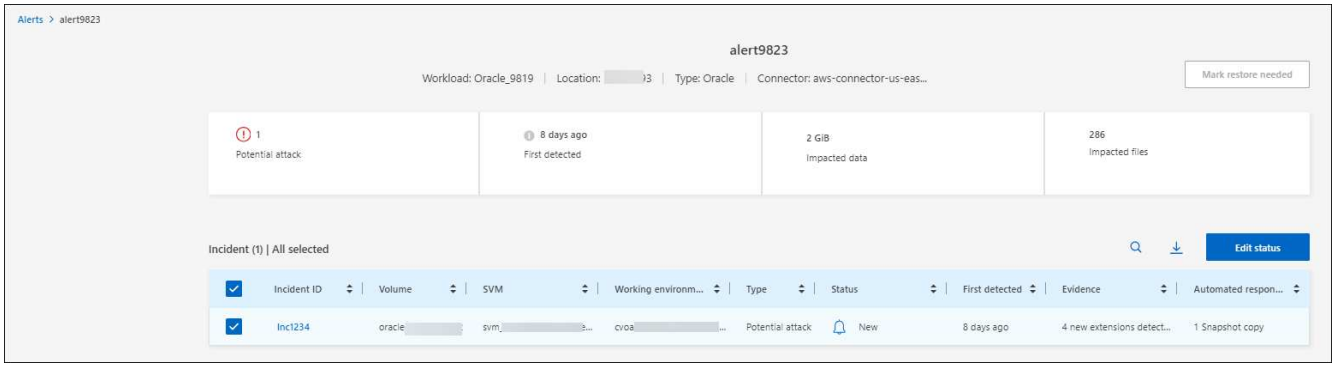
> Se si ignora un avviso, non è possibile ripristinare lo stato in qualsiasi altro stato e non è possibile annullare la modifica.

Fasi

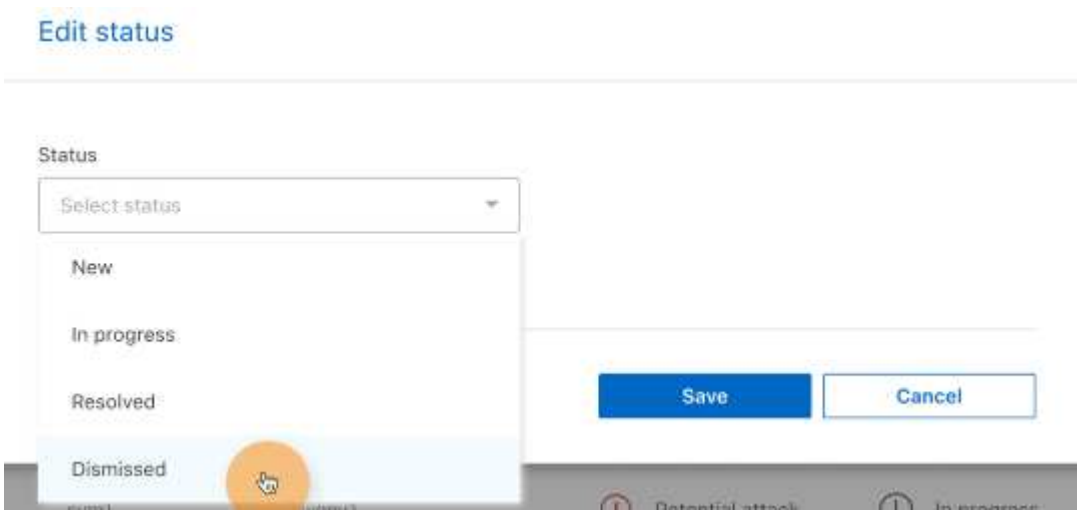
1. Dal menu di protezione dal ransomware BlueXP, seleziona **Avvisi**.



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

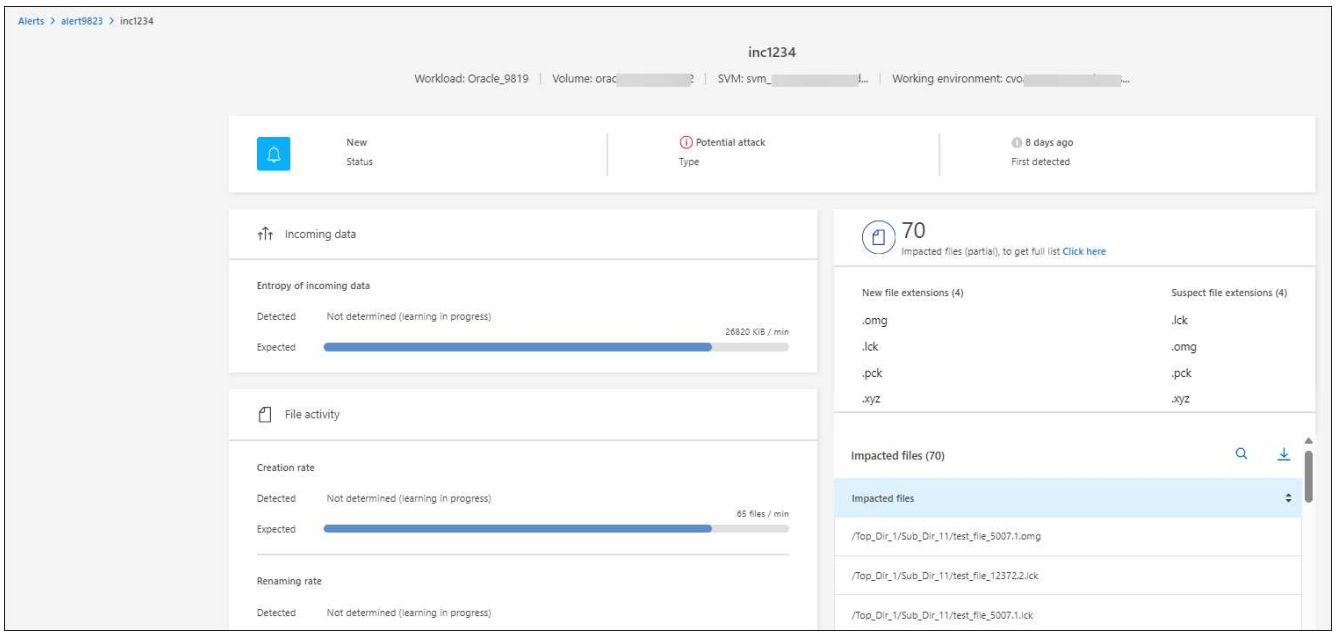
Prima di ripristinare un workload dell'applicazione a livello di file, è possibile visualizzare un elenco di file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco di file interessati. Quindi, utilizzare la pagina di ripristino per caricare l'elenco e scegliere i file da ripristinare.

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:

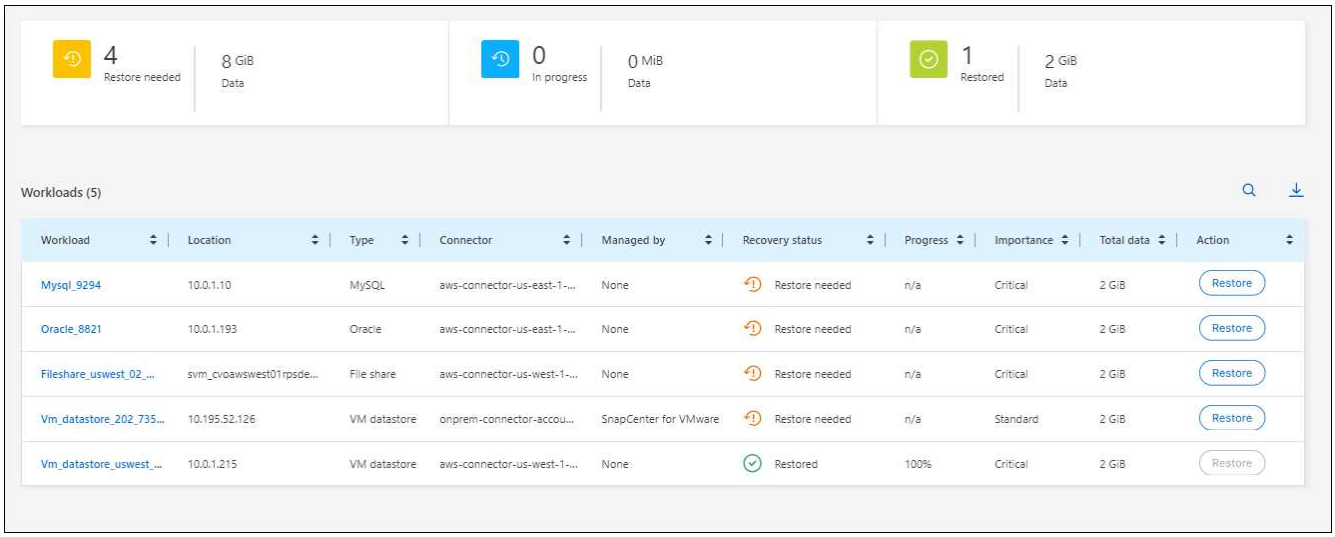
- **Necessario ripristino**: Il carico di lavoro deve essere ripristinato.
- **In corso**: L'operazione di ripristino è attualmente in corso.
- **Ripristinato**: Il carico di lavoro è stato ripristinato.
- **Non riuscito**: Impossibile completare il processo di ripristino del workload.

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**.

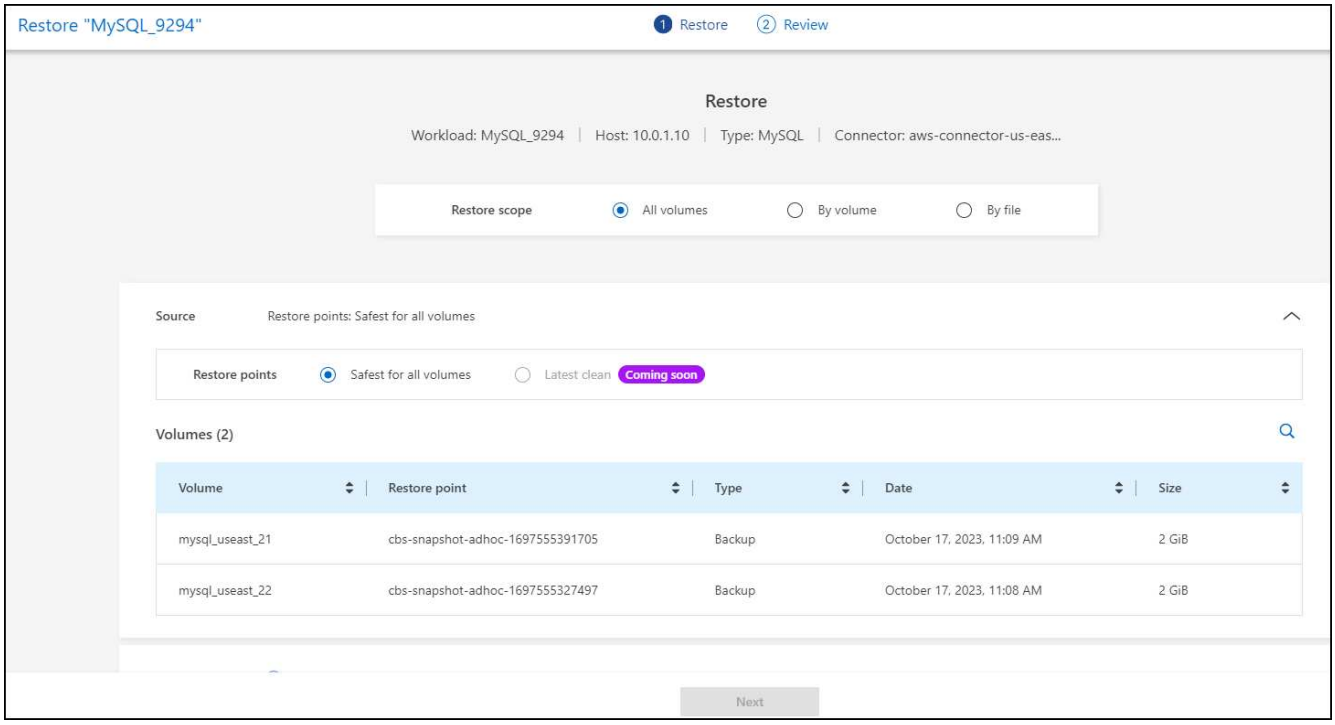
5. **Ripristina ambito**: Selezionare il tipo di ripristino che si desidera completare:
   - Tutti i volumi
   - Per volume
   - Per file: È possibile specificare una cartella o singoli file da ripristinare.

> 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.

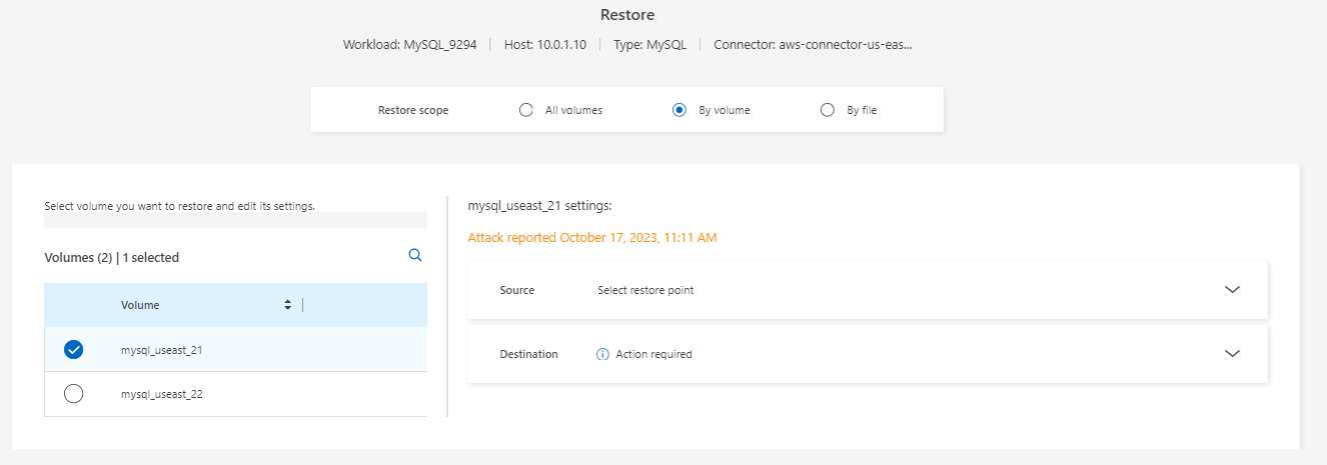
d. Modificare il prefisso del volume che verrà anteposto a tutti i nuovi volumi.

> 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.

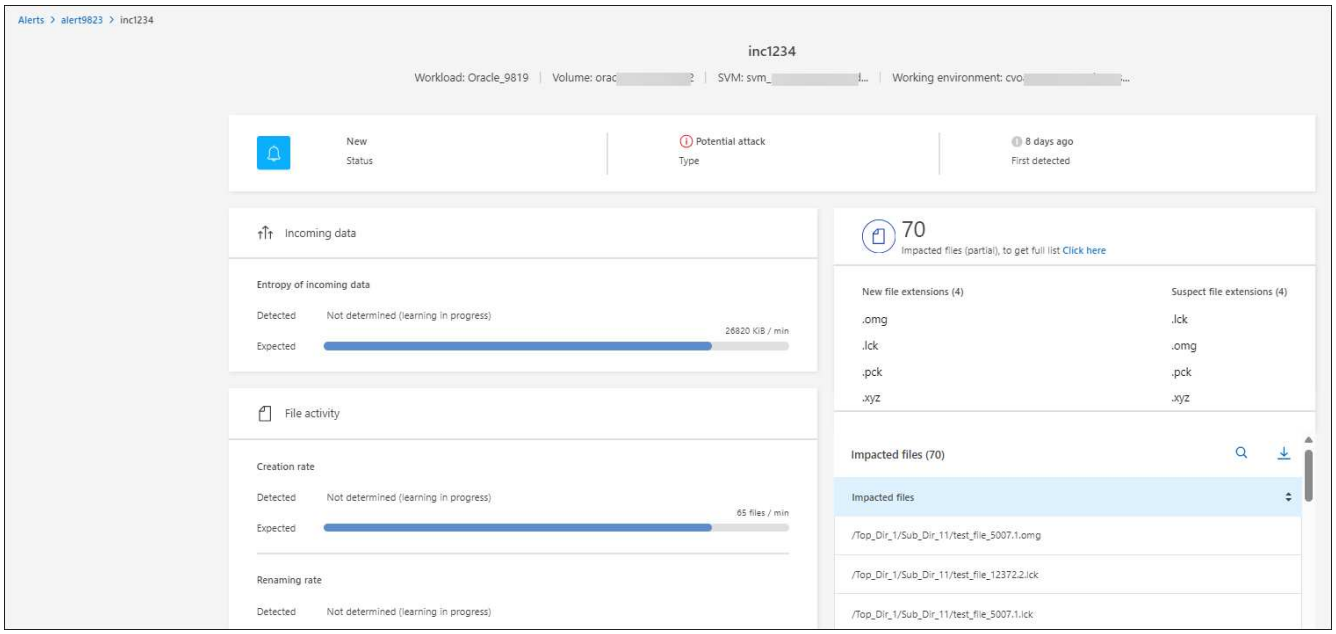
È possibile ripristinare un workload dell'applicazione a livello di file nello stesso ambiente di lavoro o in un ambiente diverso.

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.



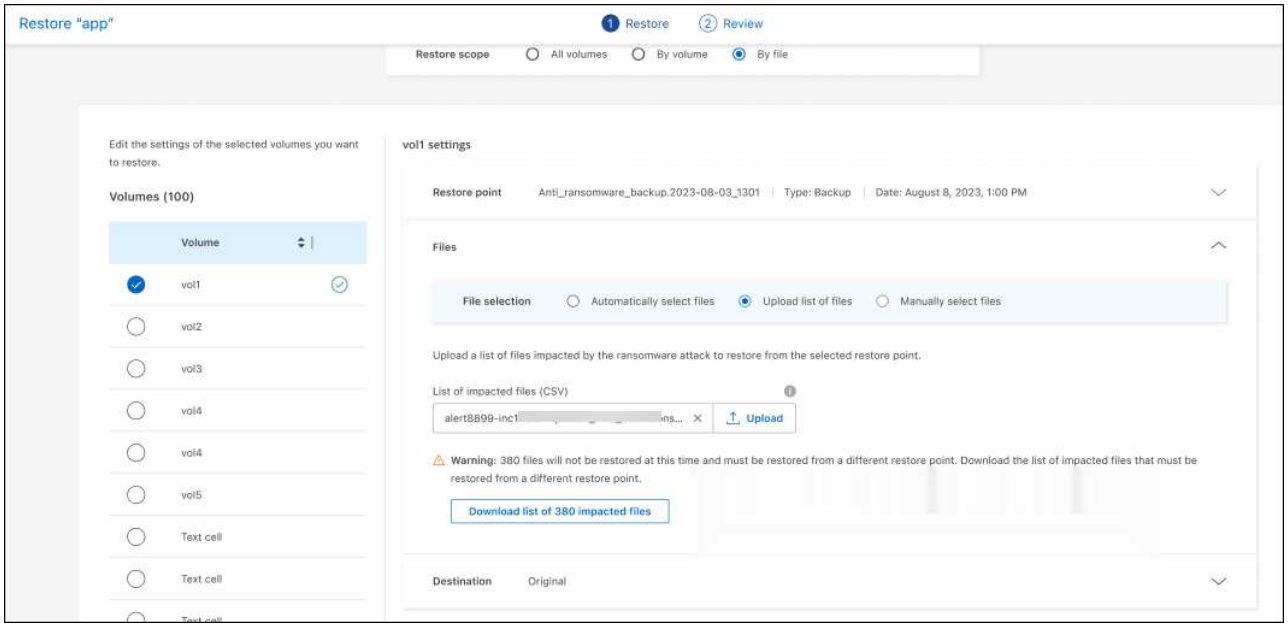
5. Per visualizzare l'elenco completo dei file, selezionare **fare clic qui** nella parte superiore del riquadro file interessati.
6. Per quell'incidente, selezionare l'icona di download e scaricare l'elenco dei file interessati in formato CSV.

Procedura per ripristinare tali file

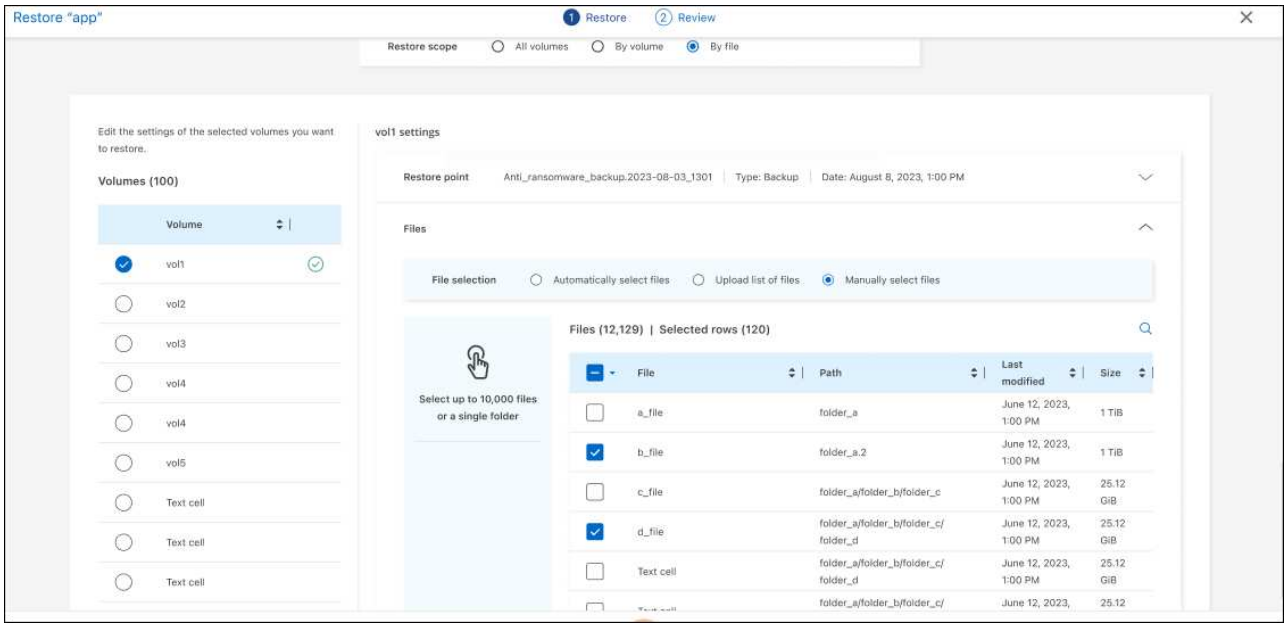
1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Seleziona un carico di lavoro dell'applicazione in stato "Ripristino necessario".
3. Per ripristinare, selezionare **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, selezionare **per file**.
5. Nell'elenco dei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

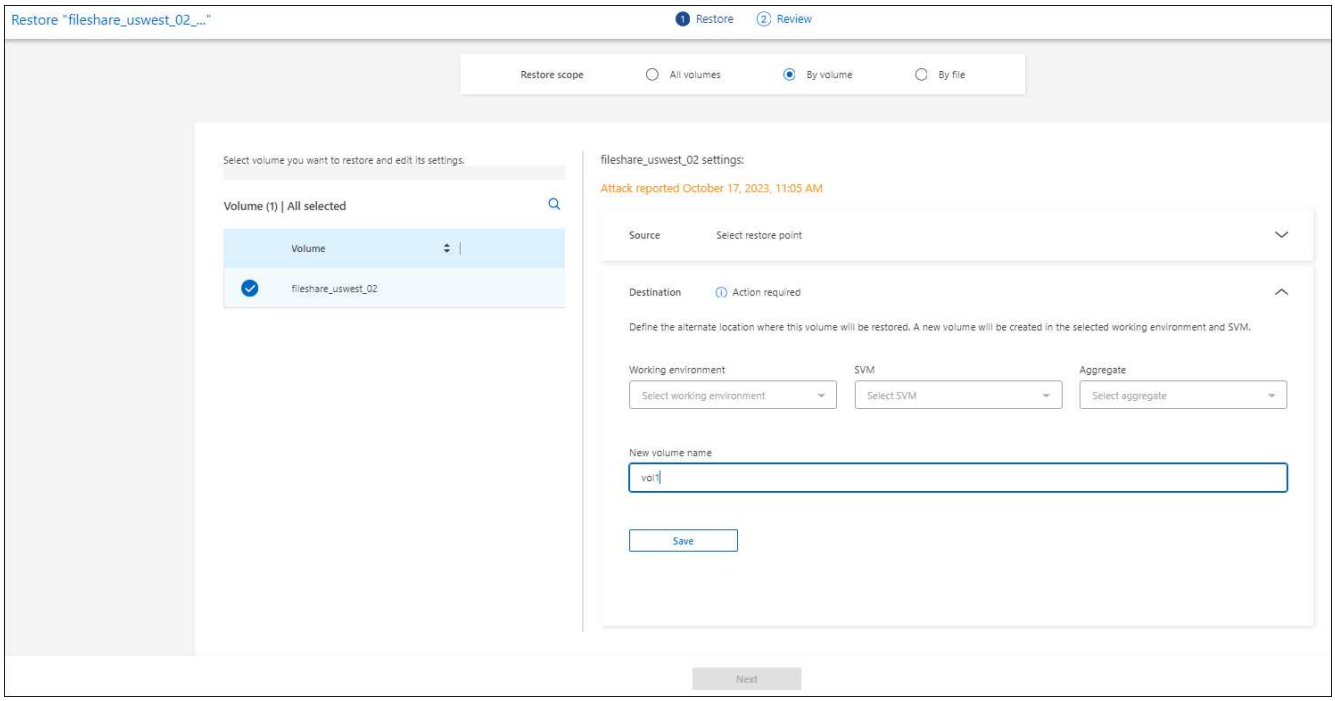
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

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.

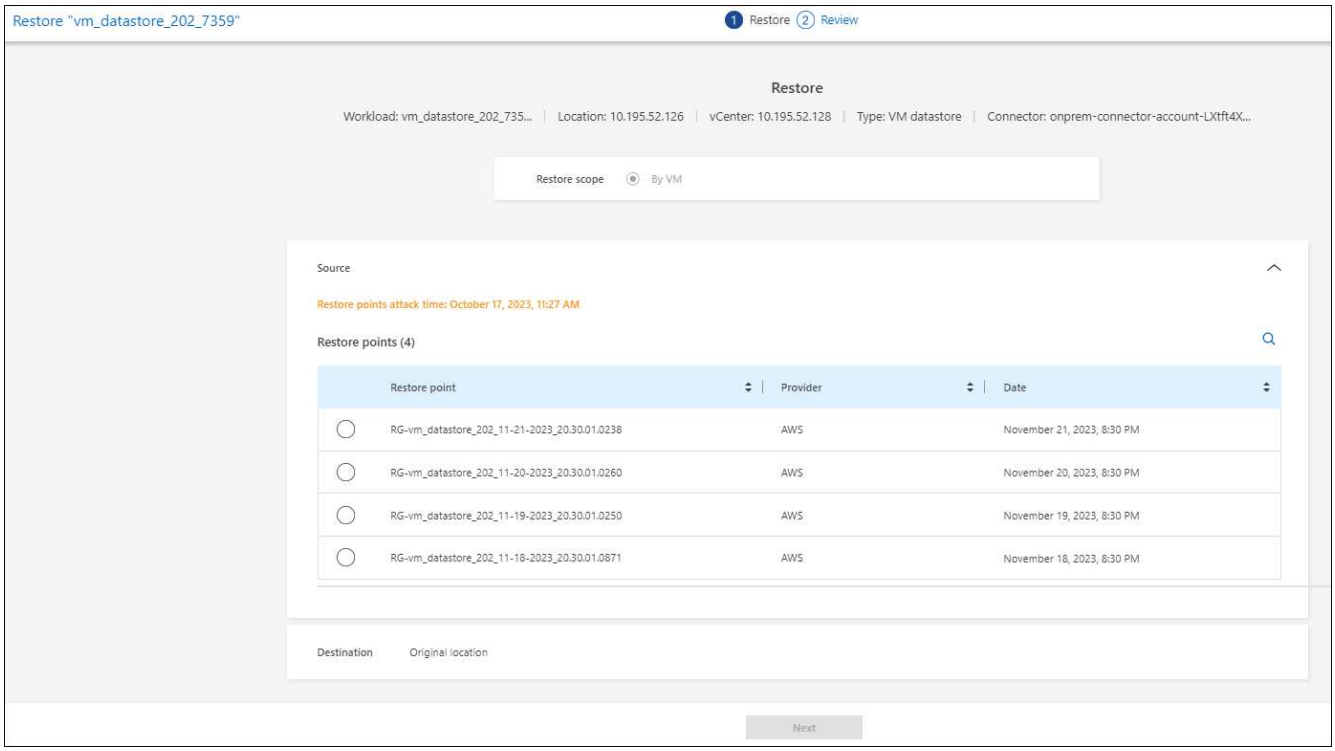
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

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:

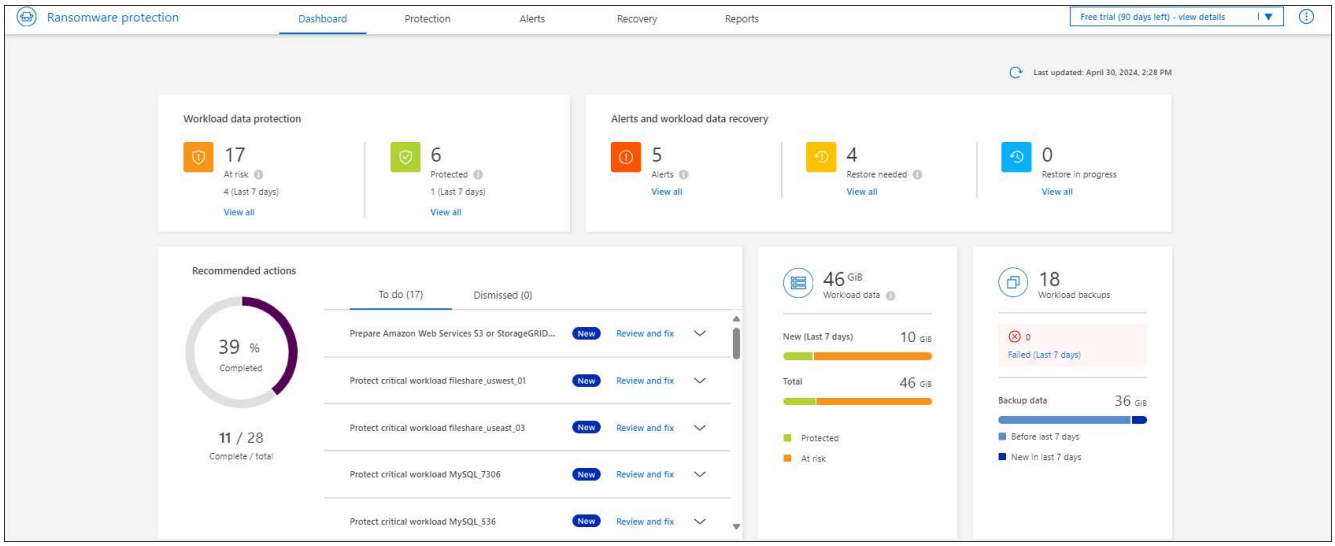
- **Protezione**: Contiene lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale protetto e a rischio.
- **Avvisi**: Include lo stato e i dettagli di tutti gli avvisi, compreso il numero totale di avvisi e istantanee automatiche.
- **Recovery**: Include lo stato e i dettagli di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

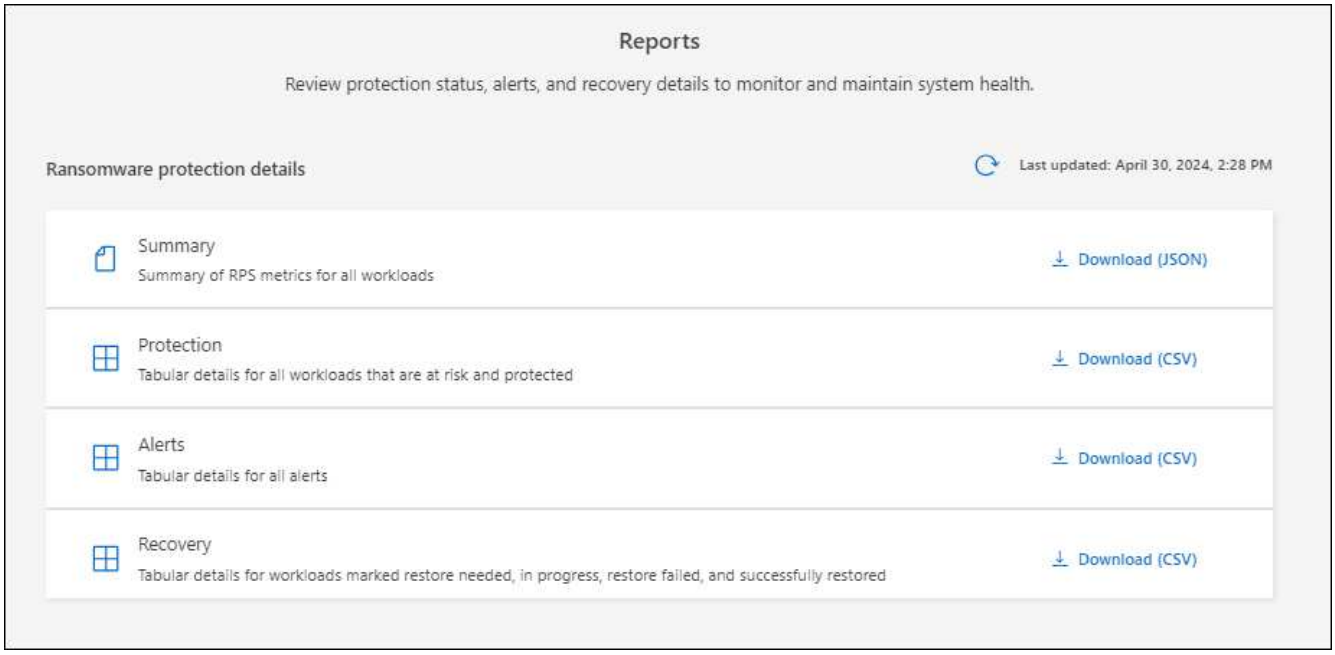
1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.



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)**.



Conoscenza e supporto

Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione del numero di serie dell'account BlueXP (il numero di serie 960xxxxxxxxx a 20 cifre si trova nella pagina risorse di supporto di BlueXP).

  Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

- Registrazione dei numeri di serie Cloud Volumes ONTAP associati a un abbonamento nel mercato del provider cloud (si tratta di numeri di serie 909201xxxxxxxx a 20 cifre).

  Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

Registrare BlueXP per ricevere assistenza NetApp

Per registrarsi per ricevere assistenza e attivare i diritti di supporto, un utente dell'organizzazione (o account) BlueXP deve associare un account del sito di supporto NetApp al proprio login BlueXP . La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

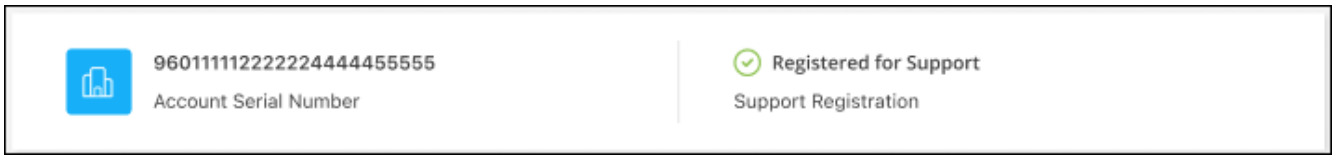
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

   La pagina **risorse** dovrebbe mostrare che l'organizzazione BlueXP è registrata per il supporto.

   Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che la tua organizzazione BlueXP non sia registrata per il supporto. Finché un utente dell'organizzazione ha seguito questi passaggi, l'organizzazione è stata registrata.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

Fasi

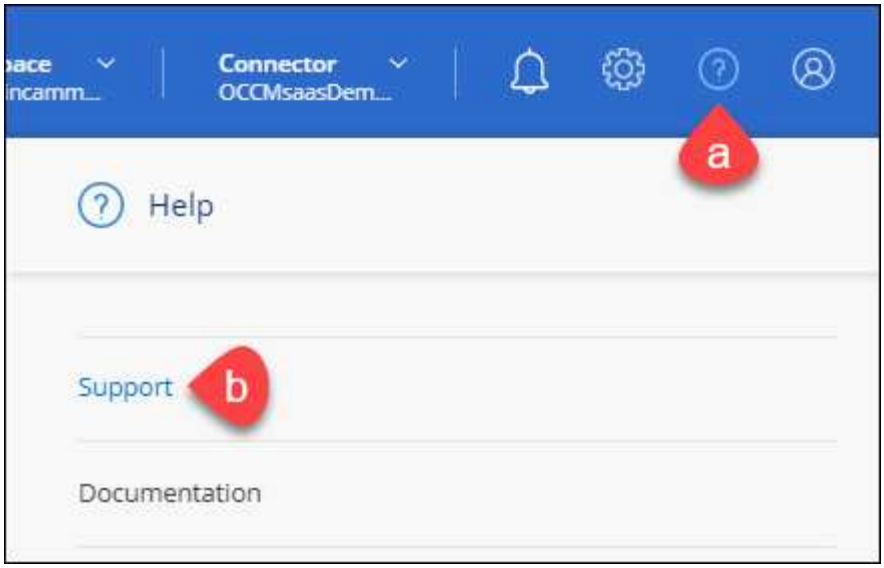
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto Cliente esistente con un account NSS.

Novità di NetApp

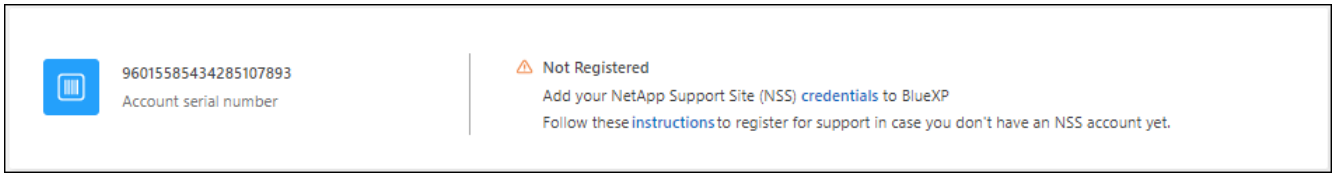
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare "Sito per la registrazione del supporto NetApp" E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

   Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

7. Confermare l'azione dall'interno dell'e-mail.

   La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

8. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account (960xxxx) utilizzato in precedenza per il campo del numero di serie. Ciò velocizzerà l'elaborazione.

Al termine

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di assunzione per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in Cliente esistente con un account NSS.

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

È necessario associare le credenziali del sito di supporto NetApp alla propria organizzazione BlueXP per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

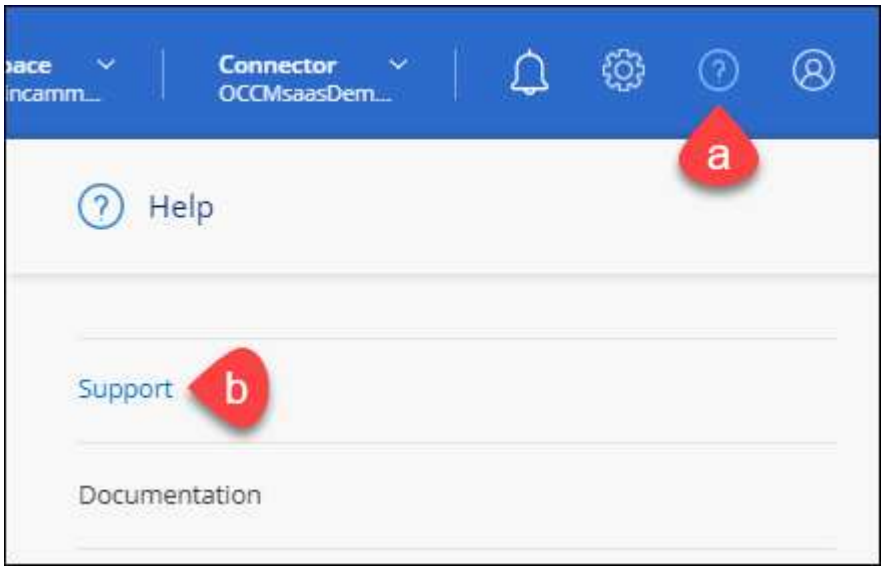
L'associazione delle credenziali NSS all'organizzazione BlueXP è diversa dall'account NSS associato a un accesso utente BlueXP .

Queste credenziali NSS sono associate all'ID organizzazione BlueXP specifico dell'utente. Gli utenti che appartengono all'organizzazione BlueXP possono accedere a queste credenziali da **supporto > Gestione NSS**.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include il supporto tecnico remoto via web ticketing.

Ottieni supporto per un file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

  Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- "Community"

  Unisciti alla community BlueXP per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo l'attivazione del supporto.

Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. "Scopri come gestire le credenziali associate all'accesso a BlueXP".
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:

   a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.

   b. Selezionare **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp:

      - **Servizio**: Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
      - **Ambiente di lavoro**: Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

        L'elenco degli ambienti di lavoro rientra nell'ambito dell'organizzazione (o account), del progetto (o dell'area di lavoro) BlueXP e del connettore selezionato nell'intestazione superiore del servizio.

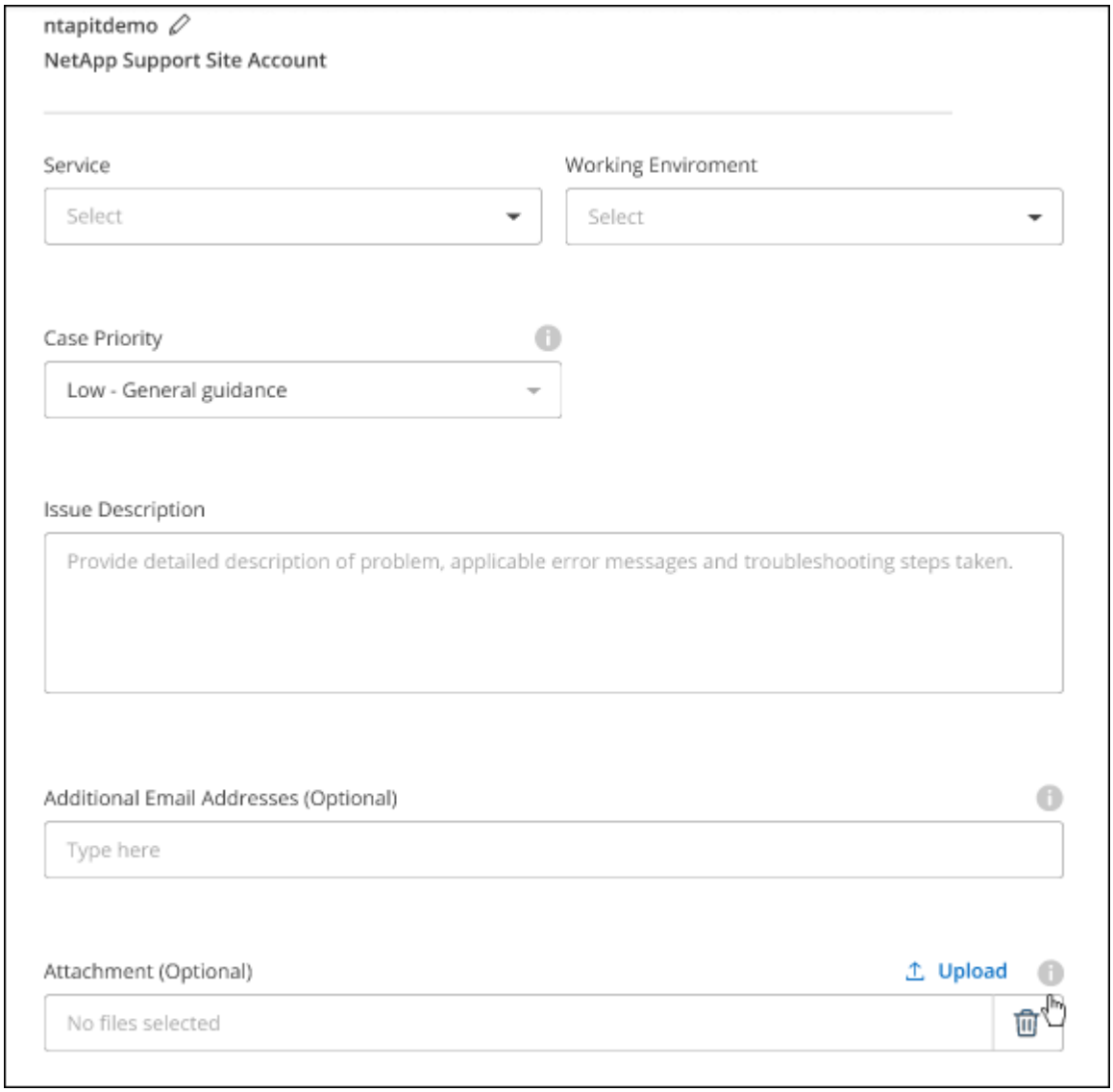
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.

      - **Descrizione del problema**: Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
      - **Indirizzi e-mail aggiuntivi**: Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale)**: Carica fino a cinque allegati, uno alla volta.

  Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo https://mysupport.netapp.com/site/help

Gestire i casi di supporto (anteprima)

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

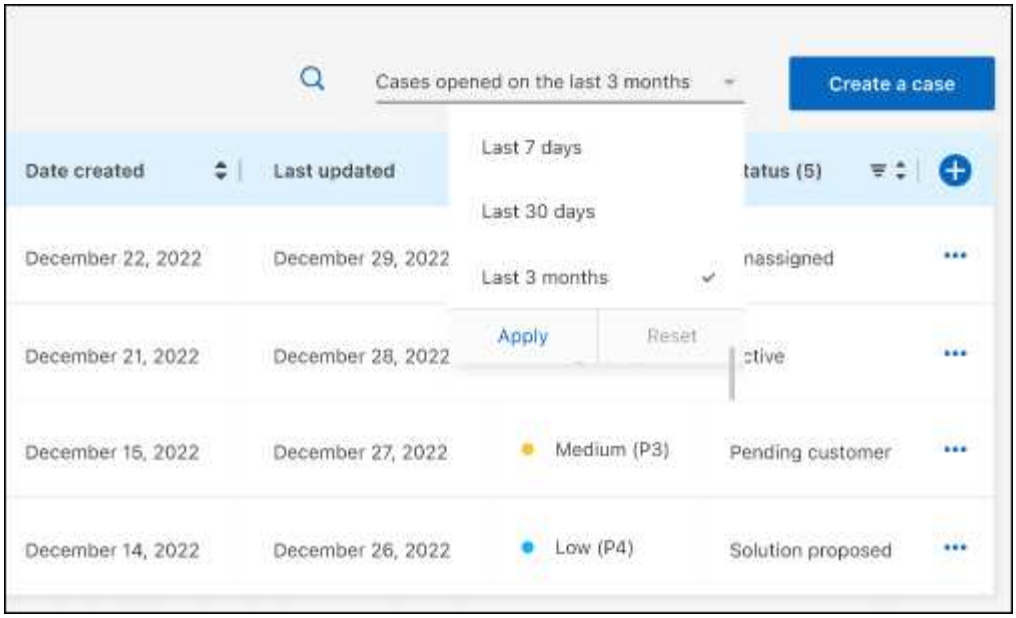
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  Per ulteriori informazioni, consulta la procedura riportata di seguito.
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

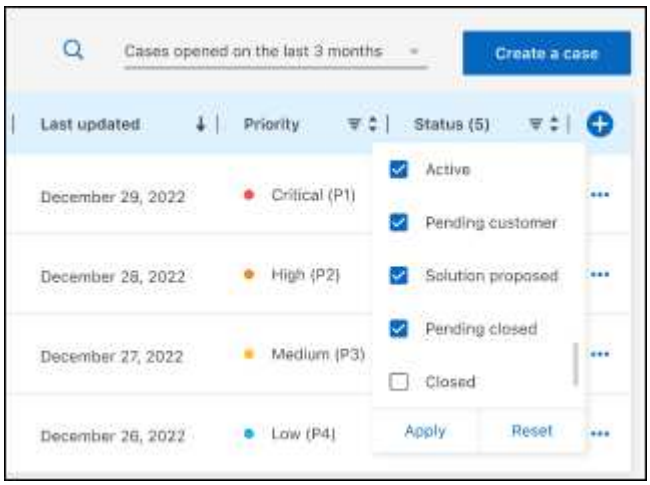
Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.

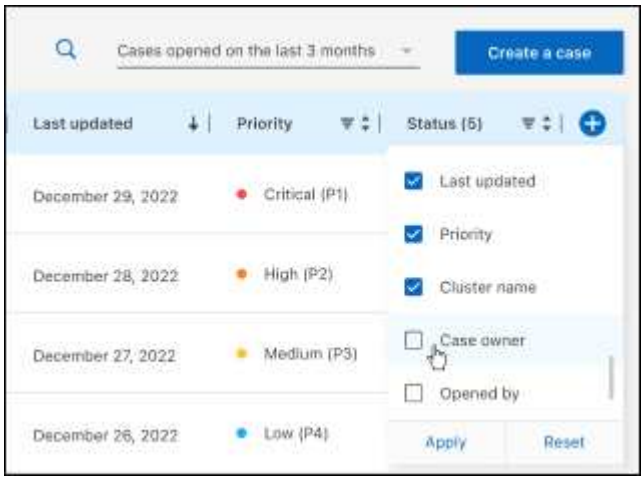
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
   - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.



- Modificare le colonne visualizzate nella tabella selezionando e quindi scegliere le colonne che si desidera visualizzare.

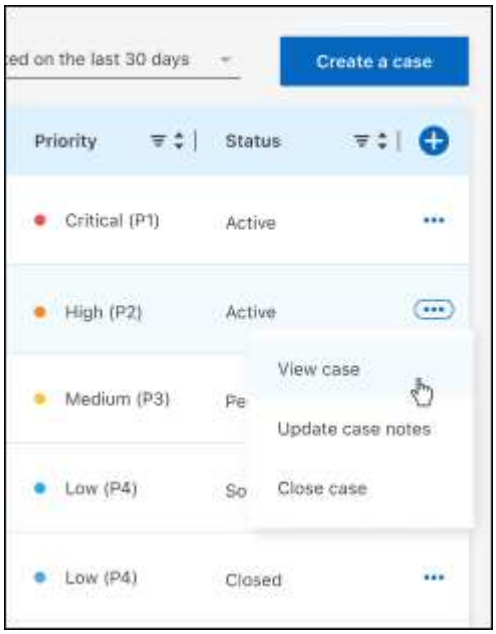


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

   - **Visualizza caso**: Visualizza tutti i dettagli relativi a un caso specifico.
   - **Aggiorna note sul caso**: Fornisci ulteriori dettagli sul problema oppure seleziona **carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - **Chiudi caso**: Fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.



Riferimento

Privileges per il controllo degli accessi in base al ruolo della protezione ransomware BlueXP

La protezione ransomware BlueXP utilizza il role-based access control (RBAC) per gestire l'accesso a funzionalità e azioni specifiche di ciascun utente. Il servizio utilizza i ruoli BlueXP principali di account Admin e Viewer (non account Admin0).

La tabella seguente indica quali azioni possono essere eseguite da ciascun ruolo.

Funzione e azione	Amministratore account BlueXP	Non amministratore (visualizzatore)
Inizia la prova gratuita	Y	N
Visualizza dashboard	Y	Y
Visualizza scheda protezione	Y	Y
Visualizza scheda Avvisi	Y	Y
Visualizza scheda Recupera	Y	Y
Visualizza scheda rapporti	Y	Y
Visualizza scheda Impostazioni	Y	Y
Avvia il rilevamento dei carichi di lavoro	Y	N
Proteggere: Modificare o eliminare i criteri	Y	N
Protezione: Aggiunta di criteri	Y	N
Proteggere: Proteggere i carichi di lavoro	Y	N
Protezione: Identificazione dei dati sensibili	Y	N
Protezione: Modifica della protezione del carico di lavoro	Y	N
Protezione: Consente di visualizzare i dettagli del carico di lavoro	Y	Y
Protezione: Download dei dati	Y	Y
Avvisi: Consente di visualizzare i dettagli degli avvisi	Y	Y

Funzione e azione	Amministratore account BlueXP	Non amministratore (visualizzatore)
Avvisi: Consente di modificare lo stato dell'incidente	Y	N
Avvisi: Consente di visualizzare i dettagli dell'incidente	Y	Y
Avvisi: Consente di ottenere l'elenco completo dei file interessati	Y	N
Avvisi: Scarica i dati degli avvisi	Y	Y
Recupera: Scarica i file interessati	Y	N
Ripristina: Ripristina il workload	Y	N
Recupera: Scarica i dati di recupero	Y	Y
Recupera: Scarica i report	Y	Y
Impostazioni: Aggiungere o modificare le destinazioni di backup	Y	N
Impostazioni: Aggiungere o modificare target SIEM	Y	N
Report: Scarica report	Y	Y
Documentazione: Consente di visualizzare la documentazione relativa al prodotto	Y	Y
Documentazione: Consente di visualizzare la documentazione sulle novità del prodotto	Y	Y

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

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

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

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

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

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

Direttiva sulla privacy

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

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per BlueXP"

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.