Inizia subito

BlueXP ransomware protection

NetApp
October 07, 2024

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

Sommario

Inizia subito . . . 1
Scopri di più sulla protezione ransomware di BlueXP . . . 1
Prerequisiti della protezione dal ransomware di BlueXP . . . 6
Avvio rapido per la protezione dal ransomware di BlueXP . . . 8
Imposta la protezione dal ransomware BlueXP . . . 9
Accedi alla protezione dal ransomware di BlueXP . . . 10
Imposta una licenza per la protezione dal ransomware di BlueXP . . . 11
Rileva i carichi di lavoro nella protezione dal ransomware di BlueXP . . . 19
Configurare le impostazioni di protezione dal ransomware BlueXP . . . 21
Domande frequenti sulla protezione dal ransomware BlueXP . . . 31

Inizia subito

Scopri di più sulla protezione ransomware di BlueXP

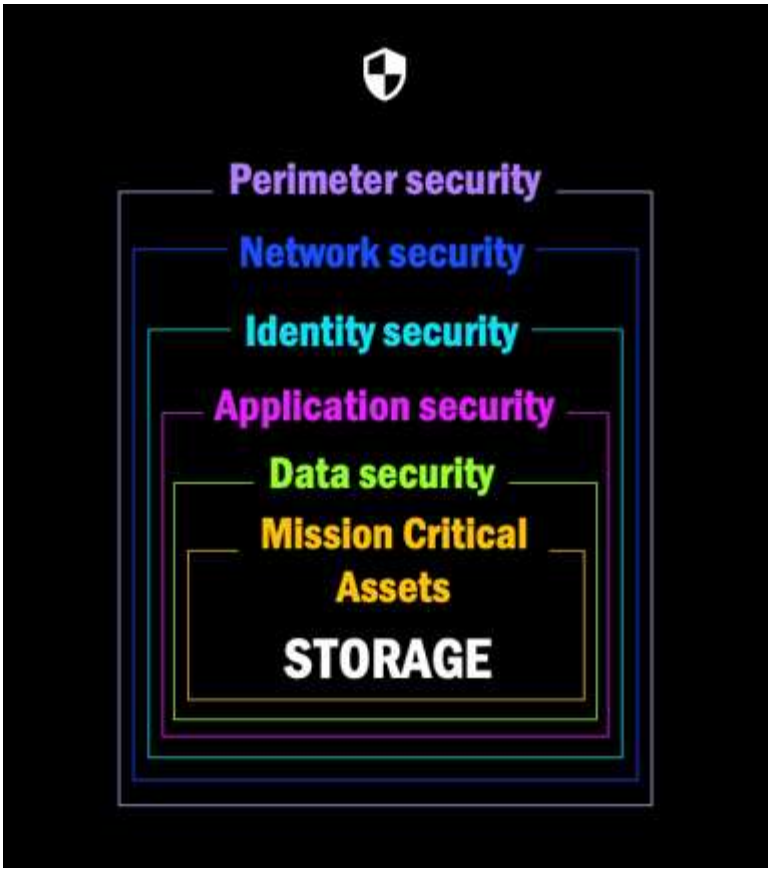
Gli attacchi ransomware possono bloccare l'accesso ai dati e gli hacker possono chiedere un riscatto in cambio del rilascio o della decrittografia dei dati. Secondo IDC, non è raro che le vittime del ransomware subiscano diversi attacchi ransomware. L'attacco può interrompere l'accesso ai tuoi dati tra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

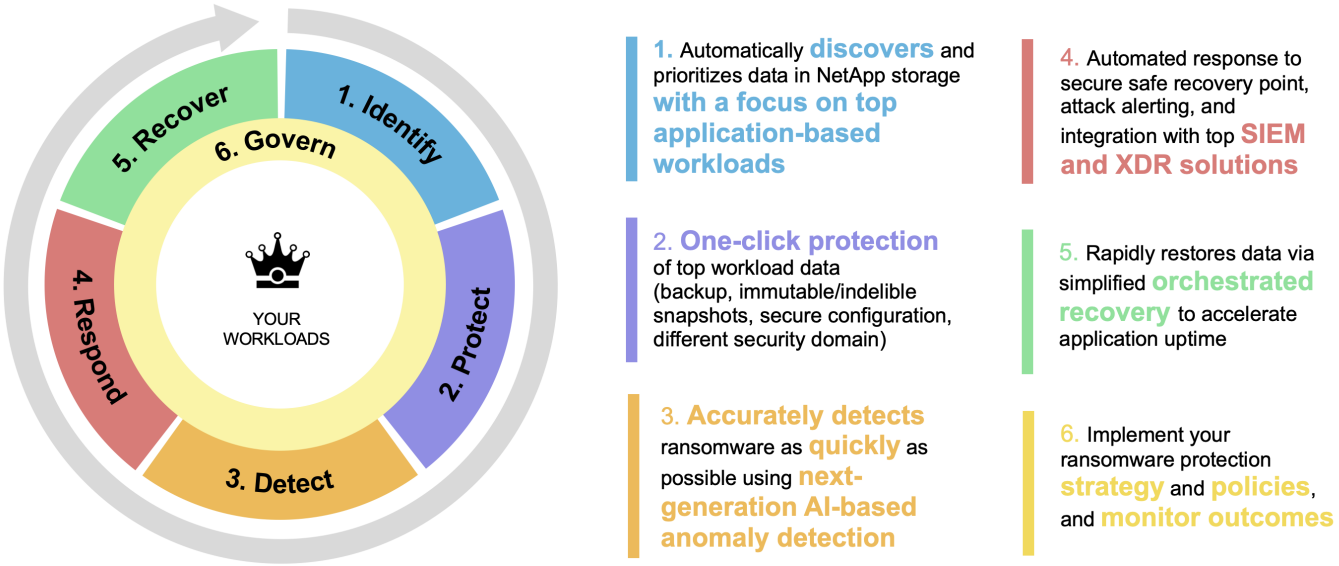
- **Livello più esterno**: Questa è la prima linea di difesa che utilizza firewall, sistemi di rilevamento delle intrusioni e reti private virtuali per salvaguardare i confini della rete.
- **Sicurezza della rete**: Questo livello si basa sulla segmentazione della rete, sul monitoraggio del traffico 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.

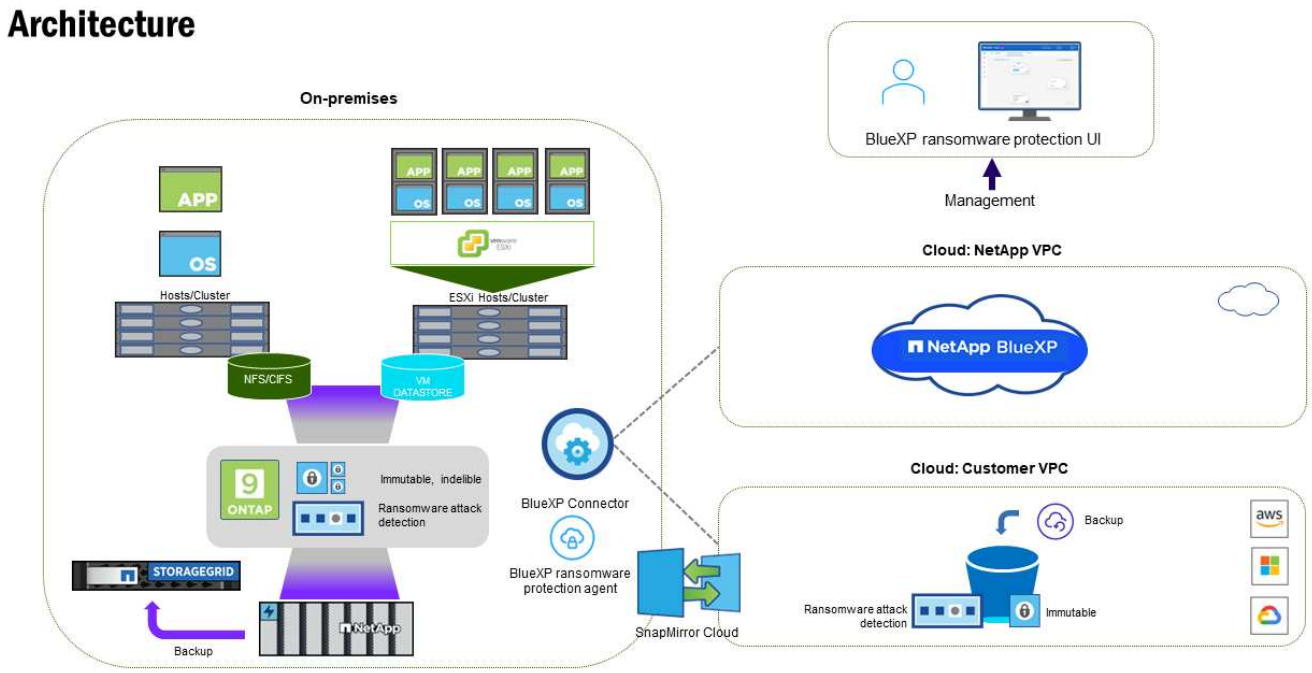
La licenza di protezione ransomware BlueXP non include prodotti NetApp aggiuntivi. La protezione dal ransomware di BlueXP può usare il backup e recovery di BlueXP anche se non disponi di una licenza per esso.

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".

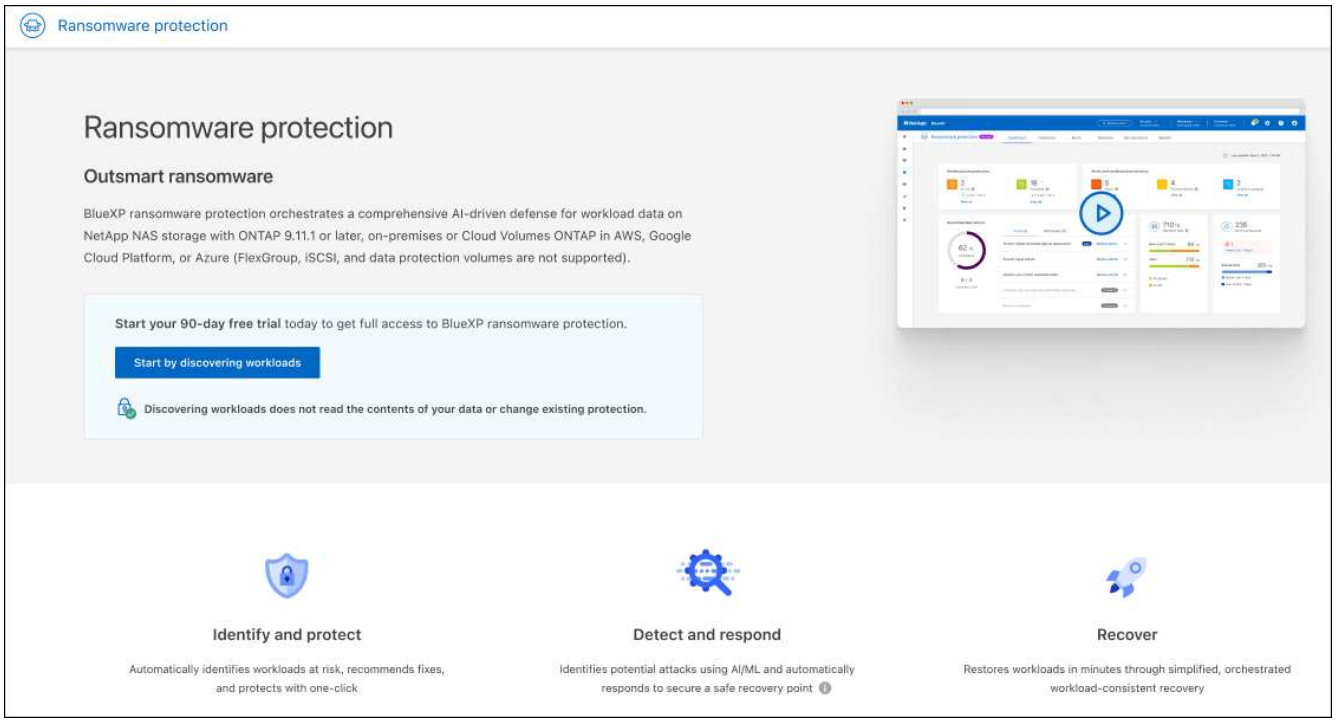
Fasi

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

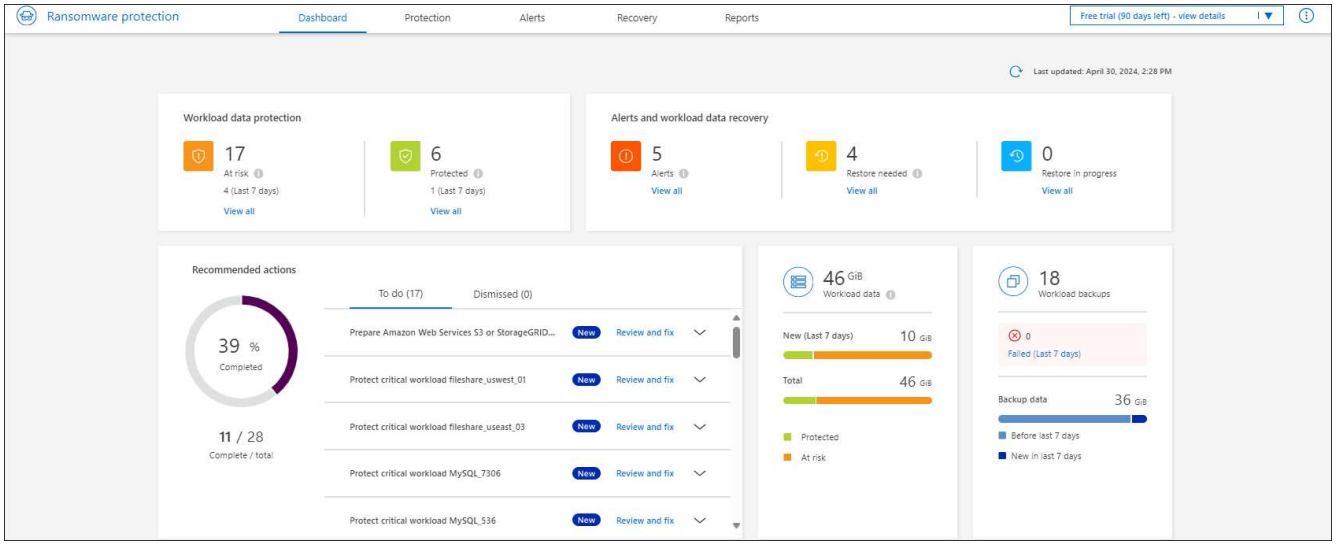
   Viene visualizzata la pagina di accesso a NetApp BlueXP.

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.

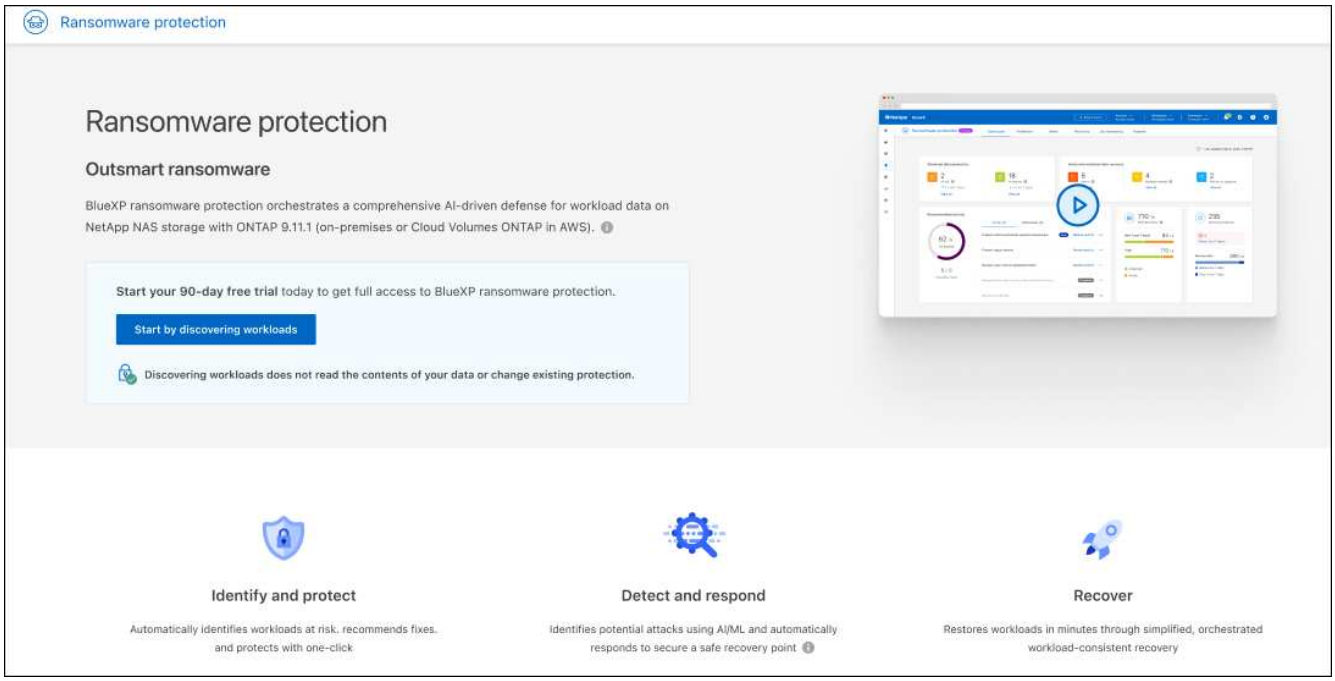
È possibile ottenere una licenza o sottoscrivere l'abbonamento in qualsiasi momento e non verrà addebitato alcun costo fino al termine della prova di 90 giorni. Per continuare dopo la prova di 90 giorni, dovrai acquistare una licenza BYOL o un abbonamento PAYGO.

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.

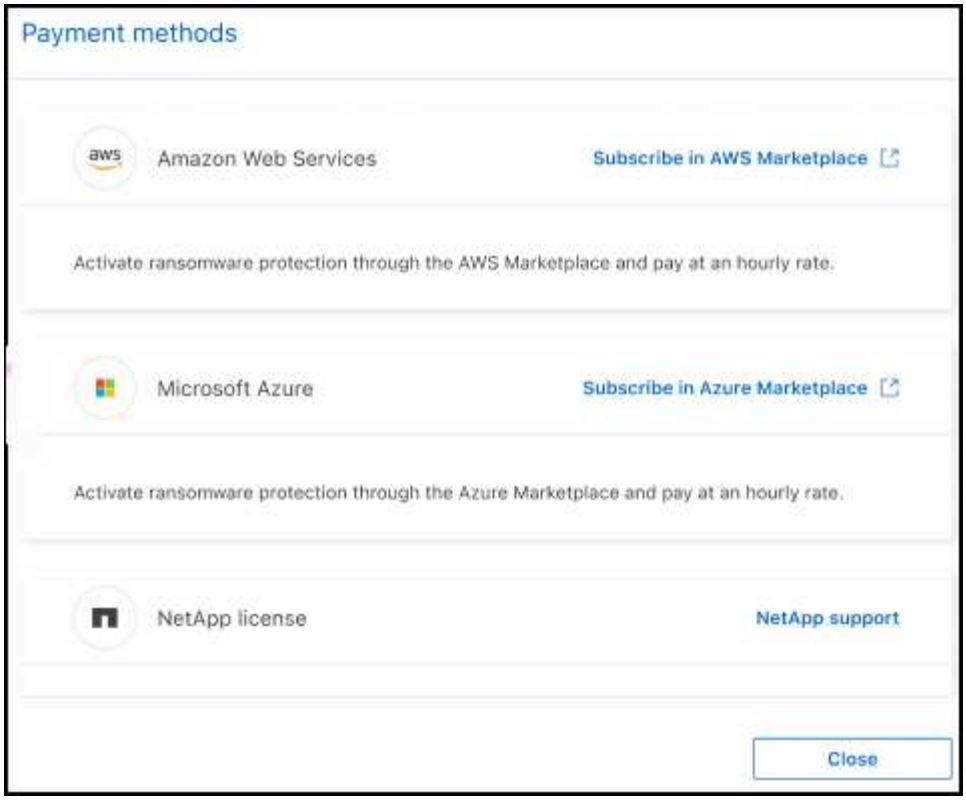
Iscriviti tramite AWS Marketplace Iscriviti tramite Microsoft Azure Marketplace BYOL

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**.

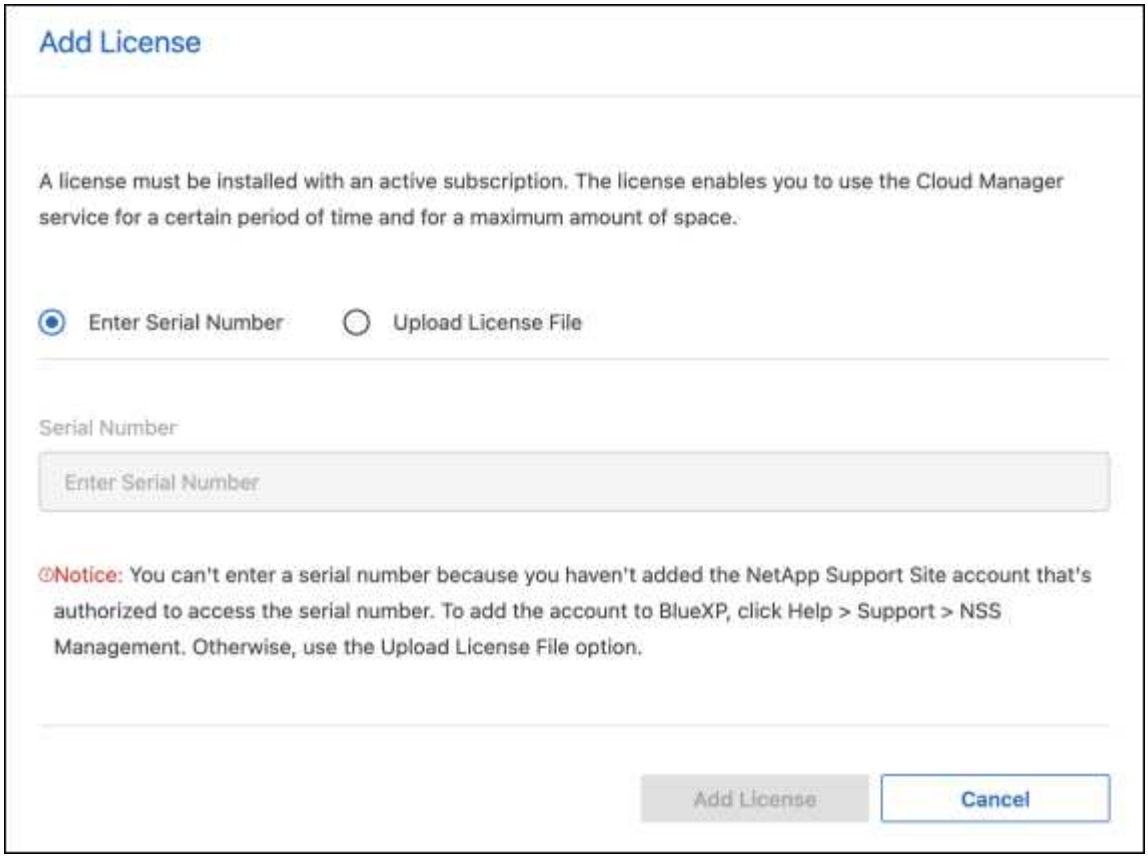


2. Nella pagina metodi di pagamento, seleziona **Iscriviti in AWS Marketplace**.
3. In AWS Marketplace, selezionare **Visualizza opzioni di acquisto**.
4. USA AWS Marketplace per sottoscrivere il servizio di protezione dal ransomware BlueXP.
5. Quando torni alla protezione ransomware di BlueXP, un messaggio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

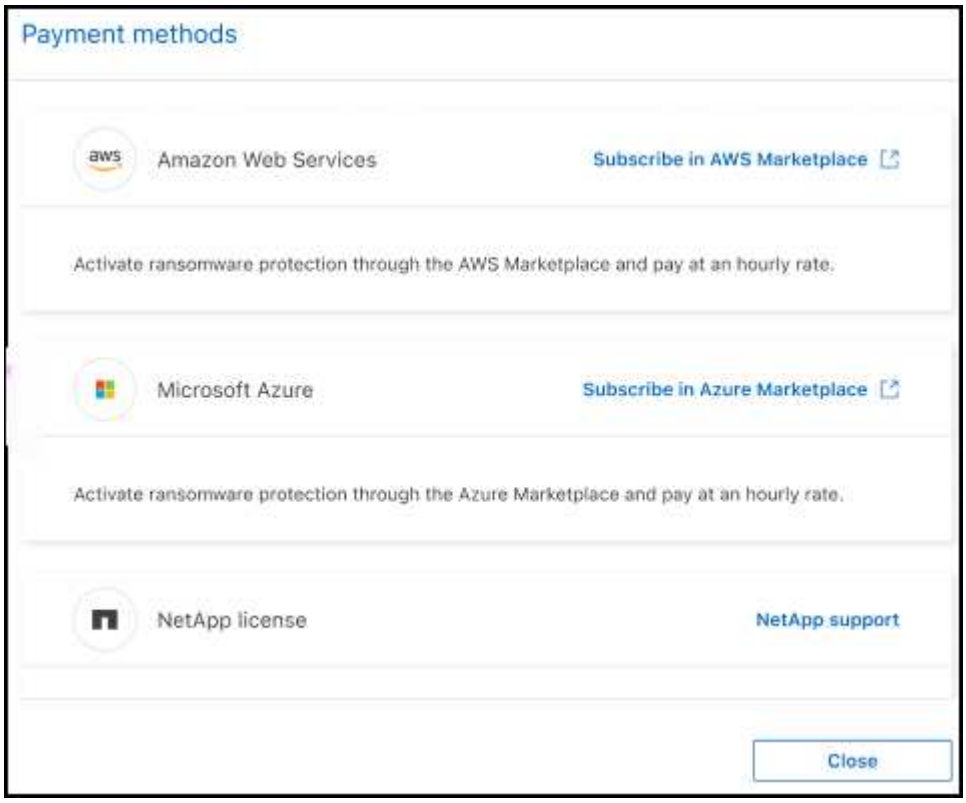
Viene visualizzato un messaggio che indica che è stata aggiunta una licenza.

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**.

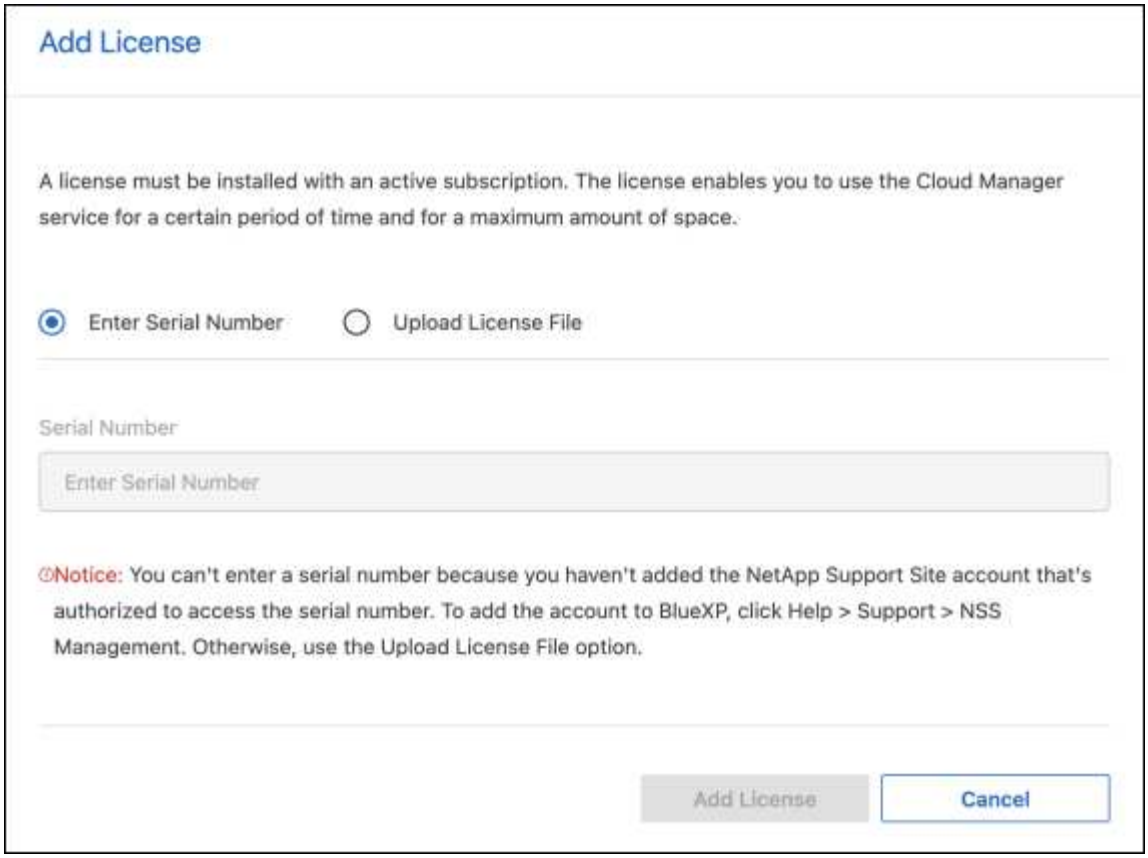


2. Nella pagina metodi di pagamento, seleziona **Sottoscrivi in Azure Marketplace**.
3. In Azure Marketplace, selezionare **Visualizza opzioni di acquisto**.
4. USA Azure Marketplace per sottoscrivere la protezione dal ransomware BlueXP.
5. Quando torni alla protezione ransomware di BlueXP, un messaggio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

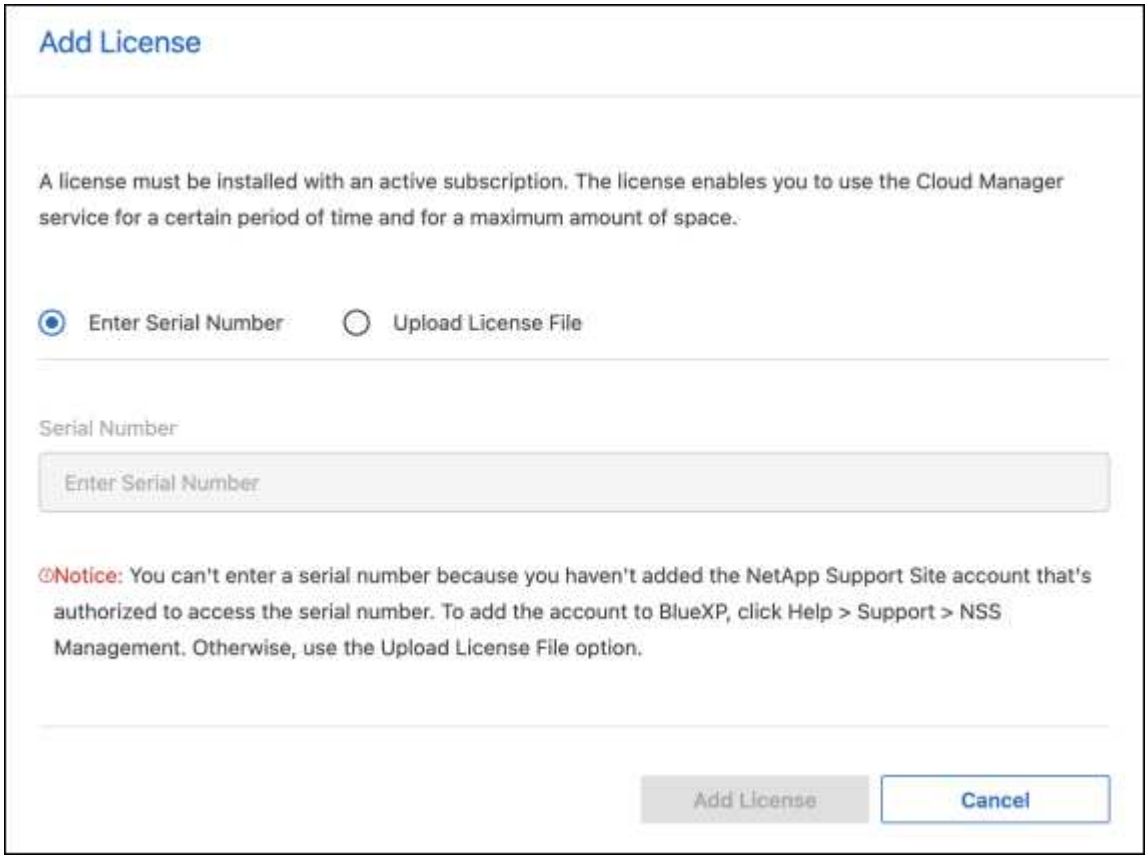
Avrai bisogno del numero di serie della protezione ransomware di BlueXP . Individua questo numero nell'ordine di vendita o contatta l'account team per ottenere queste informazioni.

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.

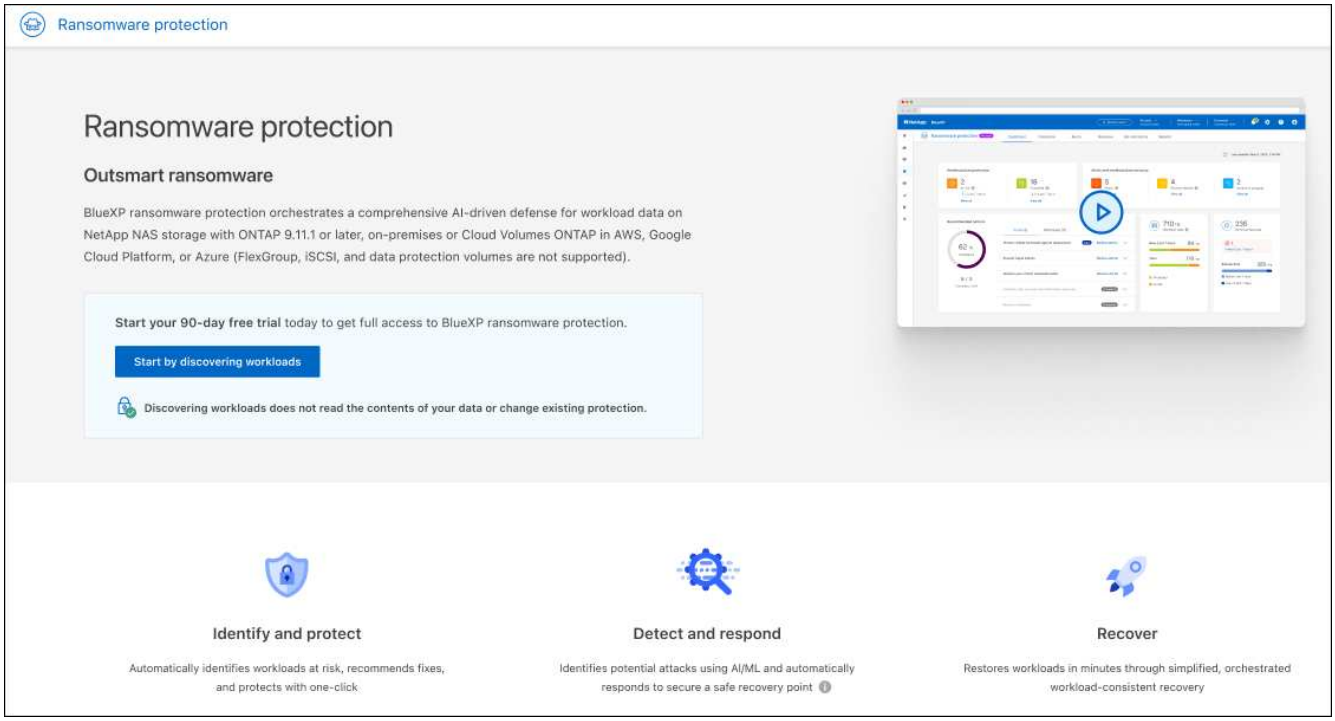
> Non verranno rilevati carichi di lavoro con volumi che utilizzano FlexGroup o iSCSI.

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

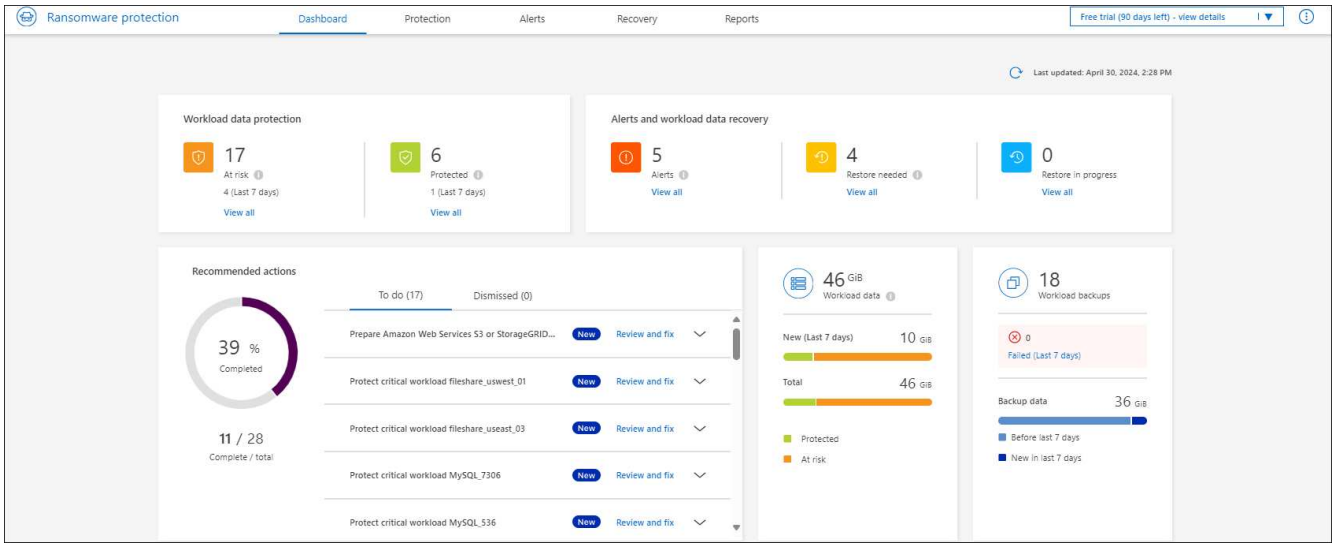
1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

   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

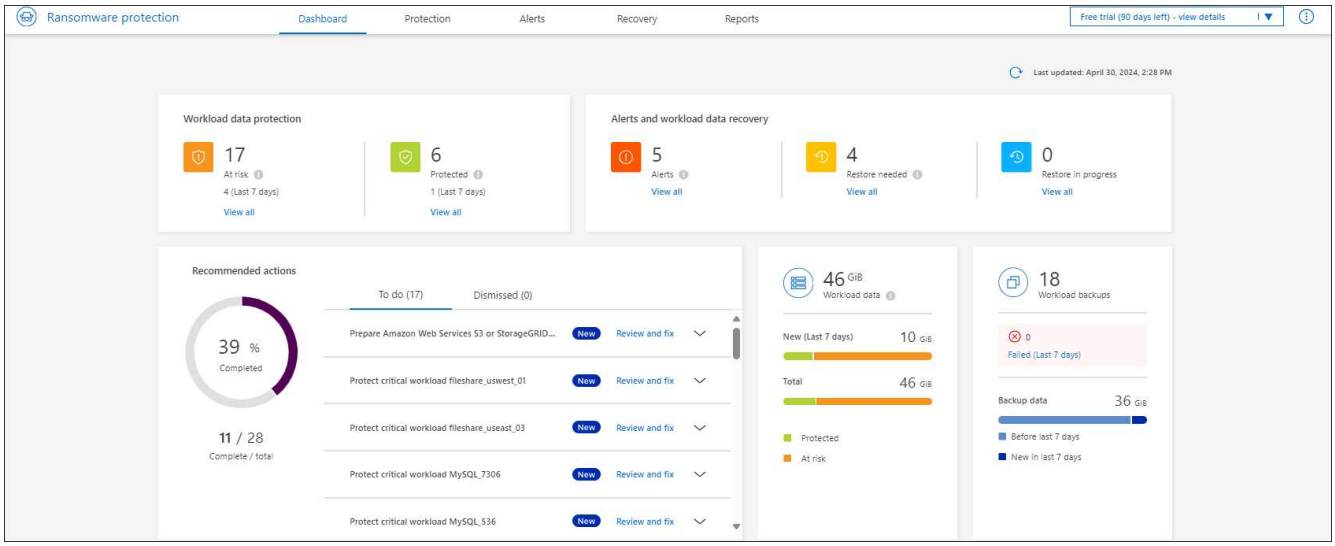
È possibile aggiungere una destinazione di backup in base all'azione consigliata dal Dashboard.

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.

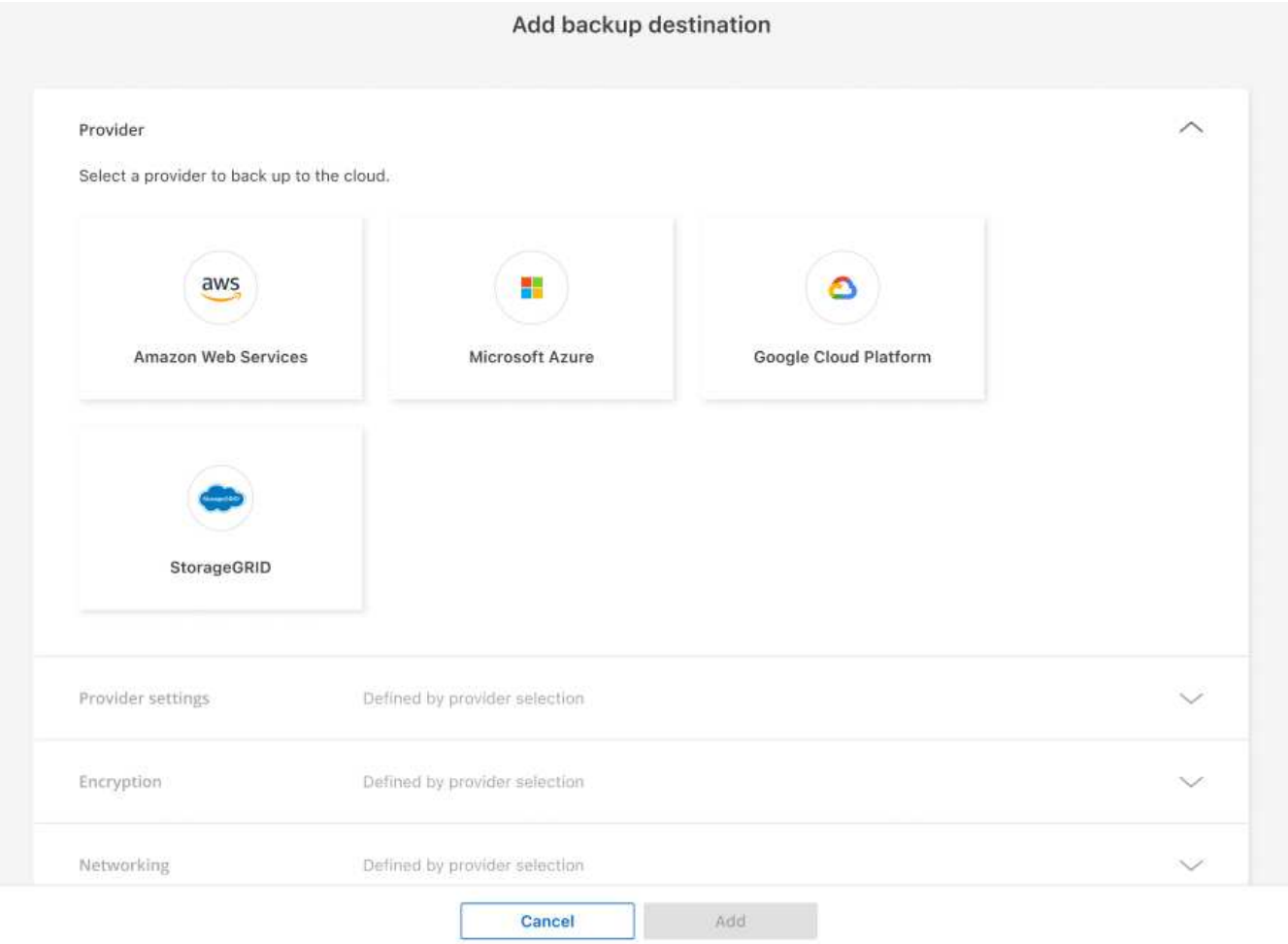
1. Dal menu di protezione dal ransomware BlueXP, seleziona il menu Vertical (verticale) … opzione in alto a destra.
2. Dal menu a discesa, selezionare **Impostazioni**.
3. Per aggiungere una destinazione di backup, selezionare **Aggiungi**.

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**.

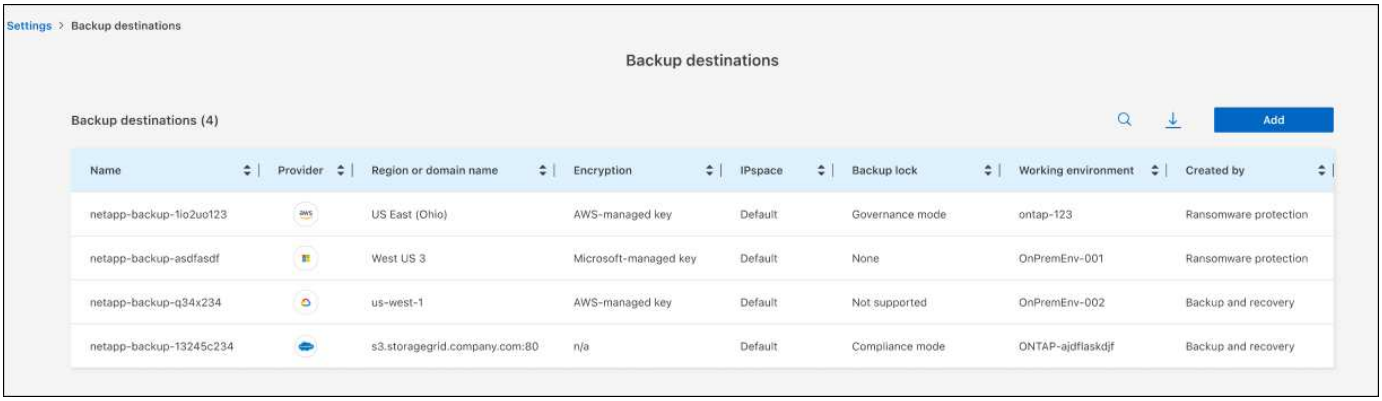
2. Immettere un nome per la destinazione di backup.



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.

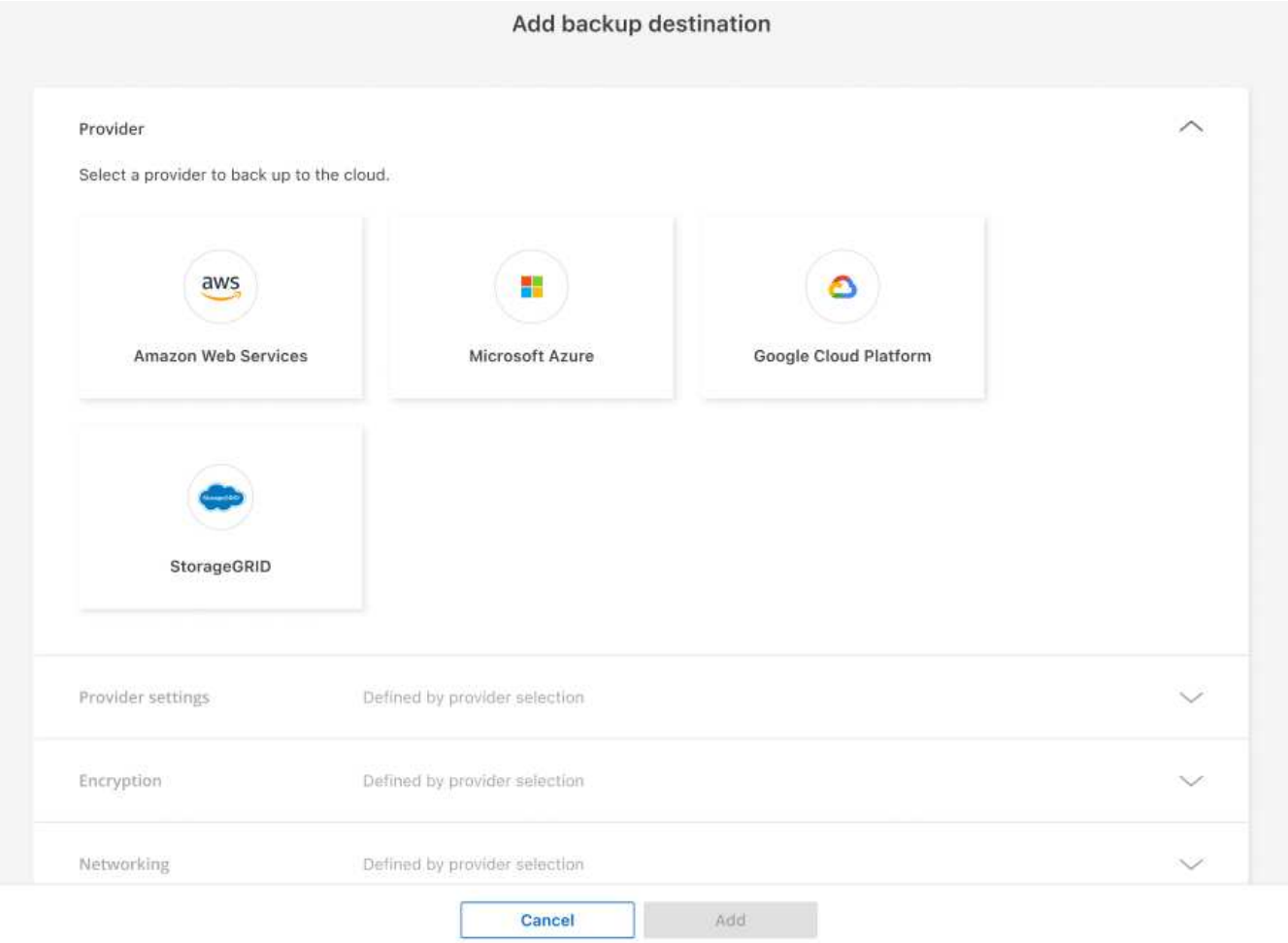


Aggiungere Amazon Web Services come destinazione di backup

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.

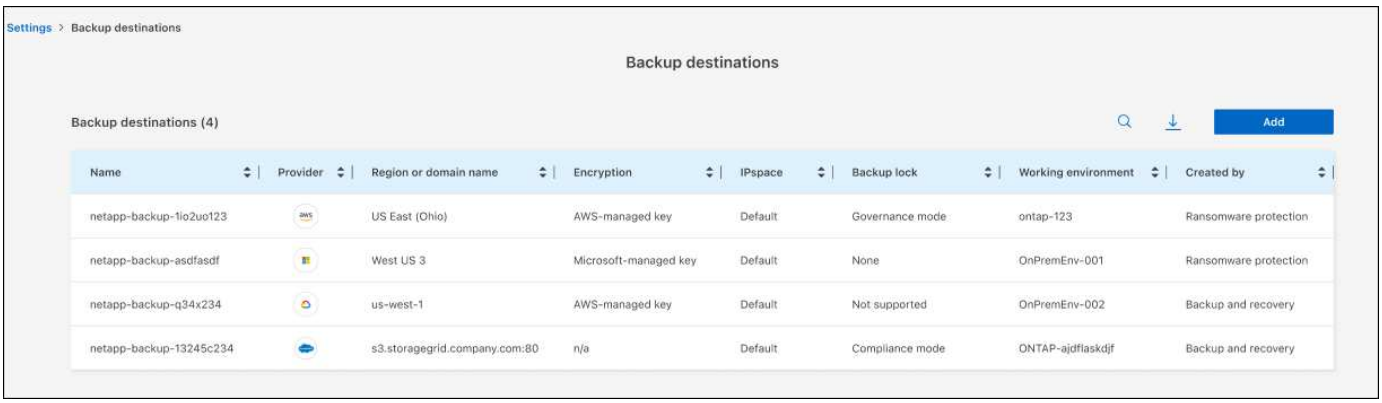
  > Se si configura ora l'impostazione del blocco di backup, non sarà possibile modificarla in un secondo momento dopo la configurazione della destinazione di backup.

  - **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.

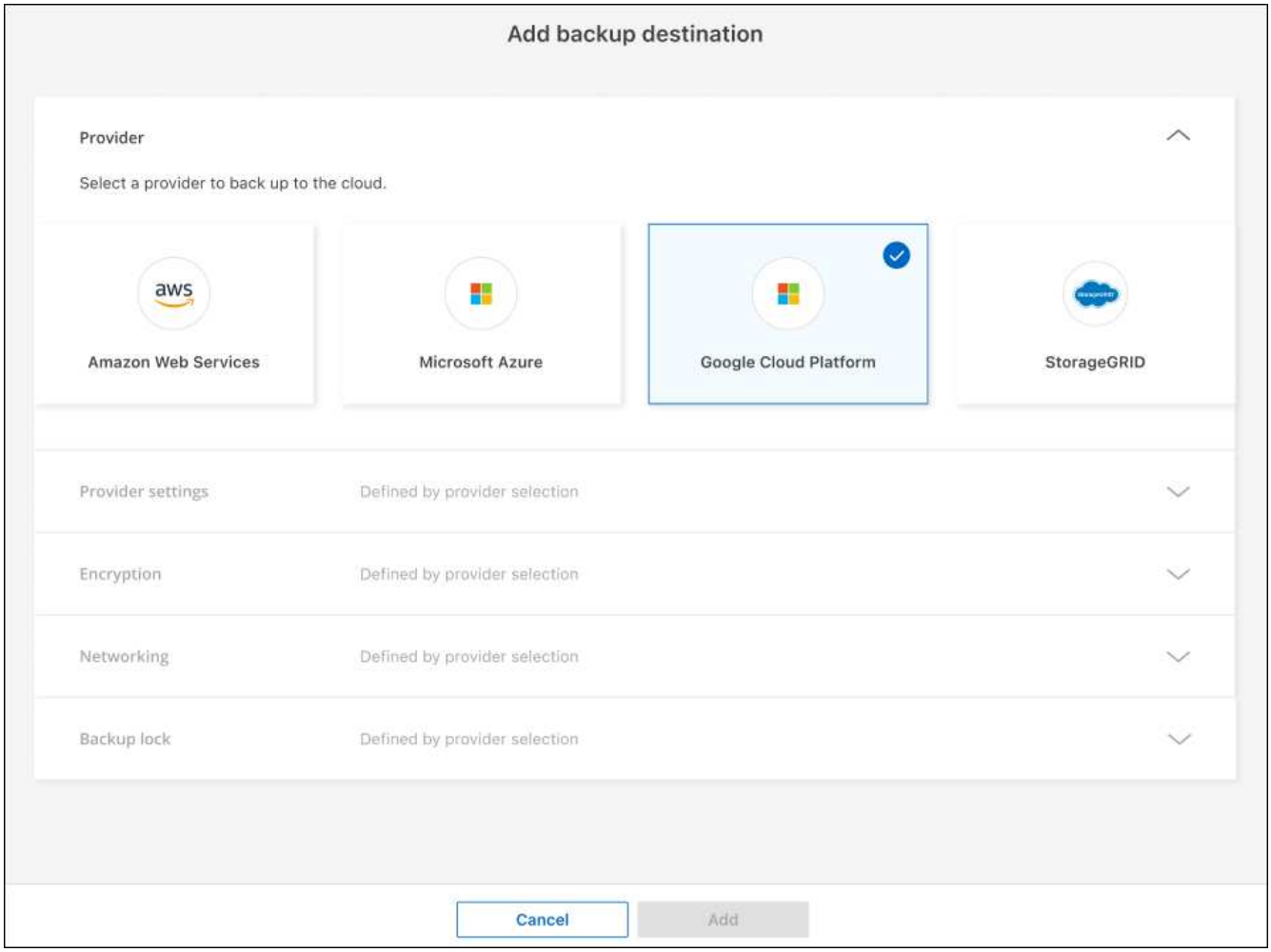


Aggiungi Google Cloud Platform come destinazione di backup

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

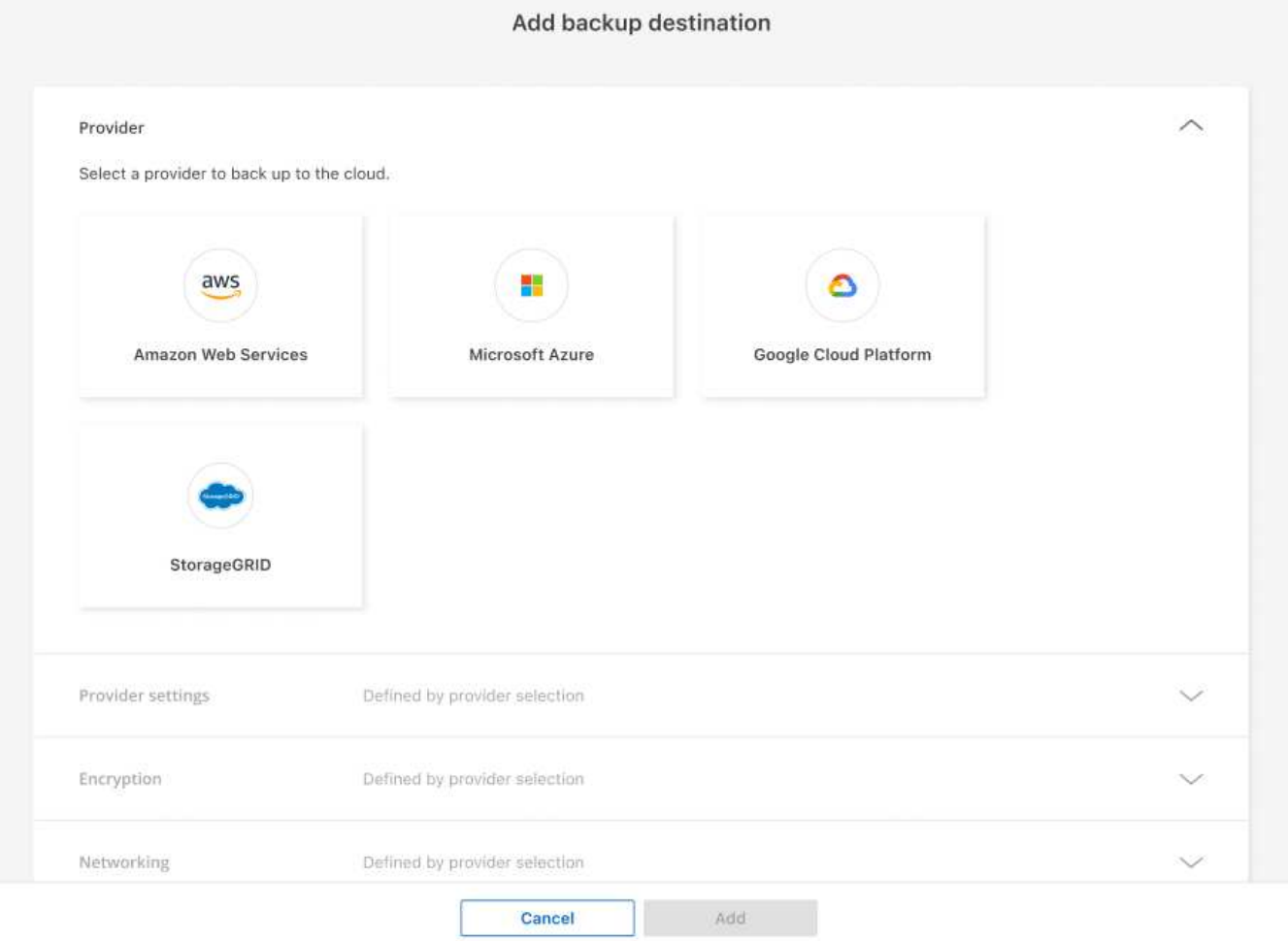
La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.

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.

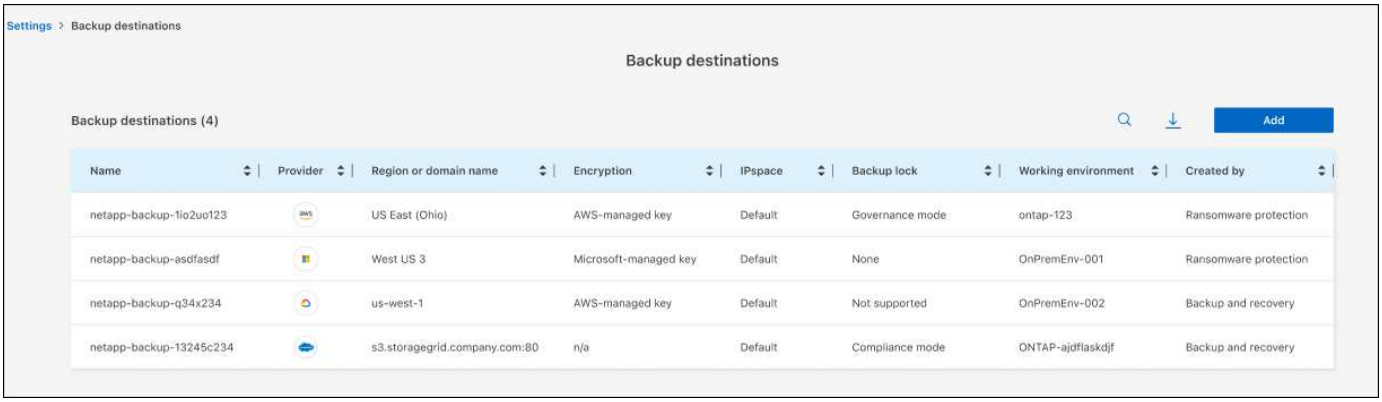
  - **Rete**: Scegliere IPSpace e se si utilizza un endpoint privato.
    - IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
    - Facoltativamente, scegliere se utilizzare un endpoint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

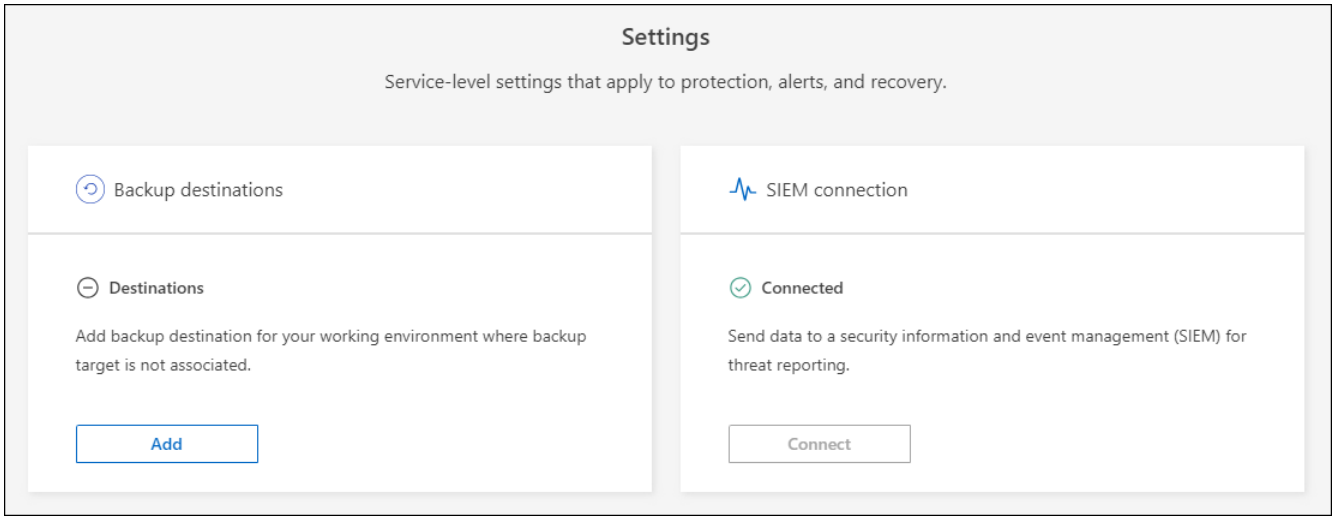
2. Selezionare **Impostazioni** > **Aggiungi dati**.
3. Selezionare **Monitor** > **HTTP Event Collector**.
4. Immettere un nome per il token e selezionare **Avanti**.
5. Selezionare un **Indice predefinito** in cui verranno inviati gli eventi, quindi selezionare **Rivedi**.
6. Verificare che tutte le 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.

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.