Inizia subito

BlueXP ransomware protection

NetApp
March 22, 2024

Sommario

Inizia subito

Scopri l'anteprima della protezione dal ransomware BlueXP

Gli attacchi ransomware possono bloccare l'accesso ai sistemi e i dati, mentre gli autori degli attacchi possono chiedere riscatti 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.

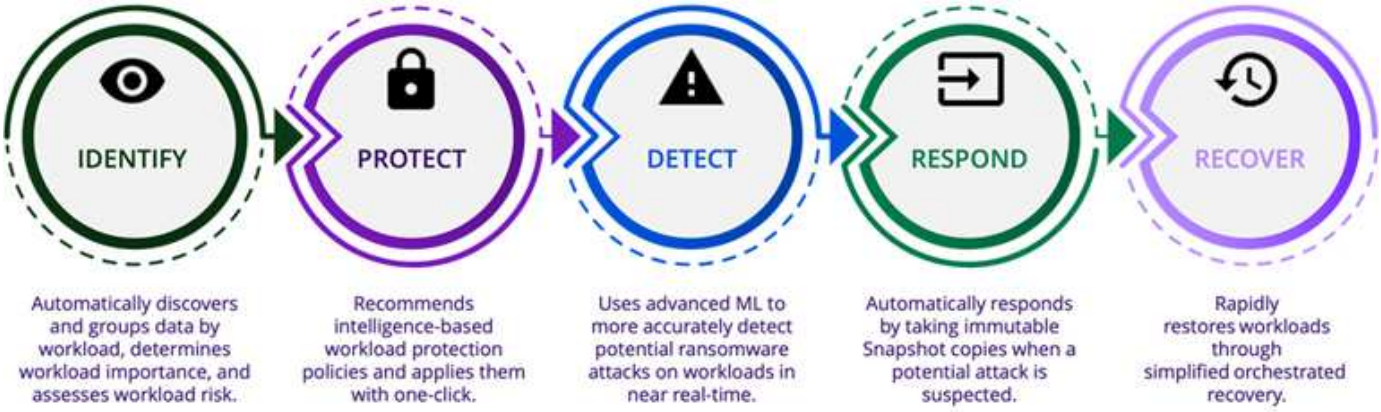
La protezione dal ransomware di BlueXP è un servizio di orchestrazione per protezione, rilevamento e recovery del ransomware. Per la versione in anteprima, il servizio protegge i carichi di lavoro basati su applicazioni dei datastore Oracle, MySQL, VM, e condivisioni di file sullo storage NAS on-premise oltre che su Cloud Volumes ONTAP in Amazon Web Services (utilizzando il protocollo NFS) tra gli account BlueXP ed effettua il backup dei dati su cloud storage Amazon Web Services o NetApp StorageGRID.

QUESTA DOCUMENTAZIONE VIENE FORNITA COME ANTEPRIMA TECNOLOGICA. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale.

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 on-premise con ambienti di lavoro NFS in BlueXP, tra account BlueXP, aree di lavoro e connettori BlueXP. Quindi, il servizio categorizza la priorità dei dati e offre consigli per i miglioramenti alla protezione dal ransomware.
- **Proteggi** i tuoi carichi di lavoro abilitando backup e copie Snapshot sui tuoi dati.
- **Detect** anomalie che potrebbero essere attacchi ransomware.
- **Rispondi** ai potenziali attacchi ransomware avviando automaticamente una copia Snapshot NetApp ONTAP.
- **Recupera** i tuoi workload che aiutano ad accelerare l'uptime dei workload orchestrando diverse tecnologie NetApp. È possibile scegliere di ripristinare volumi, cartelle o file specifici. Il servizio fornisce consigli sulle opzioni migliori.



Vantaggi dell'utilizzo della protezione dal ransomware di BlueXP

La protezione dal ransomware BlueXP offre i seguenti benefici:

- Rileva i carichi di lavoro e i set di dati, analizza la priorità in base all'indice di utilizzo 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).

Costo

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

Licensing

L'anteprima della protezione dal ransomware di BlueXP non richiede licenze speciali. Tutte le licenze di anteprima sono licenze di valutazione.

Per la versione di anteprima, NetApp aiuta a configurare la valutazione e le eventuali licenze richieste.

L'anteprima della protezione dal ransomware di BlueXP richiede le seguenti licenze:

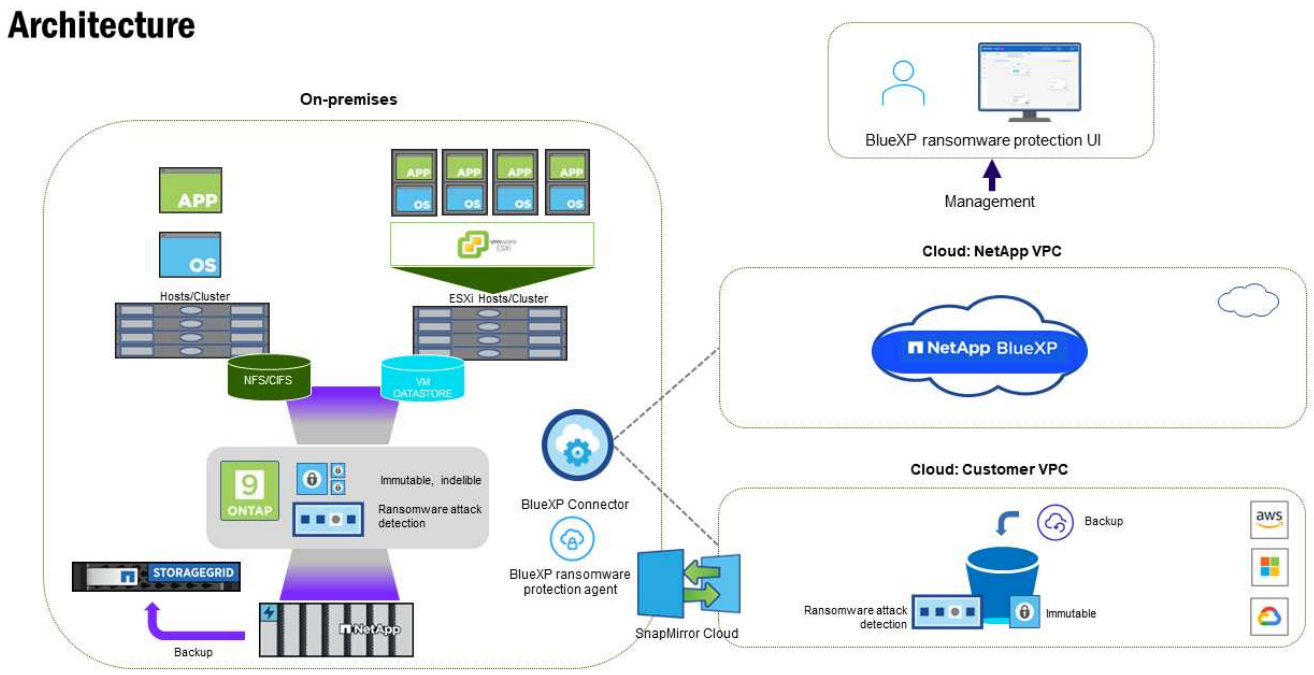
- ONTAP
- Tecnologia per la protezione autonoma dal ransomware NetApp. Fare riferimento a. "Panoramica della

protezione ransomware autonoma" per ulteriori informazioni.

- Servizio di backup e recovery di BlueXP

Come funziona la protezione ransomware di BlueXP

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



Funzione	Descrizione
IDENTIFICA	• Trova tutti i dati NAS (NFS mount) on-premise del cliente connessi ad BlueXP. • Identifica i dati dei clienti dalle API di servizio ONTAP 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, il Digital Advisor di BlueXP, i servizi e le tecnologie NetApp e ONTAP come protezione autonoma da ransomware, FPolicy, policy di backup e policy Snapshot. Scopri di più "Protezione ransomware autonoma" e. "Backup e ripristino BlueXP", "Digital Advisor di 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 protezione dal ransomware inoltre apprende le associazioni di policy e consiglia policy personalizzate per carichi di lavoro simili.

Funzione	Descrizione
PROTEGGI	• Monitora attivamente i workload e orchestra l'utilizzo di backup e recovery di BlueXP e le API 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.

Destinazioni di backup supportate, ambienti di lavoro e origini dati

Utilizza l'anteprima della protezione ransomware di BlueXP per scoprire quanto siano resilienti i tuoi dati a un attacco informatico sui seguenti tipi di destinazioni di backup, ambienti di lavoro e origini dati:

Target di backup supportati

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

Ambienti di lavoro supportati

- NAS ONTAP on-premise (con protocollo NFS)
- ONTAP Select
- Cloud Volumes ONTAP in AWS (utilizzando il protocollo NFS)

Origini dati

Per la versione di anteprima, il servizio protegge i seguenti carichi di lavoro basati su applicazioni:

- Condivisioni di file NetApp
- Datastore VMware

- Database (per la versione di anteprima, Oracle e MySQL)

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 nel ransomware di BlueXP significa garantire che snapshot e backup immutabili vengano eseguiti regolarmente su un dominio di sicurezza diverso utilizzando policy di protezione.
- **Carico di lavoro**: Un carico di lavoro nell'anteprima della 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 versione di anteprima della protezione dal ransomware di BlueXP, sono necessari i seguenti prerequisiti:

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

  Fare riferimento a. "Elenco delle autorizzazioni AWS" per ulteriori informazioni.

- ONTAP 9.11.1 e versioni successive
  - Autorizzazioni ONTAP di amministrazione cluster
  - 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".

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

- In BlueXP:
  - Configurare un connettore BlueXP per ogni cloud privato virtuale (VPC) o in un'area on-premise in BlueXP. Fare riferimento a. "Documentazione di BlueXP per configurare il connettore".

    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.

  - Servizio di backup e recovery di BlueXP con backup abilitato nell'ambiente di lavoro
  - Un ambiente di lavoro BlueXP con storage NAS NetApp on-premise
  - Un account BlueXP con almeno un connettore attivo che si connette ai cluster ONTAP on-premise. Tutti gli ambienti di origine e lavoro devono trovarsi sullo stesso account BlueXP.
  - Un account utente BlueXP con privilegi di account Admin per rilevare le risorse
  - "Requisiti standard di BlueXP"

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.

Esaminare i prerequisiti

"Assicurati che il tuo ambiente soddisfi questi requisiti".

Configurare il servizio di protezione dal ransomware

- "Preparare NetApp StorageGRID o Amazon Web Services come destinazione di backup".
- "Configurare un connettore in BlueXP".
- "Configurare le destinazioni di backup".
- "Scopri i carichi di lavoro in BlueXP".

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

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".

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

Per provare questo servizio, contattare il rappresentante di vendita NetApp. 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 tutte le aree di lavoro e tutti i connettori associati a questo account.

Accedi alla protezione dal ransomware di BlueXP

USA NetApp BlueXP per accedere al servizio di protezione dal ransomware di BlueXP. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

Per ulteriori informazioni, fare riferimento a. "Accedi alla protezione dal ransomware di BlueXP".

Configura destinazioni di backup nella protezione dal ransomware di BlueXP

Utilizza l'opzione delle destinazioni di backup della protezione anti-ransomware di BlueXP per configurare le destinazioni di backup. Per ulteriori informazioni, fare riferimento a. "Configurare le opzioni delle impostazioni".

Accedi alla protezione dal ransomware di BlueXP

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

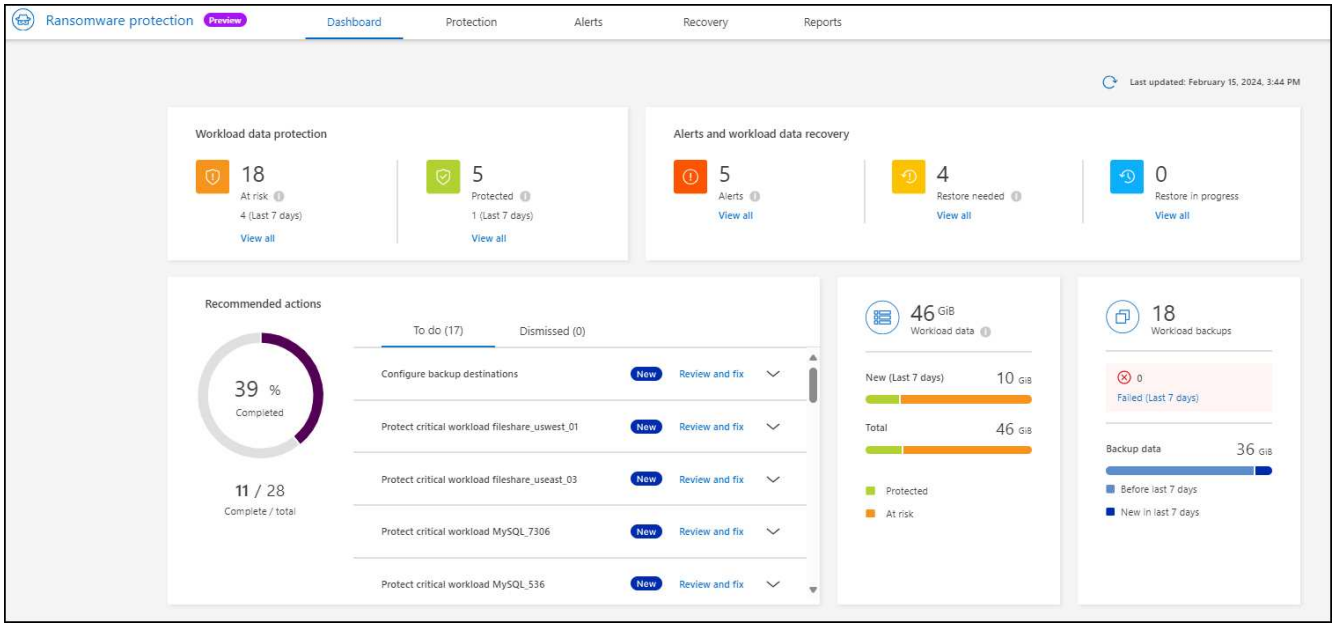
   Viene visualizzata la pagina di accesso a NetApp BlueXP.

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.



4. Iniziare a utilizzare il servizio.
   - Se non hai un connettore BlueXP o non è quello per questa anteprima, potrebbe essere necessario contattare il supporto NetApp o seguire i messaggi per iscriverti a questa anteprima.
   - Se sei un nuovo utente di BlueXP e non hai utilizzato alcun connettore, quando selezioni "**ransomware Protection**", viene visualizzato un messaggio sulla registrazione. Procedi e invia il modulo. NetApp ti contatterà in merito alla tua richiesta di valutazione.
   - Se sei un utente BlueXP con un connettore esistente, quando selezioni "**ransomware Protection**", viene visualizzato un messaggio sulla registrazione.
   - Se stai già partecipando all'anteprima, quando selezioni "**ransomware Protection**", puoi procedere con il servizio. Se non l'hai già fatto, seleziona l'opzione **rileva carichi di lavoro**.

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 il rilevamento, la protezione dal ransomware BlueXP analizza tutti i volumi e i file degli ambienti di lavoro in tutti i connettori e gli spazi di lavoro BlueXP all'interno di un account.

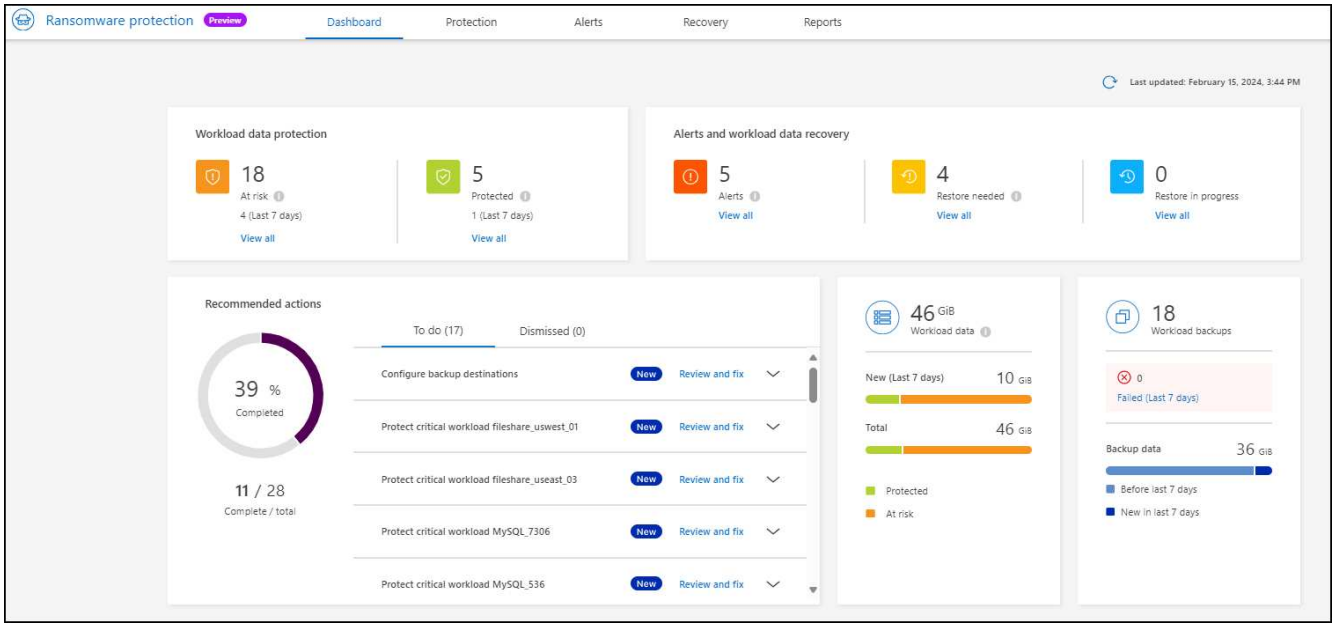
Per la versione di anteprima, la protezione dal ransomware BlueXP valuta applicazioni MySQL, applicazioni Oracle, datastore VMware e file share.

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**.
2. Selezionare **rileva carichi di lavoro** dalla landing page iniziale.

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



Configurare le impostazioni di protezione dal ransomware BlueXP

È possibile configurare una destinazione di backup esaminando i suggerimenti sul dashboard.

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)

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

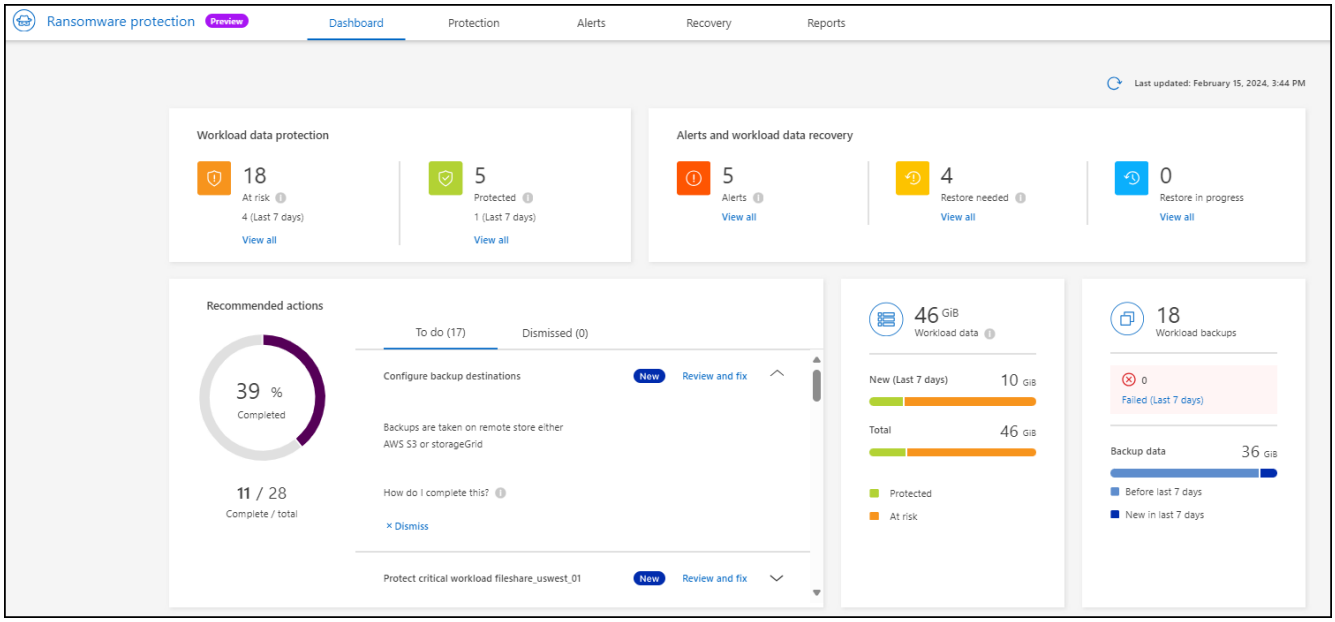
Accedere alle opzioni destinazione backup dalle azioni consigliate del dashboard

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.

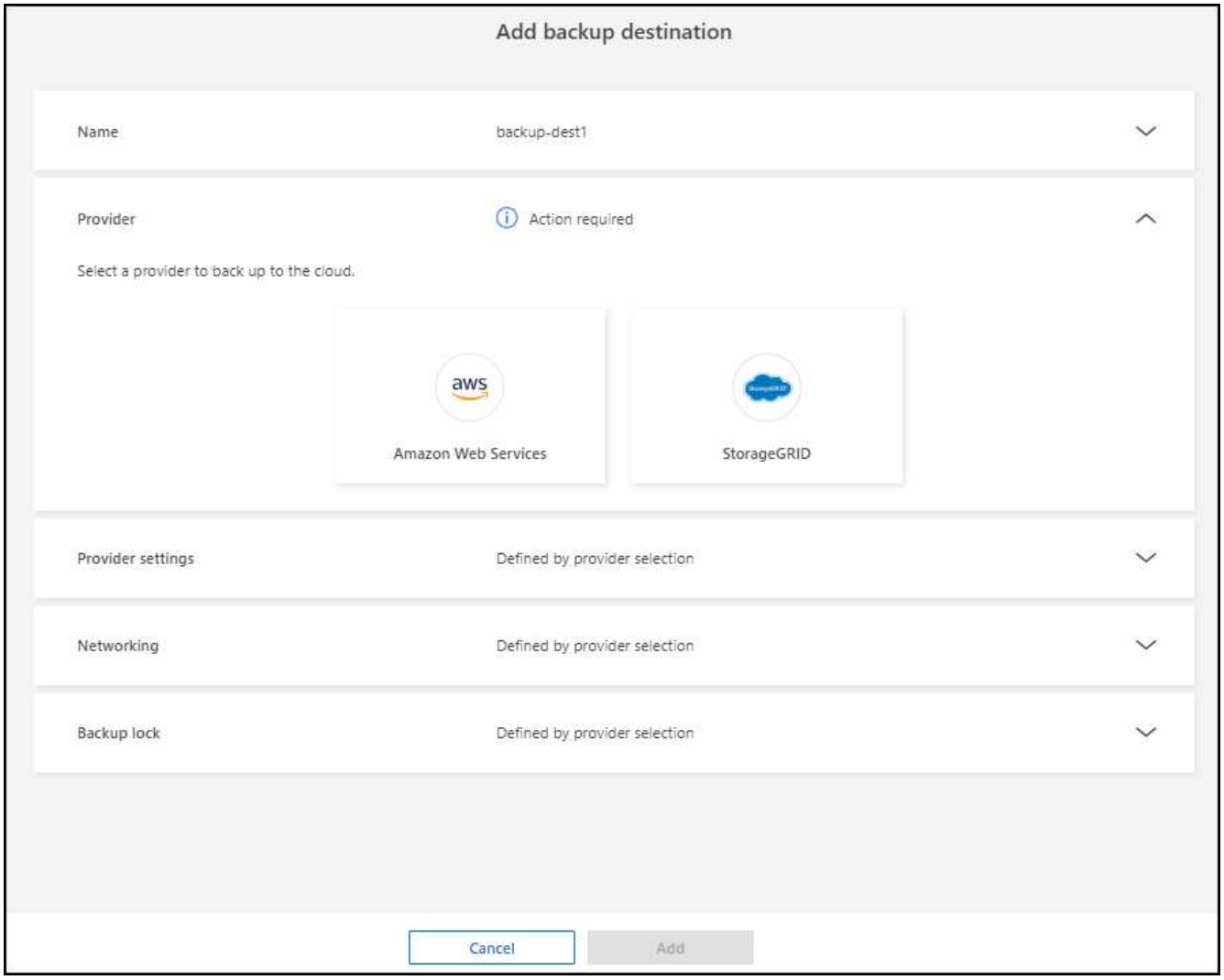


3. Nel dashboard, selezionare **Rivedi e correggi** per la raccomandazione "Configura destinazioni di backup".
4. Continuare con le istruzioni a seconda del provider di backup.

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.
   - **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.

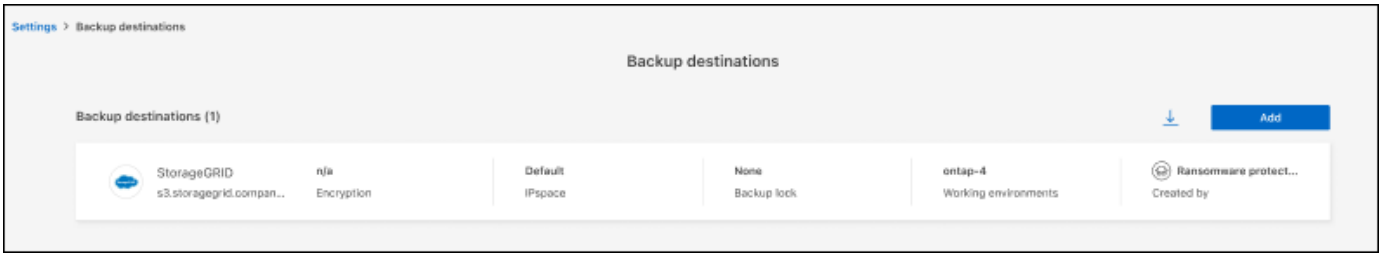
     Se si configura ora l'impostazione del blocco di backup, non sarà possibile modificarla in un secondo momento dopo la configurazione della destinazione di backup.

     - **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.

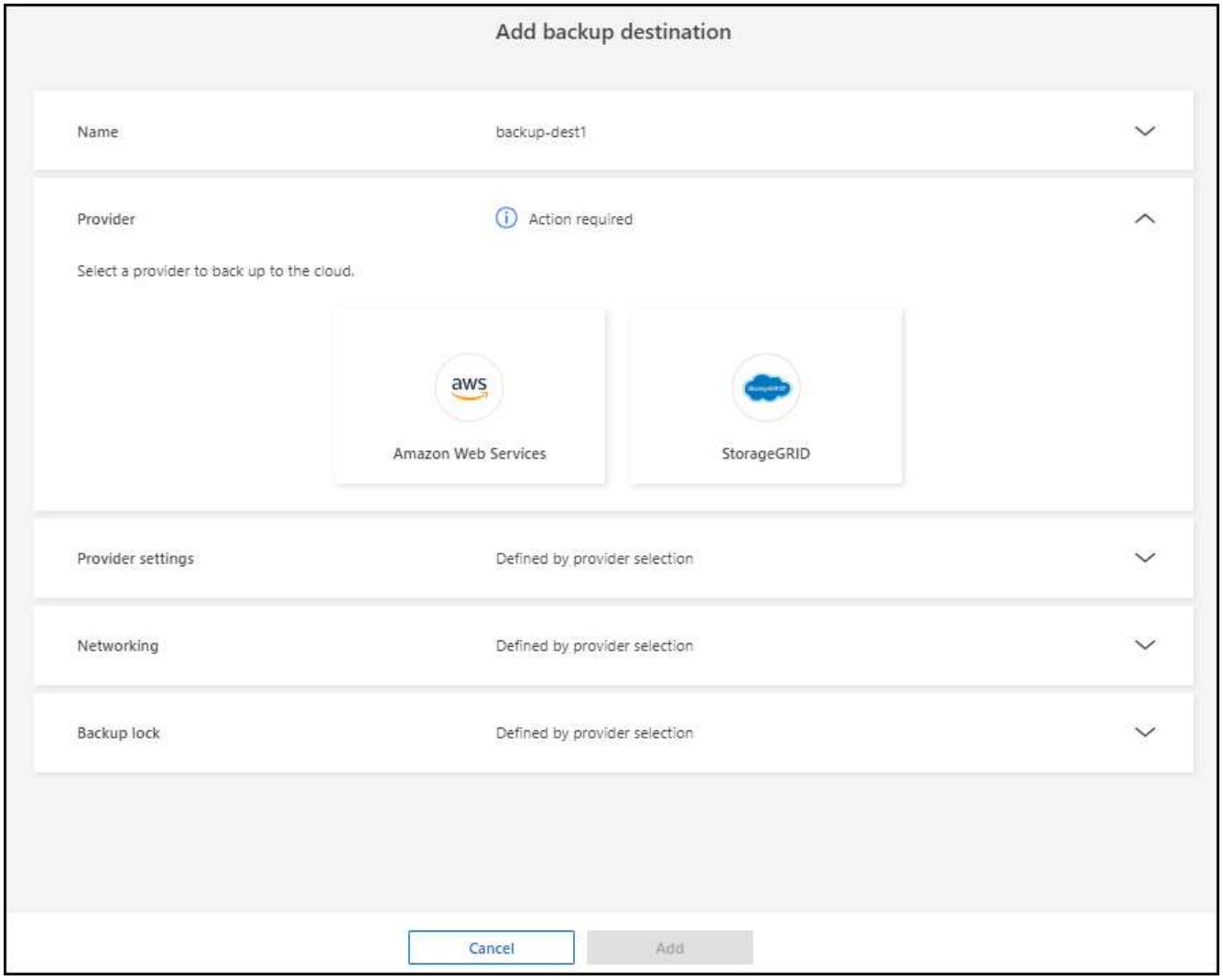


Aggiungere Amazon Web Services come destinazione di backup

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.

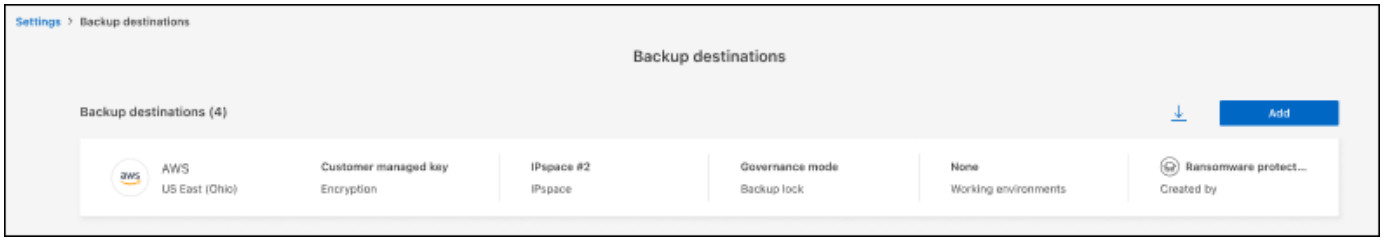
       Per utilizzare AWS PrivateLink, consultare la sezione "AWS PrivateLink per Amazon S3".
   - **Blocco di backup**: Scegliere se si desidera che il servizio protegga i backup dalla modifica o dall'eliminazione. Questa opzione utilizza la tecnologia DataLock di NetApp. Ciascun backup verrà bloccato durante 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.



Domande frequenti sulla protezione dal ransomware BlueXP

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

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.

Ti serve una licenza per usare la protezione da ransomware di BlueXP?
Non è richiesto un file di licenza NetApp (NLF). L'anteprima della protezione dal ransomware di BlueXP non richiede licenze speciali. Tutte le licenze di anteprima sono licenze di valutazione.

La versione in anteprima di questo servizio richiede una licenza del servizio di backup e recovery di BlueXP.

Per la versione di anteprima, NetApp aiuta a configurare la valutazione e le eventuali licenze richieste.

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 la versione di anteprima, devi iscriverti o contattare il tuo commerciale NetApp per provare questo servizio. Quindi, quando si utilizza il connettore BlueXP, esso includerà le funzionalità appropriate per il servizio.

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".

Come vengono gestite le autorizzazioni di accesso?
Solo gli amministratori degli account possono avviare il servizio e rilevare i carichi di lavoro (perché questo implica impegnarsi all'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.

Carichi di lavoro

Che cosa costituisce un carico di lavoro?
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 per la versione di anteprima è determinata dalle copie Snapshot effettuate e dai backup pianificati.

La priorità del carico di lavoro è determinata dalle seguenti frequenze di istantanea:

- **Critico**: Copie snapshot acquisite meno di 1 TB all'ora (pianificazione di protezione altamente aggressiva)
- **Importante**: Le copie snapshot sono state acquisite meno di 1 al giorno e più di 1 all'ora
- **Standard**: Le copie snapshot sono state acquisite più di 1 copie al giorno

Aggiunto nuovo volume, ma non appare ancora
Se è stato aggiunto un nuovo volume al proprio ambiente, ripetere il rilevamento e applicare criteri di protezione per proteggere il nuovo volume.

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