Documentazione NetApp Ransomware Resilience

NetApp Ransomware Resilience

NetApp
February 13, 2026

Sommario

Documentazione NetApp Ransomware Resilience

Note di rilascio

Novità di NetApp Ransomware Resilience

Scopri le novità di NetApp Ransomware Resilience.

19 gennaio 2026

Volumi non supportati

I report di Ransomware Resilience ora acquisiscono informazioni sui volumi supportati e non supportati nel report **Riepilogo**. Utilizzare queste informazioni per diagnosticare il motivo per cui i volumi di un sistema potrebbero non essere idonei alla protezione anti-ransomware.

Per maggiori informazioni, vedere "Scarica i report in Ransomware Resilience".

12 gennaio 2026

Replica gli snapshot su ONTAP

Ransomware Resilience ora supporta l'aggiunta della replica degli snapshot a un sito ONTAP secondario. Con i gruppi di protezione che utilizzano un criterio di replica, è possibile replicare sulla stessa destinazione o su destinazioni diverse per ogni carico di lavoro. È possibile creare una strategia di protezione dal ransomware che includa la replica oppure utilizzare la strategia predefinita.

Per maggiori informazioni, vedere "Proteggi i carichi di lavoro con Ransomware Resilience".

Escludere i carichi di lavoro dalla resilienza del ransomware

Ransomware Resilience ora supporta l'esclusione di carichi di lavoro specifici in un sistema dalla protezione e dalla dashboard di Ransomware Resilience. È possibile escludere i carichi di lavoro dopo l'individuazione e reincluderli se si desidera aggiungere la protezione ransomware. Non ti verrà addebitato alcun costo per i carichi di lavoro esclusi.

Per maggiori informazioni, vedere "Escludi carichi di lavoro".

Contrassegna gli avvisi come in revisione

Ransomware Resilience ora consente di contrassegnare gli avvisi come "In revisione". Utilizza l'etichetta "In revisione" per migliorare la chiarezza all'interno del tuo team durante la selezione e la gestione delle minacce ransomware attive.

Per maggiori informazioni, vedere "Gestisci gli avvisi in Ransomware Resilience".

08 dicembre 2025

Il blocco delle estensioni è abilitato a livello di carico di lavoro

Quando si abilita il blocco delle estensioni, ora viene abilitato a livello di carico di lavoro anziché a livello di VM di archiviazione.

Modifica lo stato dell'avviso sul comportamento dell'utente

Ransomware Resilience ora consente di modificare lo stato degli avvisi sul comportamento degli utenti. È possibile ignorare e risolvere manualmente gli avvisi.

Per maggiori informazioni, vedere "Gestisci gli avvisi in Ransomware Resilience".

Supporto per più agenti della console

Ransomware Resilience ora supporta l'utilizzo di più agenti Console per gestire gli stessi sistemi.

Per ulteriori informazioni sugli agenti della console, vedere"Creare un agente Console" .

10 novembre 2025

Questa versione include miglioramenti e miglioramenti generali.

06 ottobre 2025

La BlueXP ransomware protection è ora NetApp Ransomware Resilience

Il servizio BlueXP ransomware protection è stato rinominato NetApp Ransomware Resilience.

BlueXP è ora NetApp Console

NetApp Console offre una gestione centralizzata dei servizi di storage e dati in ambienti on-premise e cloud di livello aziendale, offrendo informazioni in tempo reale, flussi di lavoro più rapidi e amministrazione semplificata.

Per i dettagli su cosa è cambiato, vedere il "Note sulla versione NetApp Console" .

Rilevamento delle violazioni dei dati

Ransomware Resilience include un nuovo meccanismo di rilevamento che può essere attivato in pochi passaggi per rilevare letture anomale da parte dell'utente come indicatore precoce di violazione dei dati. La resilienza del ransomware raccoglie e analizza gli eventi di lettura degli utenti creando una baseline storica, ovvero un profilo del comportamento normale e previsto dai dati passati. Quando l'attività di un nuovo utente si discosta in modo significativo da questa norma consolidata (ad esempio, un'impennata di letture inaspettata combinata con modelli di lettura sospetti), viene generato un avviso. Ransomware Resilience include un modello di intelligenza artificiale per rilevare modelli di lettura sospetti.

A differenza del rilevamento della crittografia tramite ARP a livello di archiviazione, il rilevamento dell'anomalia nel comportamento dell'utente viene eseguito nel servizio Ransomware Resilience SaaS mediante la raccolta di eventi FPolicy.

> Devi usare il nuovo"Amministratore del comportamento utente di Ransomware Resilience e visualizzatore del comportamento utente di Ransomware Resilience" ruoli per accedere alle impostazioni di rilevamento dei comportamenti sospetti degli utenti.

Per maggiori informazioni, vedere"Abilita il rilevamento delle attività sospette degli utenti" E"Visualizza il comportamento anomalo dell'utente" .

Ulteriori rilevamenti di attività sospette degli utenti

Oltre al rilevamento delle violazioni dei dati, Ransomware Resilience rileva anche i seguenti tipi di avviso in base alle attività sospette osservate dagli utenti:

- **Distruzione dei dati - potenziale attacco** - Viene creato un avviso con la gravità del potenziale attacco quando il numero di eliminazioni di file supera la norma storica.
- **Comportamento sospetto dell'utente - potenziale attacco** - Viene creato un avviso con la gravità del potenziale attacco quando vengono osservate operazioni di lettura, ridenominazione ed eliminazione in una sequenza simile a un attacco ransomware
- **Comportamento sospetto dell'utente - Avviso** - Un avviso con gravità di avviso viene creato quando il numero totale di attività sui file (lettura, eliminazione, ridenominazione ecc.) supera la norma storica

Nuovi ruoli utente per il rilevamento delle violazioni dei dati

Per gestire gli avvisi di attività sospette degli utenti, Ransomware Resilience ha introdotto due nuovi ruoli per gli amministratori dell'organizzazione Console per concedere l'accesso al rilevamento di attività sospette degli utenti: amministratore del comportamento degli utenti di Ransomware Resilience e visualizzatore del comportamento degli utenti di Ransomware Resilience.

Per configurare le impostazioni relative al comportamento sospetto degli utenti, è necessario essere un amministratore del comportamento degli utenti. Il ruolo di amministratore Ransomware Resilience non è supportato per la configurazione delle impostazioni relative al comportamento sospetto degli utenti.

Per ulteriori informazioni, consultare "Accesso basato sui ruoli NetApp Ransomware Resilience" .

12 agosto 2025

Questa versione include miglioramenti e miglioramenti generali.

15 luglio 2025

Supporto del carico di lavoro SAN

Questa versione include il supporto per i carichi di lavoro SAN nella BlueXP ransomware protection. Ora è possibile proteggere i carichi di lavoro SAN oltre ai carichi di lavoro NFS e CIFS.

Per ulteriori informazioni, fare riferimento a "Prerequisiti BlueXP ransomware protection" .

Protezione migliorata del carico di lavoro

Questa versione migliora il processo di configurazione per i carichi di lavoro con policy di snapshot e backup da altri strumenti NetApp come SnapCenter o BlueXP backup and recovery. Nelle versioni precedenti, la BlueXP ransomware protection rilevava le policy di altri strumenti, consentendo solo di modificare la policy di rilevamento. Con questa versione, è possibile sostituire i criteri di snapshot e backup con i criteri BlueXP ransomware protection oppure continuare a utilizzare i criteri di altri strumenti.

Per i dettagli, fare riferimento a"Proteggere i carichi di lavoro" .

Notifiche e-mail

Se la BlueXP ransomware protection rileva un possibile attacco, viene visualizzata una notifica nelle Notifiche BlueXP e viene inviata un'e-mail all'indirizzo e-mail configurato.

L’e-mail include informazioni sulla gravità, sul carico di lavoro interessato e un collegamento all’avviso nella scheda **Avvisi** della BlueXP ransomware protection .

Se hai configurato un sistema di sicurezza e gestione degli eventi (SIEM) nella BlueXP ransomware protection, il servizio invia i dettagli dell’avviso al tuo sistema SIEM.

Per i dettagli, fare riferimento a"Gestisci gli avvisi di ransomware rilevati" .

9 giugno 2025

Aggiornamenti della landing page

Questa versione include aggiornamenti alla landing page per la BlueXP ransomware protection che semplificano l’avvio della prova gratuita e la scoperta.

Aggiornamenti sulle esercitazioni di preparazione

In precedenza, era possibile eseguire un’esercitazione di preparazione al ransomware simulando un attacco su un nuovo carico di lavoro di esempio. Grazie a questa funzionalità è possibile analizzare l’attacco simulato e recuperare il carico di lavoro. Utilizzare questa funzione per testare le notifiche di avviso, la risposta e il ripristino. Esegui e programma queste esercitazioni tutte le volte che è necessario.

Con questa versione, puoi utilizzare un nuovo pulsante sulla Dashboard BlueXP ransomware protection per eseguire un’esercitazione di preparazione al ransomware su un carico di lavoro di prova, semplificando la simulazione di attacchi ransomware, l’analisi del loro impatto e il ripristino efficiente dei carichi di lavoro, il tutto all’interno di un ambiente controllato.

Ora è possibile eseguire esercitazioni di preparazione sui carichi di lavoro CIFS (SMB) oltre che sui carichi di lavoro NFS.

Per i dettagli, fare riferimento a "Eseguire un’esercitazione di preparazione all’attacco ransomware" .

Abilita gli aggiornamenti BlueXP classification

Prima di utilizzare la BlueXP classification all’interno del servizio BlueXP ransomware protection , è necessario abilitare la BlueXP classification per eseguire la scansione dei dati. La classificazione dei dati aiuta a trovare informazioni personali identificabili (PII), il che può aumentare i rischi per la sicurezza.

È possibile distribuire la BlueXP classification su un carico di lavoro di condivisione file dall’interno BlueXP ransomware protection. Nella colonna **Esposizione alla privacy**, seleziona l’opzione **Identifica esposizione**. Se hai abilitato il servizio di classificazione, questa azione identifica l’esposizione. Altrimenti, con questa versione, una finestra di dialogo presenta l’opzione per distribuire la BlueXP classification. Selezionare **Distribuisci** per andare alla pagina di destinazione del servizio BlueXP classification , dove è possibile distribuire tale servizio. O

Per i dettagli, fare riferimento a "Distribuisci la BlueXP classification nel cloud" e per utilizzare il servizio all’interno BlueXP ransomware protection, fare riferimento a "Scansiona le informazioni di identificazione personale con la BlueXP classification" .

13 maggio 2025

Segnalazione di ambienti di lavoro non supportati nella BlueXP ransomware protection

Durante il flusso di lavoro di individuazione, la BlueXP ransomware protection segnala maggiori dettagli

quando si passa il mouse su Carichi di lavoro supportati o non supportati. Questo ti aiuterà a capire perché alcuni dei tuoi carichi di lavoro non vengono rilevati dal servizio BlueXP ransomware protection .

Esistono molti motivi per cui il servizio non supporta un ambiente di lavoro, ad esempio la versione ONTAP sul tuo ambiente di lavoro potrebbe essere inferiore a quella richiesta. Quando si passa il mouse su un ambiente di lavoro non supportato, una descrizione comandi ne mostra il motivo.

È possibile visualizzare gli ambienti di lavoro non supportati durante la fase di rilevamento iniziale, da cui è anche possibile scaricare i risultati. È anche possibile visualizzare i risultati dell'individuazione tramite l'opzione **Individuazione del carico di lavoro** nella pagina Impostazioni.

Per i dettagli, fare riferimento a "Scopri i carichi di lavoro nella BlueXP ransomware protection" .

29 aprile 2025

Supporto per Amazon FSx for NetApp ONTAP

Questa versione supporta Amazon FSx for NetApp ONTAP. Questa funzionalità ti aiuta a proteggere i tuoi carichi di lavoro FSx for ONTAP con la BlueXP ransomware protection.

FSx for ONTAP è un servizio completamente gestito che offre la potenza dello storage NetApp ONTAP nel cloud. Offre le stesse funzionalità, prestazioni e capacità amministrative che utilizzi in locale, con l'agilità e la scalabilità di un servizio AWS nativo.

Sono state apportate le seguenti modifiche al flusso di lavoro BlueXP ransomware protection :

- Discovery include carichi di lavoro negli ambienti di lavoro FSx per ONTAP 9.15.
- La scheda Protezione mostra i carichi di lavoro negli ambienti FSx per ONTAP . In questo ambiente, è necessario eseguire operazioni di backup utilizzando il servizio di backup FSx for ONTAP . È possibile ripristinare questi carichi di lavoro utilizzando gli snapshot BlueXP ransomware protection .

  Non è possibile impostare i criteri di backup per un carico di lavoro in esecuzione su FSx per ONTAP in BlueXP. Tutte le policy di backup esistenti impostate in Amazon FSx for NetApp ONTAP rimangono invariate.

- Gli incidenti di avviso mostrano il nuovo ambiente di lavoro FSx per ONTAP .

Per i dettagli, fare riferimento a "Scopri di più sulla BlueXP ransomware protection e sugli ambienti di lavoro" .

Per informazioni sulle opzioni supportate, fare riferimento a "Limitazioni BlueXP ransomware protection" .

Ruolo di accesso BlueXP richiesto

Ora è necessario uno dei seguenti ruoli di accesso per visualizzare, scoprire o gestire la BlueXP ransomware protection: amministratore dell'organizzazione, amministratore della cartella o del progetto, amministratore della protezione ransomware o visualizzatore della protezione ransomware.

"Scopri di più sui ruoli di accesso BlueXP per tutti i servizi" .

14 aprile 2025

Rapporti di esercitazione di prontezza

Con questa versione è possibile esaminare i report di esercitazione sulla preparazione agli attacchi ransomware. Un'esercitazione di preparazione consente di simulare un attacco ransomware su un carico di lavoro di esempio appena creato. Quindi, esaminare l'attacco simulato e recuperare il carico di lavoro di esempio. Questa funzionalità ti aiuta a sapere se sei preparato in caso di un vero e proprio attacco ransomware testando i processi di notifica degli avvisi, risposta e ripristino.

Per i dettagli, fare riferimento a "Eseguire un'esercitazione di preparazione all'attacco ransomware" .

Nuovi ruoli e autorizzazioni di controllo degli accessi basati sui ruoli

In precedenza, era possibile assegnare ruoli e autorizzazioni agli utenti in base alle loro responsabilità, il che aiutava a gestire l'accesso degli utenti alla BlueXP ransomware protection. Con questa versione sono disponibili due nuovi ruoli specifici per la BlueXP ransomware protection con autorizzazioni aggiornate. I nuovi ruoli sono:

- Amministratore della protezione ransomware
- Visualizzatore di protezione ransomware

Per i dettagli sui permessi, fare riferimento a "BlueXP ransomware protection con accesso basato sui ruoli alle funzionalità" .

Miglioramenti nei pagamenti

Questa versione include diversi miglioramenti al processo di pagamento.

Per i dettagli, fare riferimento a "Impostare le opzioni di licenza e pagamento" .

10 marzo 2025

Simula un attacco e rispondi

Con questa versione, simula un attacco ransomware per testare la tua risposta a un avviso ransomware. Questa funzionalità ti aiuta a sapere se sei preparato in caso di un vero e proprio attacco ransomware testando i processi di notifica degli avvisi, risposta e ripristino.

Per i dettagli, fare riferimento a "Eseguire un'esercitazione di preparazione all'attacco ransomware" .

Miglioramenti al processo di scoperta

Questa versione include miglioramenti ai processi di scoperta e riscoperta selettiva:

- Con questa versione, puoi scoprire i carichi di lavoro appena creati che sono stati aggiunti agli ambienti di lavoro selezionati in precedenza.
- In questa versione è anche possibile selezionare *nuovi* ambienti di lavoro. Questa funzionalità ti aiuta a proteggere i nuovi carichi di lavoro aggiunti al tuo ambiente.
- È possibile eseguire questi processi di individuazione durante il processo di individuazione iniziale oppure all'interno dell'opzione Impostazioni.

Per i dettagli, fare riferimento a "Scopri i carichi di lavoro appena creati per gli ambienti di lavoro selezionati in precedenza" E "Configura le funzionalità con l'opzione Impostazioni" .

Avvisi generati quando viene rilevata una crittografia elevata

Con questa versione, puoi visualizzare avvisi quando viene rilevata una crittografia elevata nei tuoi carichi di lavoro, anche senza modifiche significative alle estensioni dei file. Questa funzionalità, che utilizza l'intelligenza artificiale ONTAP Autonomous Ransomware Protection (ARP), aiuta a identificare i carichi di lavoro a rischio di attacchi ransomware. Utilizza questa funzionalità e scarica l'elenco completo dei file interessati, con o senza modifiche all'estensione.

Per i dettagli, fare riferimento a "Rispondere a un avviso di ransomware rilevato" .

16 dicembre 2024

Rileva comportamenti anomali degli utenti utilizzando Data Infrastructure Insights Storage Workload Security

Con questa versione, puoi utilizzare Data Infrastructure Insights Storage Workload Security per rilevare comportamenti anomali degli utenti nei tuoi carichi di lavoro di archiviazione. Questa funzionalità ti aiuta a identificare potenziali minacce alla sicurezza e a bloccare gli utenti potenzialmente malintenzionati per proteggere i tuoi dati.

Per i dettagli, fare riferimento a "Rispondere a un avviso di ransomware rilevato" .

Prima di utilizzare Data Infrastructure Insights Storage Workload Security per rilevare comportamenti anomali degli utenti, è necessario configurare l'opzione tramite l'opzione **Impostazioni** BlueXP ransomware protection .

Fare riferimento a "Configurare le impostazioni BlueXP ransomware protection" .

Seleziona i carichi di lavoro da scoprire e proteggere

Con questa versione, ora puoi fare quanto segue:

- All'interno di ciascun connettore, seleziona gli ambienti di lavoro in cui desideri individuare i carichi di lavoro. Questa funzionalità potrebbe rivelarsi utile se si desidera proteggere carichi di lavoro specifici nel proprio ambiente e non in altri.
- Durante l'individuazione del carico di lavoro, è possibile abilitare l'individuazione automatica dei carichi di lavoro per connettore. Questa funzionalità consente di selezionare i carichi di lavoro che si desidera proteggere.
- Scopri i carichi di lavoro appena creati per gli ambienti di lavoro selezionati in precedenza.

Fare riferimento a "Scopri i carichi di lavoro" .

7 novembre 2024

Abilita la classificazione dei dati e la scansione per informazioni di identificazione personale (PII)

Con questa versione, puoi abilitare la BlueXP classification, un componente fondamentale della famiglia BlueXP , per analizzare e classificare i dati nei carichi di lavoro di condivisione file. La classificazione dei dati aiuta a identificare se i dati contengono informazioni personali o private, il che può aumentare i rischi per la sicurezza. Questo processo influisce anche sull'importanza del carico di lavoro e ti aiuta a garantire che i carichi di lavoro vengano protetti con il giusto livello di protezione.

La scansione dei dati PII nella BlueXP ransomware protection è generalmente disponibile per i clienti che hanno implementato la BlueXP classification. La BlueXP classification è disponibile come parte della

piattaforma BlueXP senza costi aggiuntivi e può essere distribuita in locale o nel cloud del cliente.

Fare riferimento a "Configurare le impostazioni BlueXP ransomware protection" .

Per avviare la scansione, nella pagina Protezione, fare clic su **Identifica esposizione** nella colonna Esposizione alla privacy.

"Scansiona i dati sensibili identificabili personalmente con la BlueXP classification" .

Integrazione SIEM con Microsoft Sentinel

Ora puoi inviare dati al tuo sistema di sicurezza e gestione degli eventi (SIEM) per l'analisi e il rilevamento delle minacce tramite Microsoft Sentinel. In precedenza, era possibile selezionare AWS Security Hub o Splunk Cloud come SIEM.

"Scopri di più sulla configurazione delle impostazioni BlueXP ransomware protection" .

Prova gratuita ora per 30 giorni

Con questa versione, le nuove distribuzioni della BlueXP ransomware protection hanno ora 30 giorni di prova gratuita. In precedenza, la BlueXP ransomware protection era disponibile in prova gratuita per 90 giorni. Se hai già usufruito della prova gratuita di 90 giorni, l'offerta sarà valida per 90 giorni.

Ripristina il carico di lavoro dell'applicazione a livello di file per Podman

Prima di ripristinare il carico di lavoro di un'applicazione a livello di file, ora puoi visualizzare un elenco dei file che potrebbero essere stati interessati da un attacco e identificare quelli che desideri ripristinare. In precedenza, se i connettori BlueXP in un'organizzazione (in precedenza un account) utilizzavano Podman, questa funzionalità era disabilitata. Ora è abilitato per Podman. Puoi lasciare che la BlueXP ransomware protection scelga i file da ripristinare, puoi caricare un file CSV che elenca tutti i file interessati da un avviso oppure puoi identificare manualmente i file che desideri ripristinare.

"Scopri di più sul recupero da un attacco ransomware" .

30 settembre 2024

Raggruppamento personalizzato dei carichi di lavoro di condivisione file

Con questa versione, ora puoi raggruppare le condivisioni file in gruppi per proteggere più facilmente il tuo patrimonio di dati. Il servizio può proteggere contemporaneamente tutti i volumi di un gruppo. In precedenza era necessario proteggere ogni volume separatamente.

"Scopri di più sul raggruppamento dei carichi di lavoro di condivisione file nelle strategie di protezione dal ransomware" .

2 settembre 2024

Valutazione del rischio per la sicurezza da parte di Digital Advisor

La BlueXP ransomware protection ora raccoglie informazioni sui rischi per la sicurezza elevati e critici correlati a un cluster da NetApp Digital Advisor. Se viene rilevato un rischio, la BlueXP ransomware protection fornisce una raccomandazione nel riquadro **Azioni consigliate** della Dashboard: "Correggi una vulnerabilità di sicurezza nota sul cluster <nome>". Dalla raccomandazione sulla Dashboard, cliccando su **Rivedi e correggi** viene suggerito di consultare Digital Advisor e un articolo Common Vulnerability & Exposure (CVE) per

risolvere il rischio per la sicurezza. Se sono presenti più rischi per la sicurezza, rivedere le informazioni in Digital Advisor.

Fare riferimento a "Documentazione Digital Advisor" .

Esegui il backup su Google Cloud Platform

Con questa versione, puoi impostare una destinazione di backup su un bucket di Google Cloud Platform. In precedenza, era possibile aggiungere destinazioni di backup solo a NetApp StorageGRID, Amazon Web Services e Microsoft Azure.

"Scopri di più sulla configurazione delle impostazioni BlueXP ransomware protection" .

Supporto per Google Cloud Platform

Il servizio ora supporta Cloud Volumes ONTAP per Google Cloud Platform per la protezione dell'archiviazione. In precedenza, il servizio supportava solo Cloud Volumes ONTAP per Amazon Web Services e Microsoft Azure insieme a NAS locali.

"Scopri di più sulla BlueXP ransomware protection e sulle origini dati supportate, sulle destinazioni di backup e sugli ambienti di lavoro" .

Controllo degli accessi basato sui ruoli

Ora puoi limitare l'accesso ad attività specifiche con il controllo degli accessi basato sui ruoli (RBAC). La BlueXP ransomware protection utilizza due ruoli di BlueXP: amministratore dell'account BlueXP e amministratore senza account (visualizzatore).

Per i dettagli sulle azioni che ogni ruolo può eseguire, vedere "Privilegi di controllo degli accessi basati sui ruoli" .

5 agosto 2024

Rilevamento delle minacce con Splunk Cloud

È possibile inviare automaticamente i dati al sistema di gestione della sicurezza e degli eventi (SIEM) per l'analisi e il rilevamento delle minacce. Nelle versioni precedenti era possibile selezionare solo AWS Security Hub come SIEM. Con questa versione, puoi selezionare AWS Security Hub o Splunk Cloud come SIEM.

"Scopri di più sulla configurazione delle impostazioni BlueXP ransomware protection" .

1 luglio 2024

Porta la tua licenza (BYOL)

Con questa versione, puoi utilizzare una licenza BYOL, ovvero un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante commerciale NetApp .

"Scopri di più sulla configurazione delle licenze" .

Ripristinare il carico di lavoro dell'applicazione a livello di file

Prima di ripristinare il carico di lavoro di un'applicazione a livello di file, ora puoi visualizzare un elenco dei file che potrebbero essere stati interessati da un attacco e identificare quelli che desideri ripristinare. Puoi lasciare

che la BlueXP ransomware protection scelga i file da ripristinare, puoi caricare un file CSV che elenca tutti i file interessati da un avviso oppure puoi identificare manualmente i file che desideri ripristinare.

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

"Scopri di più sul recupero da un attacco ransomware" .

Scarica un elenco dei file interessati

Prima di ripristinare un carico di lavoro dell'applicazione a livello di file, è ora possibile accedere alla pagina Avvisi per scaricare un elenco dei file interessati in un file CSV e quindi utilizzare la pagina Ripristino per caricare il file CSV.

"Scopri di più sul download dei file interessati prima di ripristinare un'applicazione" .

Elimina piano di protezione

Con questa versione è ora possibile eliminare una strategia di protezione dal ransomware.

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

10 giugno 2024

Blocco della copia snapshot sullo storage primario

Abilita questa opzione per bloccare le copie snapshot sull'archiviazione primaria in modo che non possano essere modificate o eliminate per un determinato periodo di tempo, anche se un attacco ransomware riesce a raggiungere la destinazione dell'archiviazione di backup.

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

Supporto per Cloud Volumes ONTAP per Microsoft Azure

Questa versione supporta Cloud Volumes ONTAP per Microsoft Azure come sistema, oltre a Cloud Volumes ONTAP per AWS e ONTAP NAS locale.

"Avvio rapido per Cloud Volumes ONTAP in Azure"

"Scopri di più sulla BlueXP ransomware protection" .

Microsoft Azure aggiunto come destinazione di backup

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

"Scopri di più su come configurare le impostazioni di protezione" .

14 maggio 2024

Aggiornamenti sulle licenze

Puoi registrarti per una prova gratuita di 90 giorni. Presto potrai acquistare un abbonamento pay-as-you-go con Amazon Web Services Marketplace oppure portare la tua licenza NetApp .

"Scopri di più sulla configurazione delle licenze" .

protocollo CIFS

Il servizio ora supporta ONTAP on-premise e Cloud Volumes ONTAP nei sistemi AWS utilizzando i protocolli NFS e CIFS. La versione precedente supportava solo il protocollo NFS.

Dettagli del carico di lavoro

Questa versione fornisce ora maggiori dettagli nelle informazioni sul carico di lavoro dalle pagine Protezione e altre pagine per una migliore valutazione della protezione del carico di lavoro. Dai dettagli del carico di lavoro è possibile esaminare la policy attualmente assegnata e le destinazioni di backup configurate.

"Scopri di più sulla visualizzazione dei dettagli del carico di lavoro nelle pagine Protezione" .

Protezione e ripristino coerenti con l'applicazione e con la macchina virtuale

Ora puoi eseguire una protezione coerente con le applicazioni con il software NetApp SnapCenter e una protezione coerente con le VM con il SnapCenter Plug-in for VMware vSphere, ottenendo uno stato di quiescenza e coerenza per evitare potenziali perdite di dati in un secondo momento, se necessario un ripristino. Se è necessario un ripristino, è possibile ripristinare l'applicazione o la macchina virtuale a uno qualsiasi degli stati precedentemente disponibili.

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

Strategie di protezione dal ransomware

Se nel carico di lavoro non sono presenti policy di snapshot o backup, è possibile creare una strategia di protezione dal ransomware, che può includere le seguenti policy create in questo servizio:

- Politica di snapshot
- Politica di backup
- Politica di rilevamento

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

Rilevamento delle minacce

È ora possibile abilitare il rilevamento delle minacce tramite un sistema di gestione della sicurezza e degli eventi (SIEM) di terze parti. La Dashboard ora mostra una nuova raccomandazione per "Abilitare il rilevamento delle minacce", che può essere configurata nella pagina Impostazioni.

"Scopri di più sulla configurazione delle opzioni Impostazioni" .

Ignora gli avvisi di falsi positivi

Dalla scheda Avvisi, ora puoi ignorare i falsi positivi o decidere di recuperare immediatamente i tuoi dati.

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

Stato di rilevamento

Nella pagina Protezione vengono visualizzati nuovi stati di rilevamento che mostrano lo stato del rilevamento ransomware applicato al carico di lavoro.

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

Scarica i file CSV

È possibile scaricare i file CSV* dalle pagine Protezione, Avvisi e Ripristino.

"Scopri di più sul download di file CSV dalla Dashboard e da altre pagine" .

Link alla documentazione

Il collegamento alla documentazione è ora incluso nell'interfaccia utente. È possibile accedere a questa documentazione dalla verticale Dashboard **Azioni***  **opzione. Selezionare *Novità** per visualizzare i dettagli nelle Note di rilascio o **Documentazione** per visualizzare la pagina iniziale della documentazione BlueXP ransomware protection .

BlueXP backup and recovery

Non è più necessario che il servizio BlueXP backup and recovery sia già abilitato sul sistema. Vedere "prerequisiti" . Il servizio BlueXP ransomware protection aiuta a configurare una destinazione di backup tramite l'opzione Impostazioni. Vedere "Configurare le impostazioni" .

Opzione Impostazioni

Ora puoi impostare le destinazioni di backup nelle impostazioni BlueXP ransomware protection .

"Scopri di più sulla configurazione delle opzioni Impostazioni" .

5 marzo 2024

Gestione della politica di protezione

Oltre a utilizzare criteri predefiniti, ora è possibile creare criteri. "Scopri di più sulla gestione delle policy" .

Immutabilità su storage secondario (DataLock)

Ora è possibile rendere il backup immutabile nello storage secondario utilizzando la tecnologia NetApp DataLock nell'archivio oggetti. "Scopri di più sulla creazione di policy di protezione" .

Backup automatico su NetApp StorageGRID

Oltre a utilizzare AWS, ora puoi scegliere StorageGRID come destinazione di backup. "Scopri di più sulla configurazione delle destinazioni di backup" .

Funzionalità aggiuntive per indagare su potenziali attacchi

Ora è possibile visualizzare maggiori dettagli forensi per indagare sul potenziale attacco rilevato. "Scopri di più su come rispondere a un avviso di ransomware rilevato" .

Processo di recupero

Il processo di recupero è stato migliorato. Ora è possibile recuperare volume per volume o tutti i volumi di un carico di lavoro. "Scopri di più sul ripristino da un attacco ransomware (dopo che gli incidenti sono stati neutralizzati)" .

"Scopri di più sulla BlueXP ransomware protection" .

6 ottobre 2023

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

Nella versione di anteprima, il servizio protegge i carichi di lavoro basati sulle applicazioni di Oracle, i datastore delle VM e le condivisioni di file su storage NAS locale, nonché Cloud Volumes ONTAP su AWS (utilizzando il protocollo NFS) nelle singole organizzazioni BlueXP ed esegue il backup dei dati sullo storage cloud di Amazon Web Services.

Il servizio BlueXP ransomware protection sfrutta appieno diverse tecnologie NetApp , consentendo all'amministratore della sicurezza dei dati o al responsabile delle operazioni di sicurezza di raggiungere i seguenti obiettivi:

- Visualizza a colpo d'occhio la protezione ransomware su tutti i tuoi carichi di lavoro.
- Ottieni informazioni sulle raccomandazioni per la protezione dal ransomware
- Migliorare la postura di protezione in base alle raccomandazioni BlueXP ransomware protection .
- Assegna policy di protezione dal ransomware per proteggere i tuoi carichi di lavoro più importanti e i dati ad alto rischio dagli attacchi ransomware.
- Monitora lo stato dei tuoi carichi di lavoro contro gli attacchi ransomware alla ricerca di anomalie nei dati.
- Valuta rapidamente l'impatto degli incidenti ransomware sul tuo carico di lavoro.
- Ripristina in modo intelligente i dati in seguito a un attacco ransomware, assicurandoti che non si verifichi una nuova infezione dei dati archiviati.

"Scopri di più sulla BlueXP ransomware protection" .

Limitazioni note di NetApp Ransomware Resilience

Le limitazioni note identificano piattaforme, dispositivi o funzioni che non sono supportati da questa versione del prodotto o che non interagiscono correttamente con esso. Esamina attentamente queste limitazioni.

Problema con l'opzione di ripristino dell'esercitazione di preparazione

Se si seleziona un volume ONTAP 9.11.1 per l'esercitazione di preparazione all'attacco ransomware, Ransomware Resilience invia un avviso. Se si ripristinano i dati utilizzando l'opzione "clone-to-volume" e si reimposta il drill, l'operazione di reimpostazione fallisce.

Limitazioni Amazon FSx for NetApp ONTAP

Il sistema Amazon FSx for NetApp ONTAP è supportato in Ransomware Resilience. Ad Amazon FSx per ONTAP si applicano le seguenti limitazioni:

- Le policy di backup non sono supportate per Amazon FSx for ONTAP. In questo ambiente, è consigliabile eseguire le operazioni di backup utilizzando Amazon FSx . È possibile ripristinare questi carichi di lavoro utilizzando Ransomware Resilience.
- Le operazioni di ripristino vengono eseguite solo dagli snapshot.

Iniziare

Scopri di più sulla NetApp Ransomware Resilience

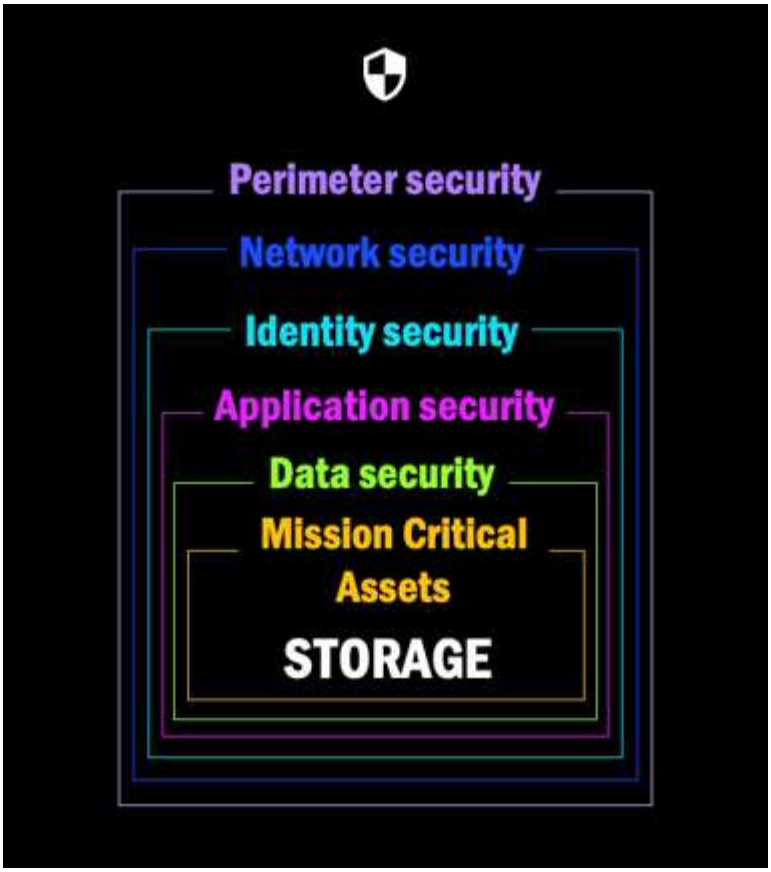
Gli attacchi ransomware possono bloccare l'accesso ai tuoi dati e gli aggressori possono chiedere un riscatto in cambio del rilascio dei dati o della decrittazione. Secondo l'IDC, non è raro che le vittime di ransomware subiscano più attacchi ransomware. L'attacco può interrompere l'accesso ai tuoi dati per un periodo che può variare da un giorno a diverse settimane.

NetApp Ransomware Resilience protegge i tuoi dati dagli attacchi ransomware. In Ransomware Resilience, la protezione è disponibile per carichi di lavoro basati su applicazioni di Oracle, datastore VM e condivisioni di file su storage NAS locale (utilizzando i protocolli NFS e CIFS) e storage SAN (FC, iSCSI e NVMe), nonché Cloud Volumes ONTAP per Amazon Web Services, Cloud Volumes ONTAP per Google Cloud, Cloud Volumes ONTAP per Microsoft Azure e Amazon FSx for NetApp ONTAP nella NetApp Console. È possibile eseguire il backup dei dati su Amazon Web Services, Google Cloud, Microsoft Azure Cloud Storage e NetApp StorageGRID.

Resilienza del ransomware a livello di dati

In genere, la tua strategia di sicurezza prevede più livelli di difesa per proteggerti da una serie di minacce informatiche.

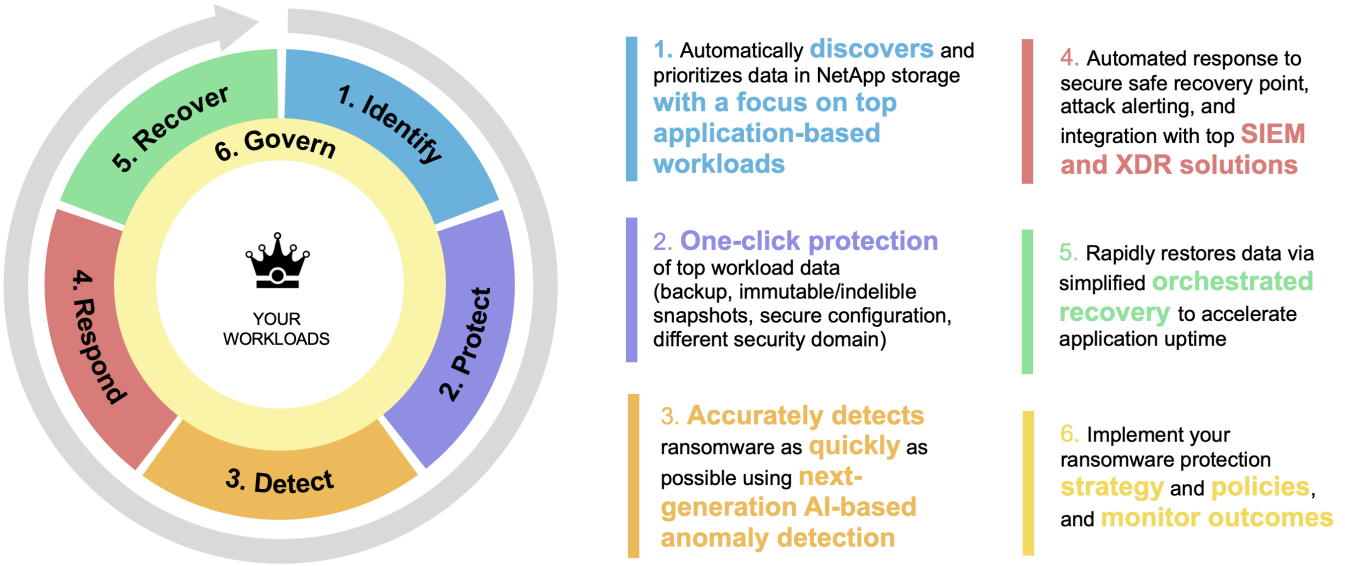
- **Strato più esterno**: questa è la prima linea di difesa che utilizza firewall, sistemi di rilevamento delle intrusioni e reti private virtuali per salvaguardare i confini della rete.
- **Sicurezza di rete**: questo livello si basa sulle fondamenta con segmentazione di rete, monitoraggio del traffico e crittografia.
- **Sicurezza dell'identità**: utilizza metodi di autenticazione, controlli di accesso e gestione dell'identità per garantire che solo gli utenti autorizzati possano accedere alle risorse sensibili.
- **Sicurezza delle applicazioni**: protegge le applicazioni software mediante pratiche di codifica sicura, test di sicurezza e autoprotezione delle applicazioni runtime.
- **Sicurezza dei dati**: salvaguarda i tuoi dati con strategie di protezione, backup e ripristino. La resilienza del ransomware opera su questo livello.



Cosa puoi fare con Ransomware Resilience

Ransomware Resilience consente di sfruttare appieno diverse tecnologie NetApp , in modo che l'amministratore dell'archiviazione, l'amministratore della sicurezza dei dati o il tecnico delle operazioni di sicurezza possano raggiungere i seguenti obiettivi:

- **Identifica** tutti i carichi di lavoro basati su applicazioni, condivisioni di file o gestiti da VMware nei sistemi NAS (NFS o CIFS) e SAN (FC, iSCSI e NVMe) locali NetApp nella NetApp Console, nei progetti e negli agenti della console. Ransomware Resilience categorizza la priorità dei dati e fornisce suggerimenti per migliorare la resilienza al ransomware.
- **Proteggi** i tuoi carichi di lavoro abilitando backup, copie snapshot e strategie di protezione dal ransomware sui tuoi dati.
- **Rileva** anomalie che potrebbero essere attacchi ransomware. [1]
- **Rispondi** ai potenziali attacchi ransomware avviando automaticamente uno snapshot point-in-time bloccato in modo che la copia non possa essere eliminata accidentalmente o intenzionalmente. I tuoi dati di backup rimarranno immutabili e protetti end-to-end dagli attacchi ransomware all'origine e nella destinazione.
- **Recupera** i tuoi carichi di lavoro che contribuiscono ad accelerare i tempi di attività dei carichi di lavoro orchestrando diverse tecnologie NetApp . È possibile scegliere di recuperare volumi specifici. Ransomware Resilience fornisce consigli sulle opzioni migliori.
- **Governare**: implementare la strategia di protezione dal ransomware e monitorarne i risultati.



Vantaggi dell'utilizzo della resilienza ransomware

Ransomware Resilience offre i seguenti vantaggi:

- Rileva i carichi di lavoro e le relative pianificazioni di snapshot e backup esistenti, classificandone l'importanza relativa.
- Valuta il tuo livello di protezione dal ransomware e lo visualizza in una dashboard di facile comprensione.
- Fornisce raccomandazioni sui passaggi successivi in base all'analisi della posizione di scoperta e protezione.
- Applica le raccomandazioni sulla protezione dei dati basate su AI/ML con accesso con un clic.
- Protegge i dati nei carichi di lavoro basati su applicazioni quali Oracle, datastore VMware e condivisioni di file.
- Rileva in tempo reale gli attacchi ransomware sui dati presenti sullo storage primario utilizzando la tecnologia AI.
- Avvia azioni automatizzate in risposta ai potenziali attacchi rilevati creando copie snapshot e inviando avvisi su attività anomale.
- Applica un ripristino curato per soddisfare i criteri RPO. Ransomware Resilience orchestra il ripristino dagli incidenti ransomware utilizzando diversi servizi di ripristino NetApp , tra cui NetApp Backup and Recovery (in precedenza Cloud Backup) e SnapCenter.
- Utilizza il controllo degli accessi basato sui ruoli (RBAC) per gestire l'accesso alle funzionalità e alle operazioni.

Costo

Puoi provare Ransomware Resilience con una prova gratuita di 30 giorni. NetApp non addebita alcun costo per l'utilizzo della versione di prova di Ransomware Resilience.

Se disponi sia di Backup and Recovery che di Ransomware Resilience, tutti i dati comuni protetti da entrambi i prodotti verranno fatturati solo da Ransomware Resilience.

Dopo aver acquistato una licenza o un abbonamento PayGo, qualsiasi carico di lavoro che abbia un criterio di rilevamento ransomware (Autonomous Ransomware Protection) abilitato (rilevato o impostato da Ransomware

Resilience) e almeno uno snapshot o un criterio di backup, Ransomware Resilience lo classifica come "Protetto" e lo conta nella capacità acquistata o nell'abbonamento PayGo. Se un carico di lavoro viene scoperto senza una policy di rilevamento, anche se dispone di policy di backup o snapshot, viene classificato come "A rischio" e *non* viene conteggiato nella capacità acquistata.

I carichi di lavoro protetti vengono conteggiati nella capacità acquistata o nell'abbonamento al termine del periodo di prova di 90 giorni. La tariffazione di Ransomware Resilience viene calcolata in base ai GB di dati associati ai carichi di lavoro protetti prima delle efficienze.

Licenza

Con Ransomware Resilience puoi utilizzare diversi piani di licenza, tra cui una prova gratuita, un abbonamento a consumo o la possibilità di utilizzare la tua licenza.

Per utilizzare Ransomware Resilience è necessaria una licenza NetApp ONTAP One.

La licenza Ransomware Resilience non include prodotti NetApp aggiuntivi. Ransomware Resilience può utilizzare Backup e Recovery anche se non si dispone di una licenza per utilizzarlo.

Per rilevare comportamenti anomali degli utenti, Ransomware Resilience utilizza NetApp Autonomous Ransomware Protection, un modello di apprendimento automatico (ML) all'interno di ONTAP che rileva attività di file dannosi. Questo modello è incluso nella licenza Ransomware Resilience.

Per maggiori dettagli, vedere "Impostare la licenza" .

NetApp Console

Ransomware Resilience è accessibile tramite la NetApp Console.

NetApp Console offre una gestione centralizzata dei servizi di storage e dati NetApp in ambienti on-premise e cloud di livello aziendale. La console è necessaria per accedere e utilizzare i servizi dati NetApp . In quanto interfaccia di gestione, consente di gestire numerose risorse di archiviazione da un'unica interfaccia. Gli amministratori della console possono controllare l'accesso allo storage e ai servizi per tutti i sistemi all'interno dell'azienda.

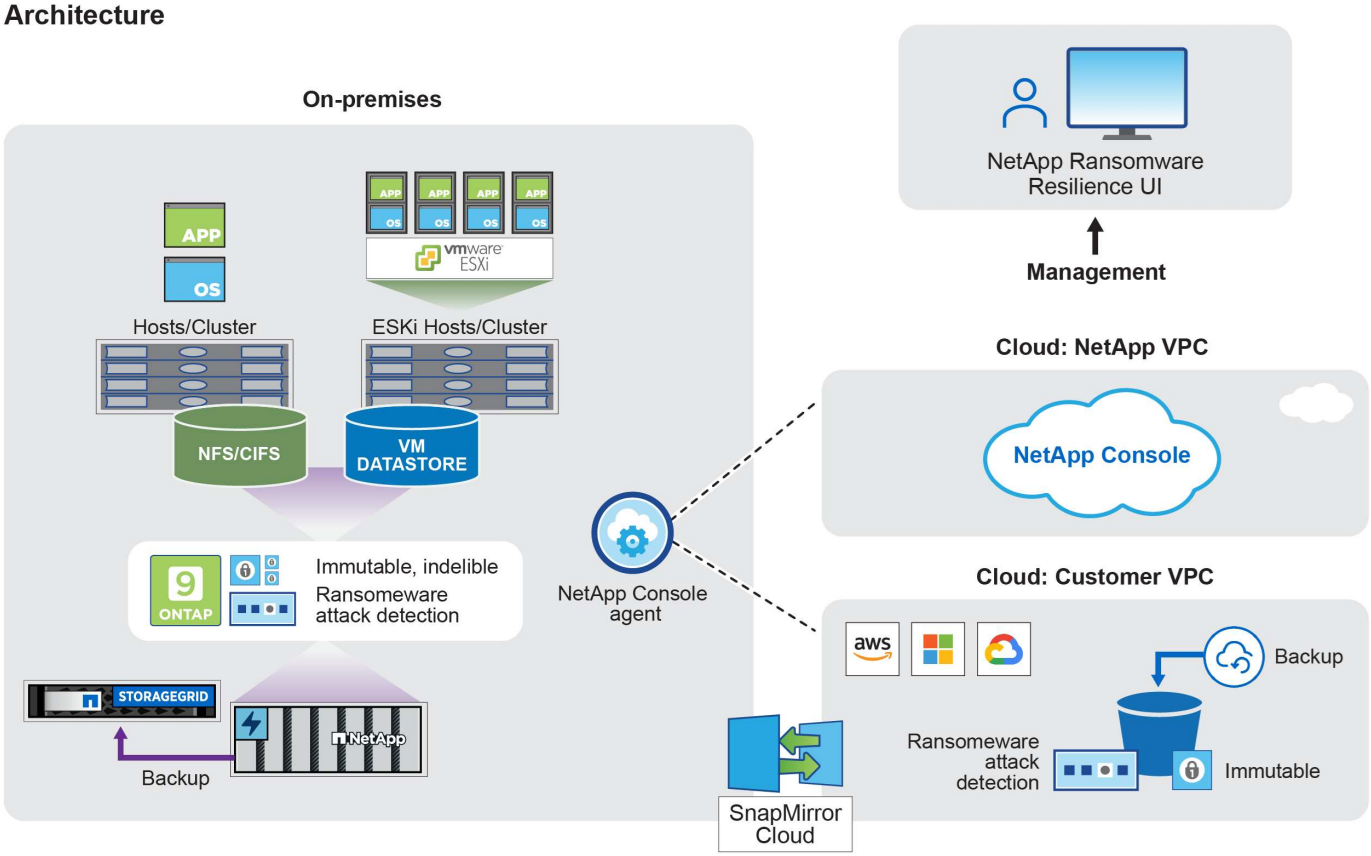
Non è necessaria una licenza o un abbonamento per iniziare a utilizzare NetApp Console e i costi saranno addebitati solo quando si distribuiscono agenti Console nel cloud per garantire la connettività ai sistemi di storage o ai servizi dati NetApp. Tuttavia, alcuni servizi dati NetApp accessibili dalla Console sono soggetti a licenza o abbonamento.

Scopri di più su"NetApp Console" .

Come funziona Ransomware Resilience

Ransomware Resilience utilizza NetApp Backup and Recovery per individuare e impostare policy di snapshot e backup per carichi di lavoro di condivisione file, e SnapCenter o SnapCenter for VMware per individuare e impostare policy di snapshot e backup per carichi di lavoro di applicazioni e VM. Inoltre, Ransomware Resilience utilizza Backup and Recovery e SnapCenter / SnapCenter per VMware per eseguire un ripristino coerente con i file e i carichi di lavoro.

Architecture



Caratteristica	Descrizione
IDENTIFICARE	• Trova tutti i dati NAS (protocolli NFS e CIFS) on-premise del cliente, SAN (FC, iSCSI e NVMe) e Cloud Volumes ONTAP connessi alla console. • Identifica i dati dei clienti dalle API dei servizi ONTAP e SnapCenter e li associa ai carichi di lavoro. Scopri di più su "ONTAP" E "Software SnapCenter" . • Rileva il livello di protezione attuale di ogni volume delle copie snapshot NetApp e delle policy di backup, nonché tutte le funzionalità di rilevamento integrate. Ransomware Resilience associa quindi questa posizione di protezione ai carichi di lavoro utilizzando Backup e Recovery, servizi ONTAP e tecnologie NetApp come Autonomous Ransomware Protection (ARP o ARP/AI a seconda della versione ONTAP), FPolicy, policy di backup e policy di snapshot. Scopri di più su "Protezione autonoma dal ransomware" , "NetApp Backup and Recovery" , E "Politica ONTAP" . • Assegna una priorità aziendale a ciascun carico di lavoro in base ai livelli di protezione rilevati automaticamente e consiglia policy di protezione per i carichi di lavoro in base alla loro priorità aziendale. La priorità del carico di lavoro si basa sulle frequenze degli snapshot già applicate a ciascun volume associato al carico di lavoro.
PROTEGGERE	• Monitora attivamente i carichi di lavoro e orchestra l'uso delle API Backup and Recovery, SnapCenter e ONTAP applicando policy a ciascuno dei carichi di lavoro identificati.

Caratteristica	Descrizione
RILEVARE	• Rileva potenziali attacchi con un modello di apprendimento automatico (ML) integrato che rileva attività e crittografia potenzialmente anomale. • Fornisce un rilevamento a doppio livello che inizia con il rilevamento di potenziali attacchi ransomware nello storage primario e risponde alle attività anomale eseguendo copie snapshot automatizzate aggiuntive per creare i punti di ripristino dei dati più vicini. Ransomware Resilience offre la possibilità di analizzare più a fondo la situazione per identificare potenziali attacchi con maggiore precisione, senza compromettere le prestazioni dei carichi di lavoro principali. • Determina i file sospetti specifici e associa gli attacchi ai carichi di lavoro associati, utilizzando le tecnologie ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI a seconda della versione ONTAP) e FPolicy.
RISPONDERE	• Mostra dati rilevanti, come l'attività dei file, l'attività degli utenti e l'entropia, per aiutarti a completare le revisioni forensi sull'attacco. • Avvia copie snapshot rapide utilizzando tecnologie e prodotti NetApp quali ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI a seconda della versione ONTAP) e FPolicy.
RECUPERARE	• Determina lo snapshot o il backup migliore e consiglia il miglior punto di ripristino effettivo (RPA) utilizzando le tecnologie e i servizi Backup and Recovery, ONTAP, Autonomous Ransomware Protection (ARP o ARP/AI a seconda della versione ONTAP) e FPolicy. • Orchestra il ripristino dei carichi di lavoro, tra cui macchine virtuali, condivisioni di file, storage a blocchi e database, garantendo la coerenza delle applicazioni.
GOVERNARE	• Assegna le strategie di protezione dal ransomware • Ti aiuta a monitorare i risultati.

Destinazioni di backup, sistemi e origini dati del carico di lavoro supportati

Ransomware Resilience supporta i seguenti obiettivi di backup, sistemi e origini dati:

Destinazioni di backup supportate

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

Sistemi supportati

Ambiente	Protocollo	Versioni supportate
Amazon FSx for NetApp ONTAP*	NFS, CIFS e SAN	N / A

Ambiente	Protocollo	Versioni supportate
Cloud Volumes ONTAP per AWS	CIFS e NFS	9.11.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive
Cloud Volumes ONTAP per Google Cloud Platform	CIFS e NFS	9.11.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive
Cloud Volumes ONTAP per Microsoft Azure	CIFS e NFS	9.12.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive
ONTAP (in sede)	CIFS e NFS	9.11.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive

{asterisco} Amazon FSx for NetApp ONTAP utilizza Autonomous Ransomware Protection (ARP) e non ARP/AI. Per maggiori informazioni sulla differenza, vedere"ARP/IA" .

> Per utilizzare ARP/AI in ONTAP è necessario ONTAP 9.16 o versione successiva. + ONTAP non fornisce supporto per la protezione ransomware per FabricPool FlexCache, volumi FlexGroup , volumi di punti di montaggio di gruppi di coerenza, volumi di percorsi di montaggio, volumi offline e volumi di protezione dati (DP). Assicurati di rivedere"configurazioni supportate e non supportate in ONTAP" .

Origini dati del carico di lavoro supportate

Ransomware Resilience protegge i seguenti carichi di lavoro basati su applicazioni su volumi di dati primari:

- Archiviazione a blocchi
- Banche dati:
  - Microsoft SQL Server
  - Oracolo
  - PostgreSQL
- Condivisioni file NetApp
- Datastore VMware

Se utilizzi SnapCenter o SnapCenter per VMware, tutti i carichi di lavoro supportati da tali prodotti sono identificati anche in Ransomware Resilience. Ransomware Resilience è in grado di proteggerli e ripristinarli in modo coerente con il carico di lavoro.

Termini chiave

Potrebbe essere utile comprendere la terminologia relativa alla protezione dal ransomware.

- **Protezione**: la protezione nella resilienza del ransomware significa garantire che gli 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 in Ransomware Resilience può includere database Oracle, datastore VMware o condivisioni di file.

Prerequisiti per la NetApp Ransomware Resilience

Inizia a usare NetApp Ransomware Resilience verificando la preparazione del tuo ambiente operativo, dell'accesso alla rete e del browser web.

Per utilizzare Ransomware Resilience, assicurati di soddisfare i prerequisiti.

Sistemi supportati

Assicurati di utilizzare un sistema supportato:

Ambiente	Protocollo	Versioni supportate
Amazon FSx for NetApp ONTAP*	NFS, CIFS e SAN	N / A
Cloud Volumes ONTAP per AWS	CIFS e NFS	9.11.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive
Cloud Volumes ONTAP per Google Cloud Platform	CIFS e NFS	9.11.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive
Cloud Volumes ONTAP per Microsoft Azure	CIFS e NFS	9.12.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive
ONTAP (in sede)	CIFS e NFS	9.11.1 e versioni successive
	SAN (FC, iSCSI e NVMe)	9.17.1 e versioni successive

{asterisco} Amazon FSx for NetApp ONTAP utilizza Autonomous Ransomware Protection (ARP) e non ARP/AI. Per maggiori informazioni sulla differenza, vedere"ARP/IA" .

Requisiti NetApp Console

La configurazione NetApp Console richiede:

- Un account utente NetApp Console con privilegi di amministratore dell'organizzazione per l'individuazione delle risorse.
- Un'organizzazione e un sistema di console con almeno un agente di console attivo che si connette a un"sistema supportato" .
  - Se i cluster ONTAP locali o Cloud Volumes ONTAP in AWS o nel cloud di Azure non sono configurati nella Console, vedere"Scopri come configurare un agente Console" E"requisiti standard della console" .

> Se sono presenti più agenti Console in un'unica organizzazione Console, Ransomware Resilience analizzerà le risorse ONTAP su tutti gli agenti Console, a parte quello attualmente selezionato nell'interfaccia utente della Console.

- L'agente della console deve avere `cloudmanager-ransomware-protection` contenitore in stato attivo.
- Almeno un sistema Console con un cluster ONTAP locale NetApp o Cloud Volumes ONTAP in AWS o Azure. Ransomware Resilience supporta sia i protocolli NAS (NFS e SMB) sia SAN (iSCSI, FC e NVMe).

- Ransomware Resilience è supportato con i cluster ONTAP o Cloud Volumes ONTAP con ONTAP versione 9.11.1 o successiva.

> Per utilizzare Ransomware Resilience sui carichi di lavoro SAN, è necessario eseguire ONTAP 9.17.1 o versione successiva.

Requisiti ONTAP

- È necessario eseguire ONTAP 9.11.1 o versione successiva con una licenza ONTAP One abilitata sull'istanza ONTAP locale. Per ulteriori informazioni sul supporto ONTAP , vedere"Panoramica sulla protezione autonoma dal ransomware" .
- Per applicare le configurazioni di protezione (ad esempio, abilitando la protezione autonoma contro i ransomware), Ransomware Resilience necessita delle autorizzazioni di amministratore sul cluster ONTAP . Il cluster ONTAP avrebbe dovuto essere integrato utilizzando solo le credenziali utente amministratore del cluster ONTAP .

> Se hai connesso un cluster ONTAP alla Console con credenziali non amministrative, [devi aggiornare le credenziali nel cluster ONTAP](#update-non-admin-user-permissions-in-an-ontap-system).

Backup dei dati

- Un account in NetApp StorageGRID, AWS S3, Azure Blob o Google Cloud Platform per le destinazioni di backup con autorizzazioni di accesso appropriate configurate.

  Fare riferimento al "Elenco delle autorizzazioni AWS, Azure o S3" per i dettagli.

- Non è necessario abilitare NetApp Backup and Recovery sul sistema.

  Ransomware Resilience aiuta a configurare una destinazione di backup tramite l'opzione Impostazioni. Vedere "Configurare le impostazioni" .

Requisiti relativi al comportamento sospetto dell'utente

Affinché Ransomware Resilience fornisca avvisi su comportamenti sospetti degli utenti, è necessario configurare un agente di attività utente. Per installare un agente di attività utente, assicurarsi che il sistema soddisfi "i requisiti".

Aggiornare le autorizzazioni degli utenti non amministratori in un sistema ONTAP

Se è necessario aggiornare le autorizzazioni degli utenti non amministratori per un particolare sistema, utilizzare questi passaggi della procedura.

1. Accedi alla Console. Nella dashboard, identifica il sistema che necessita di aggiornare le autorizzazioni utente ONTAP.
2. Seleziona il sistema per visualizzarne i dettagli.
3. Selezionare **Visualizza informazioni aggiuntive** per visualizzare il nome utente.
4. Accedere alla CLI del cluster ONTAP come utente amministratore.
5. Visualizza i ruoli esistenti per quell'utente:

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

6. Cambia il ruolo dell'utente. Inserisci:

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

7. Torna alla NetApp Console per utilizzare Ransomware Resilience.

Avvio rapido per NetApp Ransomware Resilience

Scopri i passaggi principali da seguire per impostare la Ransomware Resilience e proteggere i tuoi carichi di lavoro.

Per informazioni dettagliate, seguire i link presenti in ogni passaggio.

Rivedere i prerequisiti

Per queste attività è richiesto il ruolo di *Amministratore della console*.

- "Assicurati di aver installato un agente Console"
- "Assicurati che il tuo sistema soddisfi i requisiti"
- "Esaminare i ruoli utente di Ransomware Resilience e assegnare autorizzazioni agli utenti che accedono a Ransomware Resilience"
- "Impostare la licenza"

Inizia con Ransomware Resilience

Per queste attività è richiesto il ruolo di *amministratore di Ransomware Resilience*.

- "Scopri i carichi di lavoro nella Console"
- "Visualizza lo stato di protezione del carico di lavoro nella Dashboard"
- "Facoltativamente, eseguire un'esercitazione di preparazione all'attacco ransomware"

Configurare la protezione e il rilevamento in Ransomware Resilience

Per queste attività è richiesto il ruolo di *amministratore di Ransomware Resilience*. Per configurare attività di comportamento utente sospette è necessario il ruolo aggiuntivo *Ransomware Resilience user behavior admin*.

- "Proteggere i carichi di lavoro"
  - Facoltativamente,"migliorare la protezione configurando il rilevamento delle attività sospette degli utenti"

- Facoltativamente, configurare le destinazioni di backup:
  - "Preparare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform o Microsoft Azure come destinazione di backup" .
  - "Configurare le destinazioni di backup"
- "Rispondere al rilevamento di potenziali attacchi ransomware"
- "Recuperare da un attacco (dopo che gli incidenti sono stati neutralizzati)"

4 **Cosa succederà adesso?**

Dopo aver configurato la protezione in Ransomware Resilience, ecco cosa potresti fare.

- "Abilita la classificazione dei dati per identificare i rischi di governance e sicurezza"
- "Invia avvisi a SIEM"
- "Scarica report di allerta, protezione, esercitazione di prontezza, ripristino o riepilogo"

Imposta NetApp Ransomware Resilience

Puoi implementare facilmente NetApp Ransomware Resilience. Prima di iniziare, rivedere"prerequisiti" per garantire che il tuo ambiente sia pronto.

Preparare la destinazione del backup

Preparare una delle seguenti destinazioni di backup:

- NetApp StorageGRID
- Servizi Web Amazon
- Piattaforma Google Cloud
- Microsoft Azure

Dopo aver configurato le opzioni nella destinazione di backup stessa, in seguito la configurerai come destinazione di backup in Ransomware Resilience. Per i dettagli su come configurare la destinazione di backup in Ransomware Resilience, fare riferimento a"Configurare le destinazioni di backup" .

Preparare StorageGRID per diventare una destinazione di backup

Se si desidera utilizzare StorageGRID come destinazione di backup, fare riferimento a "Documentazione StorageGRID" per i dettagli su StorageGRID.

Preparare AWS a diventare una destinazione di backup

- Crea un account su AWS.
- Configurare "Autorizzazioni AWS" in AWS.

Per i dettagli sulla gestione dell'archiviazione AWS nella Console, fare riferimento a "Gestisci i tuoi bucket Amazon S3" .

Preparare Azure per diventare una destinazione di backup

- Configura un account in Azure.
- Configurare "Autorizzazioni di Azure" in Azzurro.

Per informazioni dettagliate sulla gestione dell'archiviazione di Azure nella console, fare riferimento a "Gestisci i tuoi account di archiviazione di Azure" .

Configurare la NetApp Console

Il passaggio successivo consiste nell'impostare la console e la resilienza del ransomware.

Revisione "Requisiti della console per la modalità standard" .

Creare un agente Console

Contatta il tuo rappresentante commerciale NetApp per provare o utilizzare questo servizio. Quindi, quando si utilizza l'agente Console, saranno incluse le funzionalità appropriate per Ransomware Resilience.

Per creare un agente Console utilizzando Ransomware Resilience, contattare l'amministratore dell'organizzazione Console che dispone delle autorizzazioni per creare agenti Console e fare riferimento alla documentazione che descrive "come creare un agente Console" .

> Se si dispone di più agenti della Console, Ransomware Resilience esegue la scansione dei dati su tutti gli agenti della Console, ad eccezione di quello attualmente visualizzato nella Console. Questo servizio rileva tutti i progetti e tutti gli agenti della console associati a questa organizzazione.

Accedi NetApp Ransomware Resilience

Accedi a NetApp Ransomware Resilience tramite la NetApp Console.

Per accedere alla Console, puoi utilizzare le credenziali del sito di supporto NetApp oppure registrarti per un accesso cloud NetApp utilizzando il tuo indirizzo email e una password. "Scopri di più sull'accesso" .

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

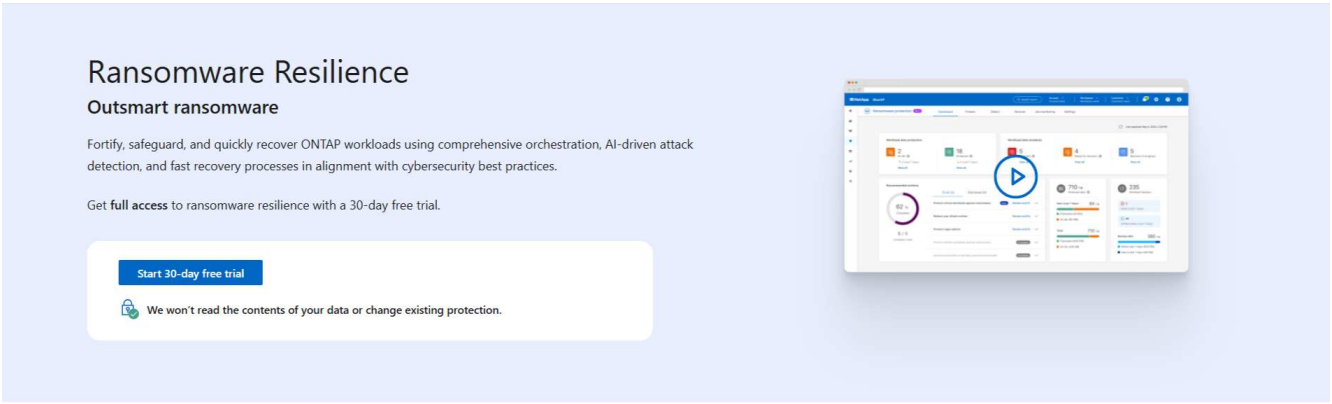
1. Apri un browser web e vai su"la console" .

   Viene visualizzata la pagina di accesso alla console.

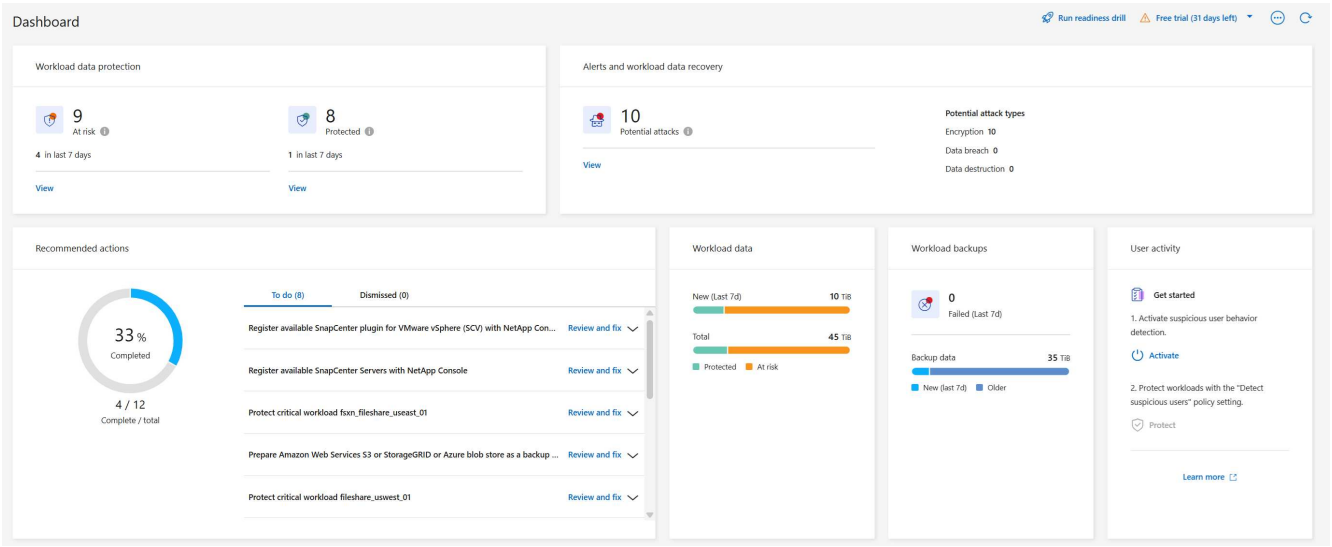
2. Accedi alla Console.
3. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.

   Se è la prima volta che accedi a questo servizio, verrà visualizzata la pagina di destinazione.

   > Se non si dispone di un agente Console o non è quello adatto a questo servizio, è necessario distribuirne uno. "Scopri come configurare un agente Console" .



In caso contrario, viene visualizzata la dashboard Ransomware Resilience.



4. Se non lo hai ancora fatto, seleziona l'opzione **Scopri carichi di lavoro**.

   Fare riferimento a "Scopri i carichi di lavoro" .

Imposta la licenza per NetApp Ransomware Resilience

Con NetApp Ransomware Resilience puoi utilizzare diversi piani di licenza.

Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, della cartella o del progetto. "Scopri di più sui ruoli di accesso alla console" .

Tipi di licenza

Ransomware Resilience è disponibile con i seguenti tipi di licenza:

- Prova gratuita di 30 giorni

- Acquista un abbonamento pay-as-you-go (PAYGO) con Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace o Azure Marketplace
- Bring your own license (BYOL): un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante commerciale NetApp . È possibile utilizzare il numero di serie della licenza per attivare BYOL nella Console.

Dopo aver impostato BYOL o acquistato un abbonamento PAYGO, puoi visualizzare la licenza nella sezione Licenses and subscriptions della Console.

Una volta terminato il periodo di prova gratuito o scaduta la licenza o l'abbonamento, puoi comunque:

- Visualizza i carichi di lavoro e lo stato di integrità dei carichi di lavoro
- Elimina risorse come le policy
- Esegui tutte le operazioni pianificate create durante il periodo di prova o sotto la licenza

Altre licenze

La licenza Ransomware Resilience non include prodotti NetApp aggiuntivi. Tuttavia, Ransomware Resilience può essere integrato con NetApp Backup and Recovery, anche se non si dispone di una licenza separata per Backup and Recovery.

Se disponi sia di Backup and Recovery che di Ransomware Resilience, tutti i dati comuni protetti da entrambi i prodotti verranno fatturati solo da Ransomware Resilience.

Prova Ransomware Resilience con una prova gratuita di 30 giorni

Puoi provare Ransomware Resilience con una prova gratuita di 30 giorni. Per iniziare la prova gratuita devi essere un amministratore dell'organizzazione della console.

Durante la prova non vengono applicati limiti alla capacità di archiviazione.

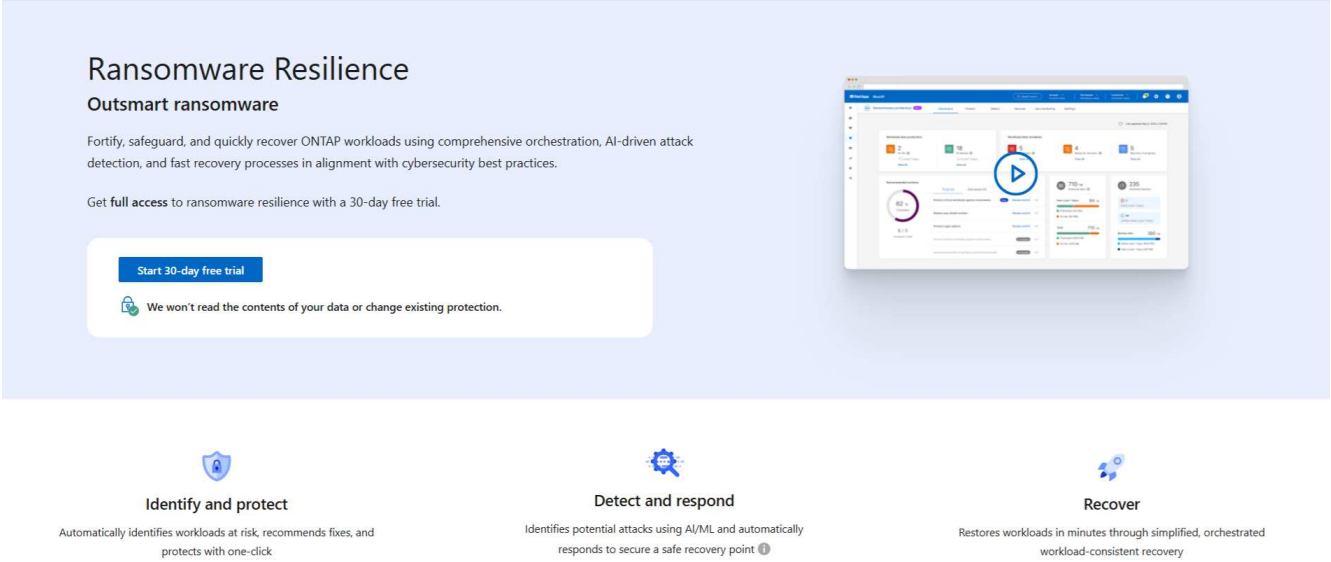
Puoi ottenere una licenza o abbonarti in qualsiasi momento e non ti verrà addebitato alcun costo fino al termine del periodo di prova di 30 giorni. Per continuare dopo il periodo di prova di 30 giorni, dovrai acquistare una licenza BYOL o un abbonamento PAYGO.

Durante la prova avrai piena funzionalità.

Passi

1. Accedi al "Consolle" .
2. Accedi alla Console.
3. Dalla NetApp Console, seleziona **Protezione** > **Ransomware Resilience**.

   Se è la prima volta che accedi a questo servizio, verrà visualizzata la pagina di destinazione.



4. Se non hai ancora aggiunto un agente Console per altri servizi,"aggiungine uno" .
5. Nella landing page di Ransomware Resilience, seleziona **Inizia individuando i carichi di lavoro** per individuare i tuoi carichi di lavoro.

   Questa opzione è disponibile solo se hai installato correttamente un agente Console.

6. Per rivedere le informazioni sulla prova gratuita, seleziona l'opzione a discesa in alto a destra.

Al termine del periodo di prova, ottieni un abbonamento o una licenza

Al termine del periodo di prova gratuito, puoi abbonarti tramite uno dei Marketplace oppure acquistare una licenza da NetApp.

Se hai già un abbonamento PAYGO, la licenza verrà automaticamente trasferita all'abbonamento al termine del periodo di prova gratuito.

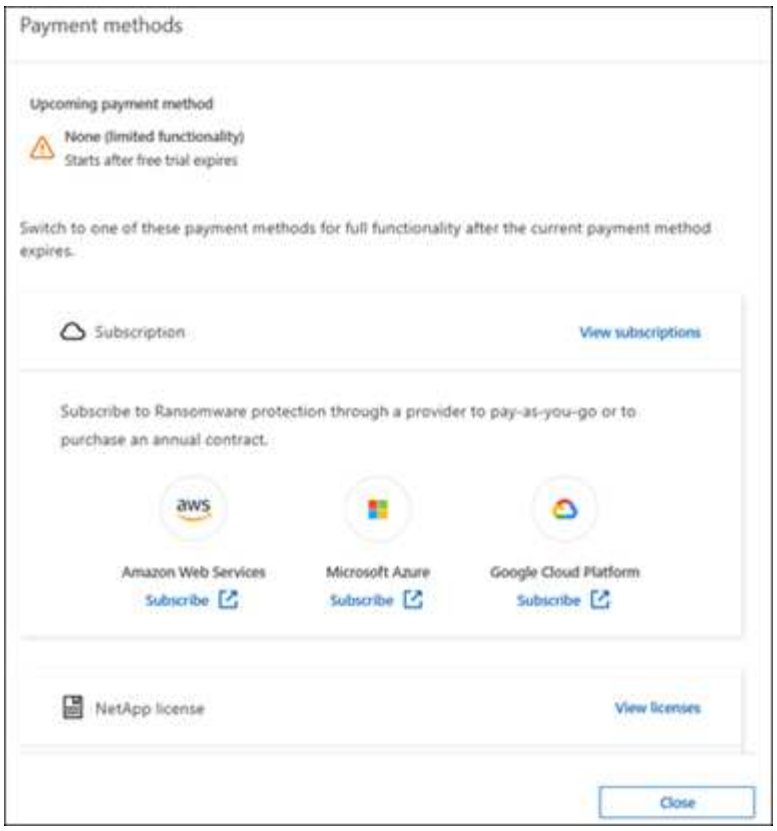
Iscriviti tramite AWS Marketplace Iscriviti tramite Microsoft Azure Marketplace Iscriviti tramite Google Cloud Platform Marketplace Porta la tua licenza (BYOL)

Iscriviti tramite AWS Marketplace

Questa procedura fornisce una panoramica di alto livello su come abbonarsi direttamente ad AWS Marketplace.

Passi

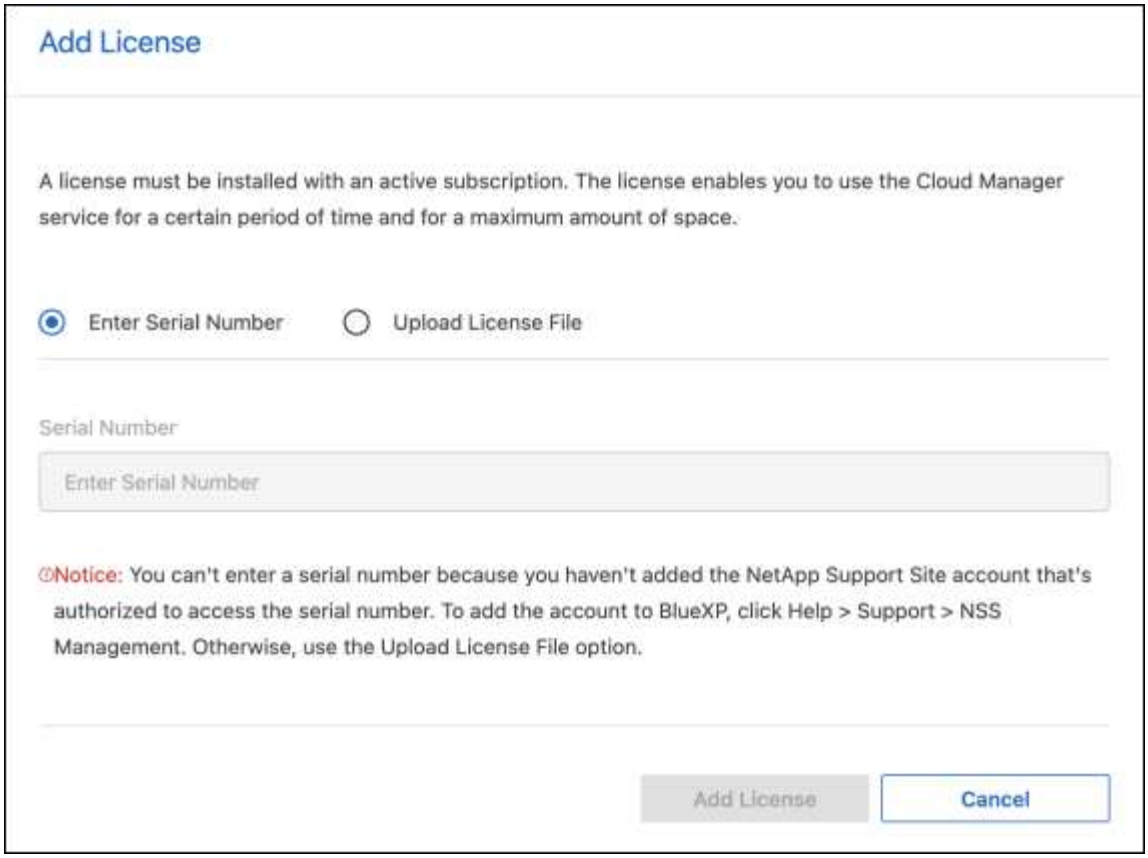
1. In Ransomware Resilience, esegui una delle seguenti operazioni:
   - Se ricevi un messaggio che indica che la prova gratuita sta per scadere, seleziona **Visualizza metodi di pagamento**.
   - Se non hai ancora iniziato la prova, seleziona l'avviso **Prova gratuita** in alto a destra, quindi **Visualizza metodi di pagamento**.



2. Nella pagina Metodi di pagamento, seleziona **Iscriviti** per **Amazon Web Services**.
3. In AWS Marketplace, seleziona **Visualizza opzioni di acquisto**.
4. Utilizza AWS Marketplace per abbonarti a * NetApp Intelligent Services* e **Ransomware Resilience**.
5. Quando torni a Ransomware Resilience, un messaggio ti informa che sei iscritto.

> Ti verrà inviata un'e-mail contenente il numero di serie di Ransomware Resilience e che indica che Ransomware Resilience è abbonato ad AWS Marketplace.

6. Torna alla pagina dei metodi di pagamento di Ransomware Resilience.
7. Aggiungere la licenza alla Console selezionando **Aggiungi licenza**.



8. Nella pagina Aggiungi licenza, seleziona **Inserisci numero di serie**, inserisci il numero di serie incluso nell'e-mail che ti è stata inviata, quindi seleziona **Aggiungi licenza**.
9. Per visualizzare i dettagli della licenza, dal menu di navigazione a sinistra della Console, selezionare **Amministrazione** > * Licenses and subscriptions*.
   - Per visualizzare le informazioni sull'abbonamento, seleziona **Abbonamenti**.
   - Per visualizzare le licenze BYOL, selezionare **Licenze servizi dati**.
10. Ritorno alla resilienza del ransomware. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.

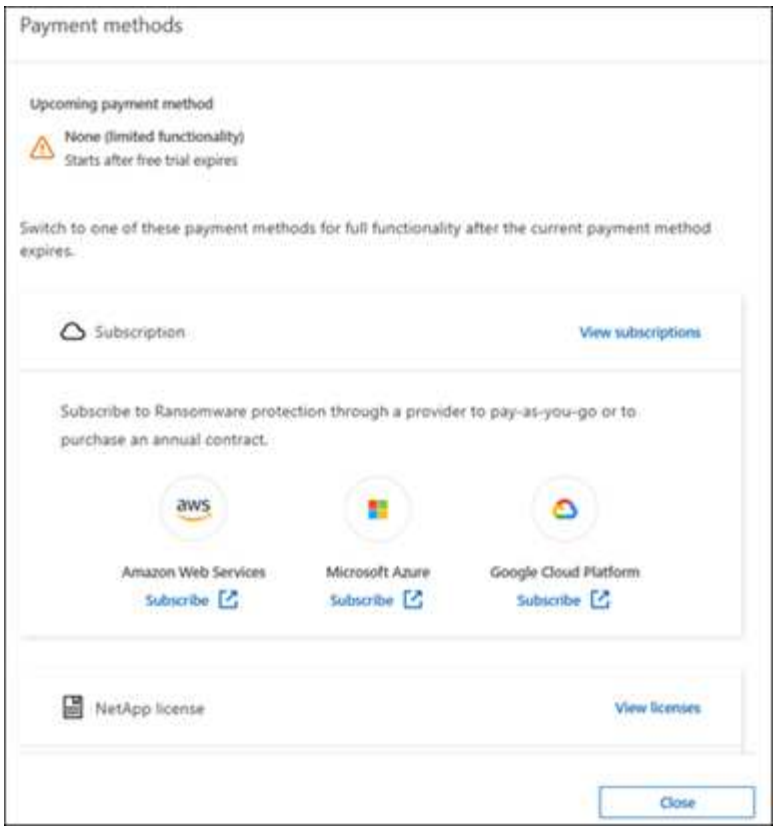
    Un messaggio conferma che è stata aggiunta una licenza.

Iscriviti tramite Microsoft Azure Marketplace

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

Passi

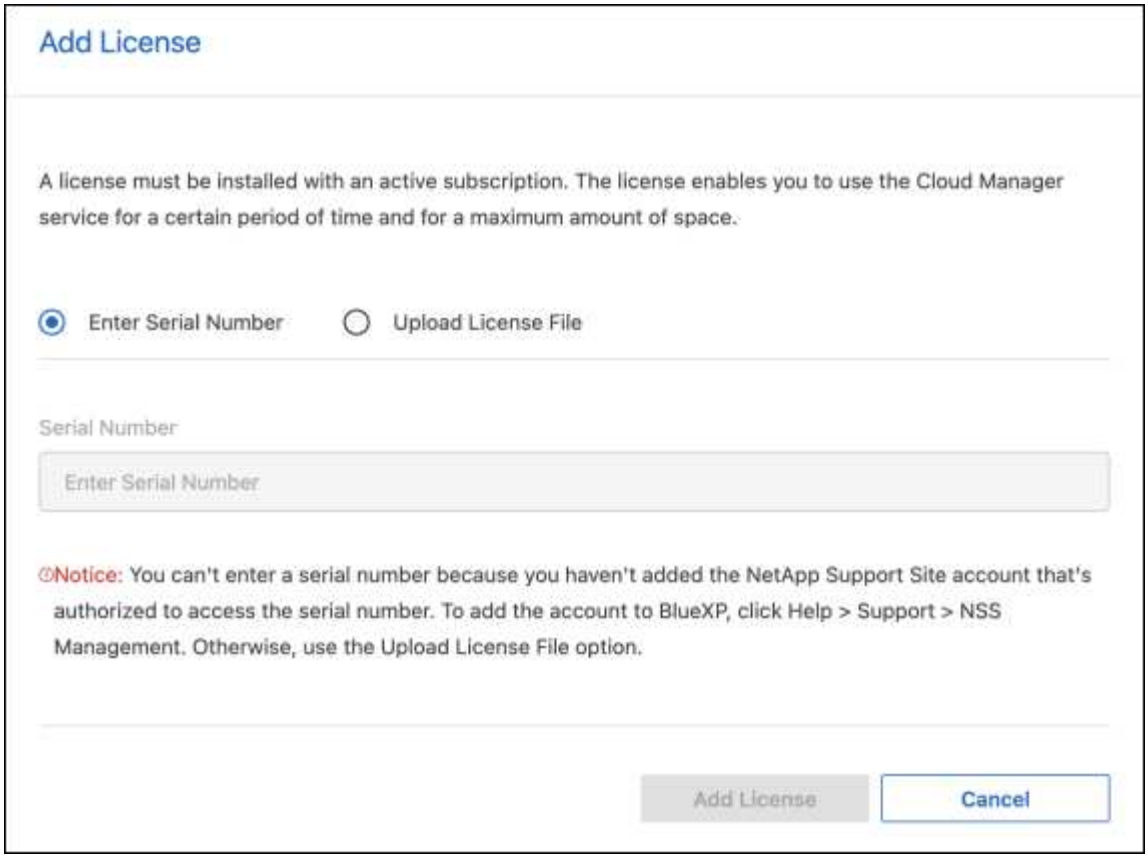
1. In Ransomware Resilience, esegui una delle seguenti operazioni:
   - Se ricevi un messaggio che indica che la prova gratuita sta per scadere, seleziona **Visualizza metodi di pagamento**.
   - Se non hai ancora iniziato la prova, seleziona l'avviso **Prova gratuita** in alto a destra, quindi **Visualizza metodi di pagamento**.



2. Nella pagina Metodi di pagamento, seleziona **Iscriviti** per **Microsoft Azure Marketplace**.
3. In Azure Marketplace, seleziona **Visualizza opzioni di acquisto**.
4. Utilizza Azure Marketplace per abbonarti a * NetApp Intelligent Services* e **Ransomware Resilience**.
5. Quando torni a Ransomware Resilience, un messaggio ti informa che sei iscritto.

> Ti verrà inviata un'e-mail contenente il numero di serie di Ransomware Resilience e che indica che Ransomware Resilience è abbonato ad Azure Marketplace.

6. Torna alla pagina dei metodi di pagamento di Ransomware Resilience.
7. Per aggiungere la licenza, seleziona **Aggiungi una licenza**.



8. Nella pagina Aggiungi licenza, seleziona **Inserisci numero di serie**, quindi inserisci il numero di serie che hai ricevuto tramite e-mail. Selezionare **Aggiungi licenza**.
9. Per visualizzare i dettagli della licenza in Licenses and subscriptions, dal menu di navigazione a sinistra della Console, selezionare **Governance** > * Licenses and subscriptions*.
   - Per visualizzare le informazioni sull'abbonamento, seleziona **Abbonamenti**.
   - Per visualizzare le licenze BYOL, selezionare **Licenze servizi dati**.
10. Ritorno alla resilienza del ransomware. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.

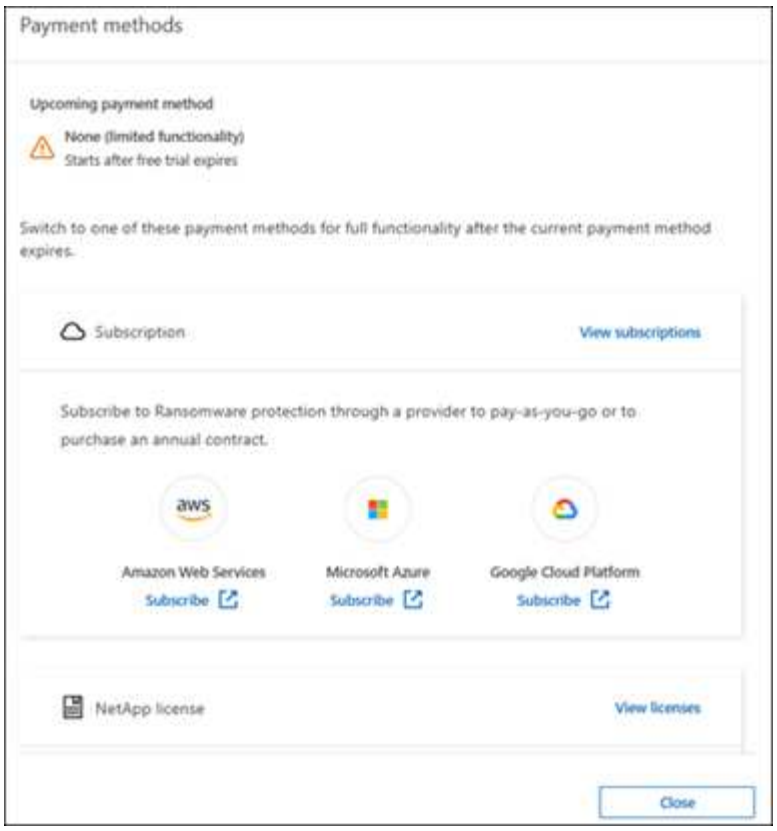
    Viene visualizzato un messaggio che indica che è stata aggiunta una licenza.

Iscriviti tramite Google Cloud Platform Marketplace

Questa procedura fornisce una panoramica di alto livello su come abbonarsi direttamente a Google Cloud Platform Marketplace.

Passi

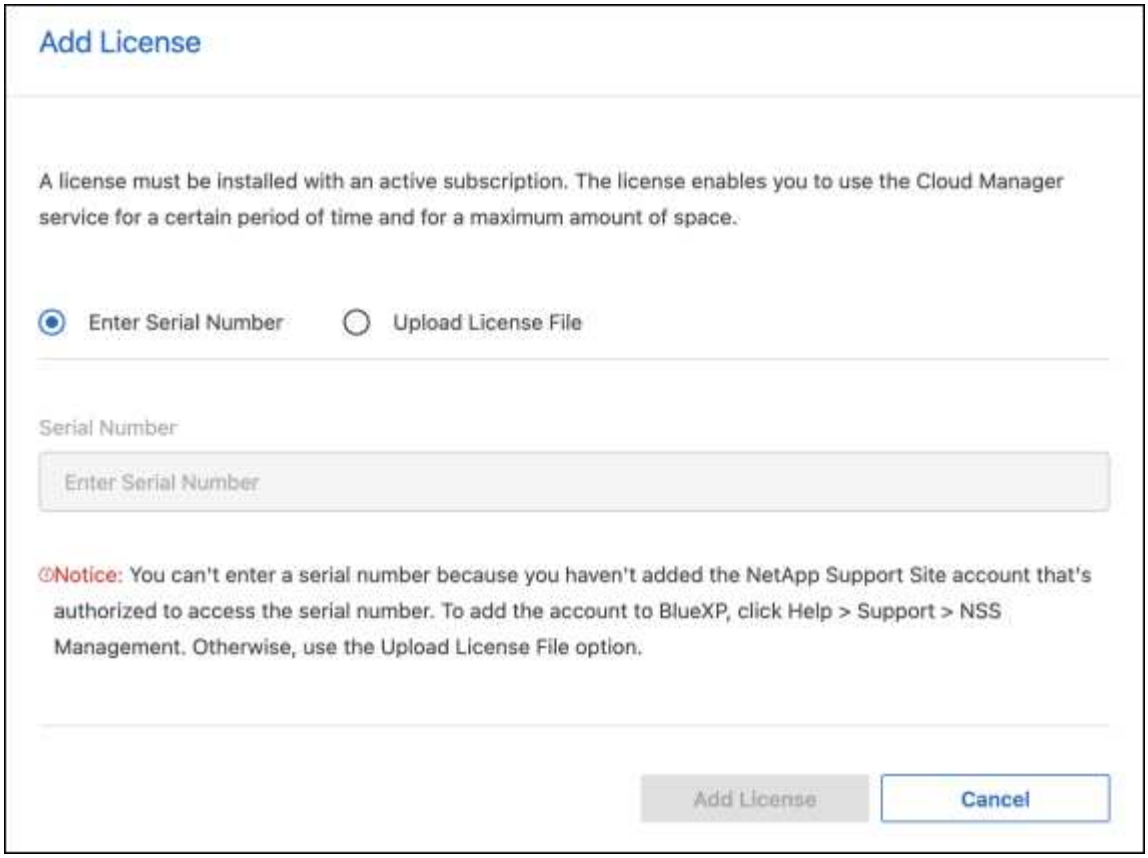
1. In Ransomware Resilience, esegui una delle seguenti operazioni:
   - Se ricevi un messaggio che indica che la prova gratuita sta per scadere, seleziona **Visualizza metodi di pagamento**.
   - Se non hai ancora iniziato la prova, seleziona l'avviso **Prova gratuita** in alto a destra, quindi **Visualizza metodi di pagamento**.



2. Nella pagina Metodi di pagamento, seleziona **Iscriviti** per Google Cloud Platform Marketplace*.
3. In Google Cloud Platform Marketplace, seleziona **Iscriviti**.
4. Utilizza Google Cloud Platform Marketplace per abbonarti a * NetApp Intelligent Services* e **Ransomware Resilience**.
5. Quando torni a Ransomware Resilience, un messaggio ti informa che sei iscritto.

> Ti verrà inviata un'e-mail contenente il numero di serie di Ransomware Resilience e che indica che Ransomware Resilience è abbonato a Google Cloud Platform Marketplace.

6. Torna alla pagina dei metodi di pagamento di Ransomware Resilience.
7. Per aggiungere la licenza alla Console, seleziona **Aggiungi licenza**.



8. Nella pagina Aggiungi licenza, seleziona **Inserisci numero di serie**. Inserisci il numero di serie che hai ricevuto via email. Selezionare **Aggiungi licenza**.
9. Per visualizzare i dettagli della licenza, dal menu di navigazione a sinistra della Console, selezionare **Governance** > * Licenses and subscriptions*.
   - Per visualizzare le informazioni sull'abbonamento, seleziona **Abbonamenti**.
   - Per visualizzare le licenze BYOL, selezionare **Licenze servizi dati**.
10. Ritorno alla resilienza del ransomware. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.

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

Porta la tua licenza (BYOL)

Se si desidera utilizzare la propria licenza (BYOL), è necessario acquistare la licenza, ottenere il file di licenza NetApp (NLF) e quindi aggiungere la licenza alla console.

Aggiungi il tuo file di licenza alla Console

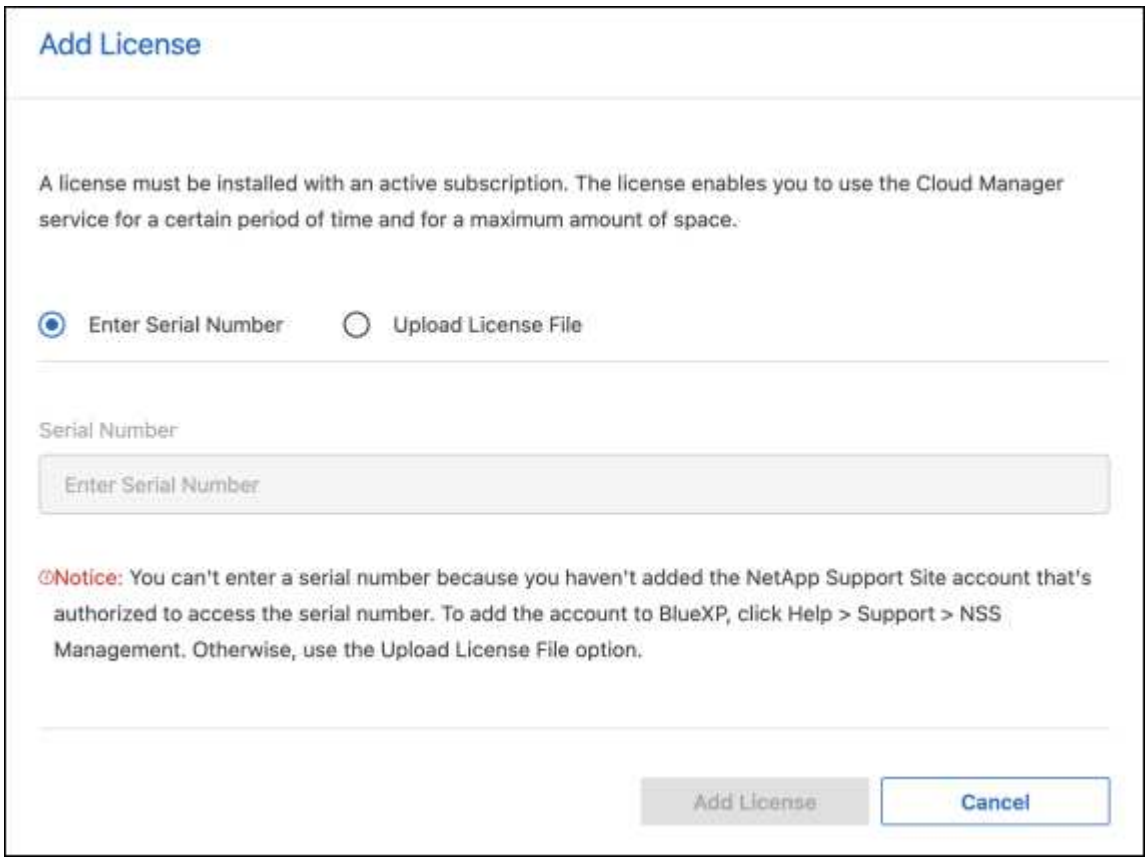
Dopo aver acquistato la licenza Ransomware Resilience dal tuo rappresentante commerciale NetApp , puoi attivarla inserendo il numero di serie di Ransomware Resilience e le informazioni dell'account NetApp Support Site (NSS).

Prima di iniziare

È necessario il numero di serie di Ransomware Resilience. Individua questo numero nel tuo ordine di vendita oppure contatta il team dell'account per ottenere queste informazioni.

Passi

1. Dopo aver ottenuto la licenza, torna a Ransomware Resilience. Seleziona l'opzione **Visualizza metodi di pagamento** in alto a destra. Oppure, nel messaggio che informa della scadenza della prova gratuita, seleziona **Abbonati o acquista una licenza**.
2. Selezionare **Aggiungi licenza** per andare alla pagina Licenze e abbonamenti della console.
3. Dalla scheda **Licenze servizi dati**, seleziona **Aggiungi licenza**.



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

     Se il tuo account del sito di supporto NetApp non è disponibile nell'elenco a discesa, "aggiungere l'account NSS alla Console" .

   - Se disponi del file di licenza zvondolr (necessario quando l'installazione avviene in un sito buio), seleziona l'opzione **Carica file di licenza** e segui le istruzioni per allegare il file.
5. Selezionare **Aggiungi licenza**.

Risultato

Nella pagina Licenses and subscriptions viene mostrato che Ransomware Resilience ha una licenza.

Aggiorna la licenza della tua console quando scade

Se il termine della licenza si avvicina alla data di scadenza o se la capacità della licenza sta raggiungendo il limite, verrai avvisato nell'interfaccia utente di Ransomware Resilience. Puoi aggiornare la tua licenza

Ransomware Resilience prima che scada, in modo da non interrompere l'accesso ai dati scansionati.

Questo messaggio appare anche in Licenses and subscriptions e in "Impostazioni di notifica" .

Passi

1. Puoi inviare un'e-mail all'assistenza per richiedere un aggiornamento della tua licenza.

   Dopo aver pagato la licenza e averla registrata sul sito di supporto NetApp , la console aggiorna automaticamente la licenza. La pagina Licenze dei servizi dati rifletterà la modifica entro 5-10 minuti.

2. Se la Console non riesce ad aggiornare automaticamente la licenza, è necessario caricare manualmente il file di licenza.
   a. È possibile ottenere il file di licenza dal sito di supporto NetApp .
   b. Nella Console, seleziona **Amministrazione** > **Licenses and subscriptions**.
   c. Selezionare la scheda **Licenze servizi dati**, selezionare l'icona **Azioni…** per il numero di serie che si sta aggiornando, quindi selezionare **Aggiorna licenza**.

Disdire l'abbonamento PAYGO

Se desideri disdire il tuo abbonamento PAYGO, puoi farlo in qualsiasi momento.

Passi

1. In Ransomware Resilience, in alto a destra, seleziona l'opzione della licenza.
2. Seleziona **Visualizza metodi di pagamento**.
3. Nei dettagli a discesa, deseleziona la casella **Utilizza dopo la scadenza del metodo di pagamento corrente**.
4. Seleziona **Salva**.

Ulteriori informazioni

- "Documentazione sulle licenze e gli abbonamenti NetApp Console"

Scopri i carichi di lavoro in NetApp Ransomware Resilience

Prima di poter utilizzare NetApp Ransomware Resilience, è necessario rilevare i dati del carico di lavoro. Durante la fase di individuazione, Ransomware Resilience analizza tutti i volumi e i file nei sistemi di tutti gli agenti Console e progetti all'interno di un'organizzazione.

Nella dashboard Discovery, Ransomware Resilience visualizza le configurazioni di sistema supportate e non supportate. Ransomware Resilience valuta le applicazioni Oracle, gli archivi dati VMware, le condivisioni di file e lo storage a blocchi.

Ransomware Resilience non rileva carichi di lavoro con volumi che utilizzano FlexGroup.

Ransomware Resilience verifica la protezione di backup corrente, le copie snapshot e le opzioni di protezione autonoma dai ransomware NetApp . Ransomware Resilience rileva anche le informazioni di protezione da SnapCenter per VMware per i datastore delle VM, SnapCenter per Oracle e NetApp Backup and Recovery per

le condivisioni di file e le condivisioni di file delle VM. Quindi consiglia modi per migliorare la protezione contro il ransomware.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

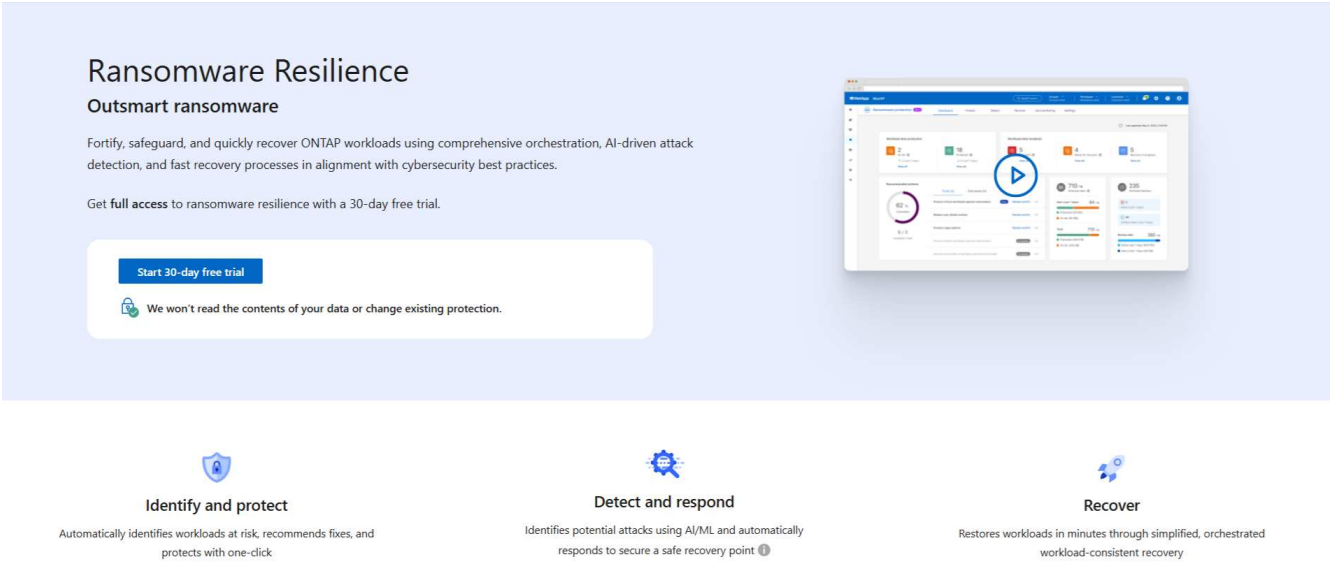
Seleziona i carichi di lavoro da scoprire e proteggere

All'interno di ciascun agente della console, seleziona i sistemi in cui desideri rilevare i carichi di lavoro.

Passi

1. Dalla NetApp Console, seleziona **Protezione** > **Protezione ransomware**.

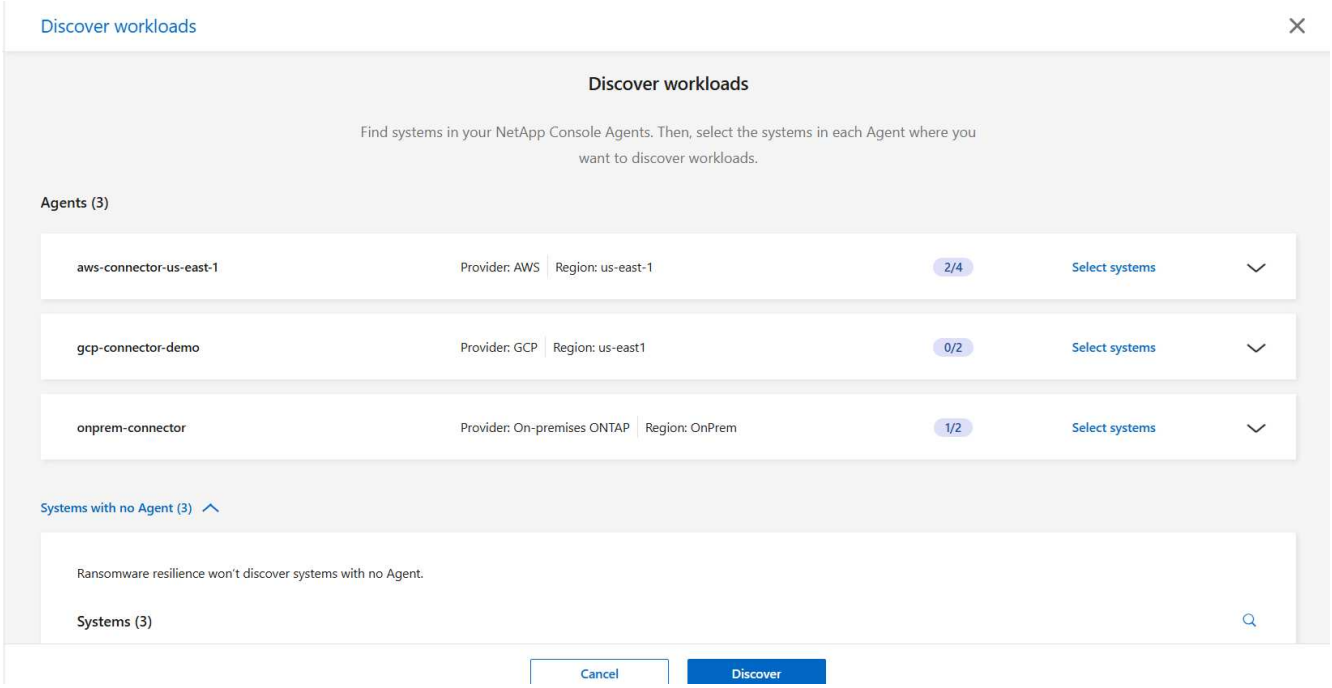
   Se è il tuo primo accesso, verrà visualizzata la landing page.



   Se hai avviato la prova gratuita, l'etichetta del pulsante **Avvia la prova gratuita di 30 giorni** cambia in **Inizia scoprendo i carichi di lavoro**.

2. Dalla landing page iniziale, seleziona **Inizia scoprendo i carichi di lavoro**.

   Ransomware Resilience rileva sia i sistemi supportati che quelli non supportati. Questo processo potrebbe richiedere alcuni minuti.

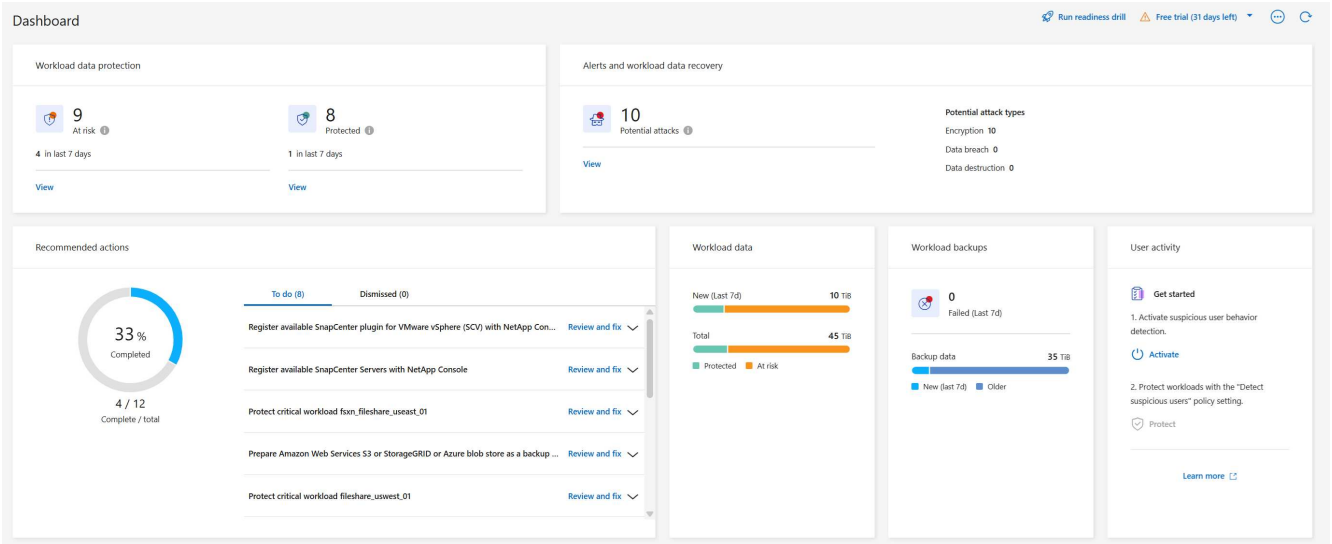


3. Per individuare i carichi di lavoro per uno specifico agente della console, seleziona **Seleziona sistemi** accanto all'agente della console in cui desideri individuare i carichi di lavoro.
4. Seleziona i sistemi in cui desideri rilevare i carichi di lavoro.
5. Seleziona **Scopri**.

   Ransomware Resilience rileva i dati del carico di lavoro solo quando selezioni il sistema. Il processo di scoperta può richiedere diversi minuti.

6. Per scaricare l'elenco dei carichi di lavoro rilevati, seleziona **Scarica risultati**.
7. Per visualizzare la dashboard di Ransomware Resilience, seleziona **Vai alla dashboard**.

   La Dashboard mostra lo stato di salute della protezione dei dati. Numero di aggiornamenti dei carichi di lavoro a rischio o protetti man mano che vengono scoperti nuovi carichi di lavoro.



"Scopri cosa ti mostra la Dashboard."

Scopri i carichi di lavoro appena creati per i sistemi selezionati in precedenza

Se hai aggiunto carichi di lavoro a un sistema precedentemente rilevato, devi riavviare la rilevazione per proteggere i nuovi carichi di lavoro.

Passi

1. Per identificare l'ora dell'ultima scoperta, guarda la data e l'ora accanto all'icona **Aggiorna** in alto a destra nella dashboard di Ransomware Resilience.
2. Dalla Dashboard, seleziona l'icona **Aggiorna** per trovare nuovi carichi di lavoro.

Se noti che alcuni volumi non vengono visualizzati per il sistema individuato, è possibile che non siano supportati. Per trovare un elenco dei volumi non supportati, vai al menu **Impostazioni**, quindi seleziona il menu Azione nella scheda Individuazione del carico di lavoro per scaricare un report JSON dei volumi supportati e non supportati.

Scopri nuovi sistemi

Se hai già scoperto dei sistemi, puoi trovarne di nuovi o non selezionati in precedenza.

Passi

1. Dal menu Ransomware Resilience, seleziona la verticale " opzione category='inline-code'/> in alto a destra. Dal menu a discesa, seleziona **Impostazioni**.
2. Nella scheda Individuazione carichi di lavoro, seleziona **Individuazione carichi di lavoro**. La scoperta potrebbe richiedere alcuni minuti. Un'icona di caricamento mostra l'avanzamento.
3. Ransomware Resilience rileva sia i sistemi supportati che quelli non supportati. Non supporta un sistema se la sua versione ONTAP è inferiore alla versione richiesta. Passando il mouse su un sistema non supportato, viene visualizzato un suggerimento che ne indica il motivo. Seleziona i sistemi in cui desideri rilevare i carichi di lavoro.
4. Seleziona **Scopri**.

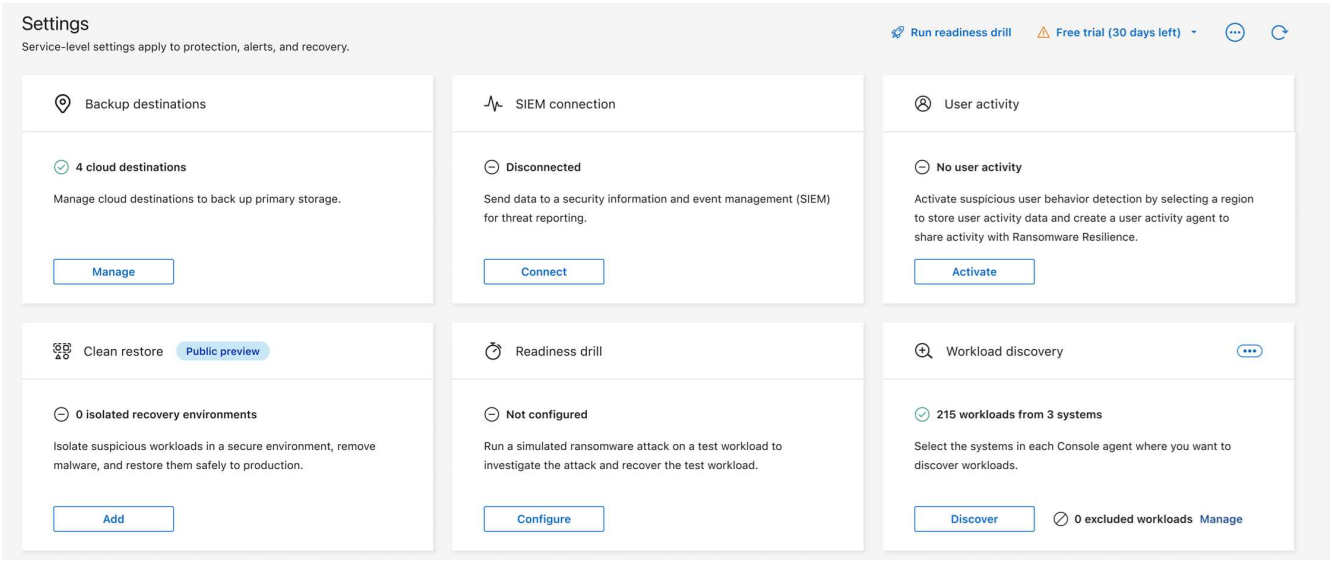
Escludi carichi di lavoro

Ransomware Resilience consente di escludere carichi di lavoro specifici in un sistema dalla protezione e dal rilevamento del ransomware.

È possibile escludere solo i carichi di lavoro supportati e rilevati correttamente. È possibile modificare l'elenco dei carichi di lavoro esclusi in qualsiasi momento. Non ti verrà addebitato alcun costo per i carichi di lavoro esclusi da Ransomware Resilience.

Aggiungi carichi di lavoro all'elenco dei carichi di lavoro esclusi

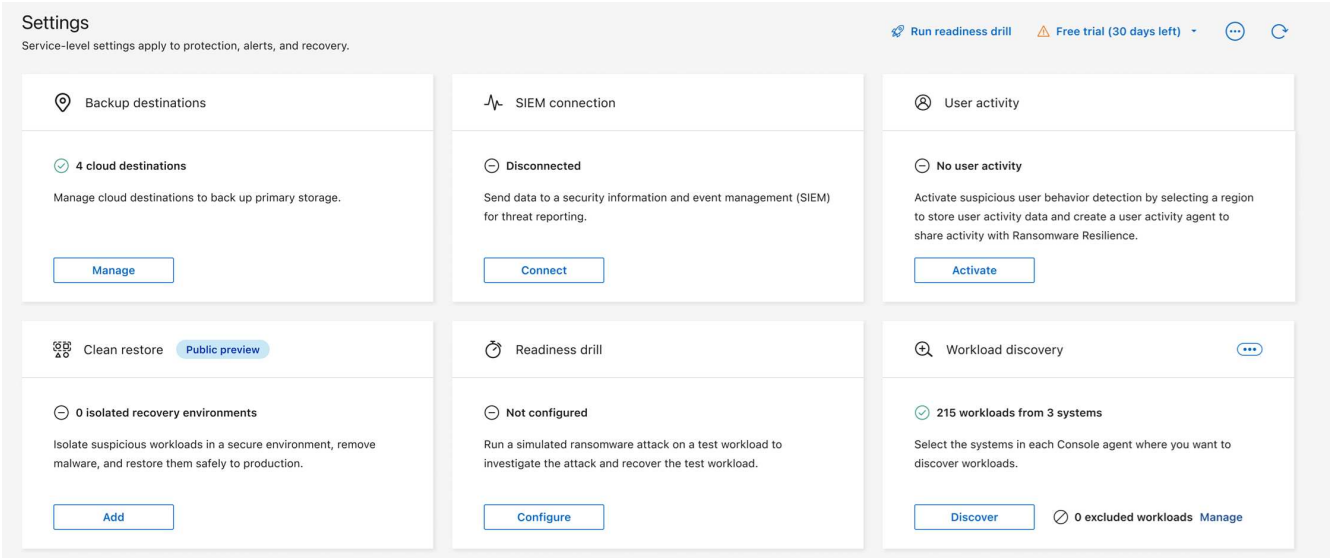
1. In Ransomware Resilience, seleziona **Impostazioni**.
2. Nella dashboard Impostazioni, individua la dashboard Individuazione del carico di lavoro. La scheda identifica il numero di carichi di lavoro esclusi. Per aggiungere carichi di lavoro, accanto ai carichi di lavoro esclusi, seleziona **Gestisci**.



3. Nella pagina Carichi di lavoro esclusi, seleziona **Aggiungi**.
4. Seleziona i carichi di lavoro che vuoi escludere, quindi **Aggiungi**.
5. Esaminare i carichi di lavoro esclusi nella pagina Carichi di lavoro esclusi. Durante l'aggiunta del carico di lavoro, accanto al suo nome viene visualizzato un indicatore di avanzamento. Se un carico di lavoro non è stato escluso correttamente, non viene visualizzato nella pagina.

Rimuovi i carichi di lavoro dall'elenco dei carichi di lavoro esclusi

1. In Ransomware Resilience, seleziona **Impostazioni**.
2. Nella dashboard Impostazioni, individua la dashboard Individuazione del carico di lavoro. La scheda identifica il numero di carichi di lavoro esclusi. Accanto ai carichi di lavoro esclusi, seleziona **Gestisci**.

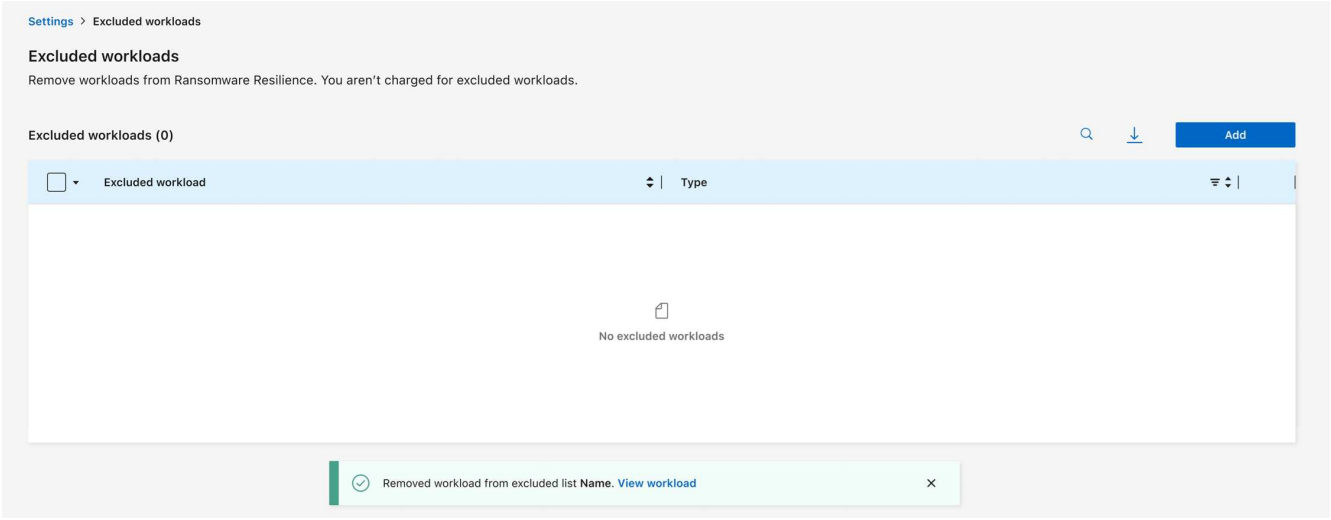


3. Per rimuovere un singolo carico di lavoro, seleziona il menu azioni per il carico di lavoro che desideri rimuovere dall'elenco degli esclusi.

   Per rimuovere più carichi di lavoro, seleziona la casella di controllo accanto ai carichi di lavoro che desideri rimuovere, quindi **Rimuovi da esclusi**.

4. Nella finestra di dialogo, seleziona **Rimuovi** per confermare che desideri rimuovere i carichi di lavoro dall'elenco delle esclusioni.

5. Se il carico di lavoro viene rimosso correttamente dall'elenco dei carichi di lavoro esclusi, nella pagina Carico di lavoro escluso viene visualizzato un messaggio di operazione riuscita e il carico di lavoro non viene più visualizzato nell'elenco dei carichi di lavoro esclusi. Se l'azione fallisce, viene visualizzato un messaggio di errore; riprovare l'operazione.



Esegui un'esercitazione di preparazione agli attacchi ransomware in NetApp Ransomware Resilience

Esegui un'esercitazione di preparazione ad un attacco ransomware simulando un attacco su un nuovo carico di lavoro di esempio. Esaminare l'attacco simulato e recuperare il carico di lavoro. Utilizzare questa funzione per testare le notifiche di avviso, la risposta e il ripristino. Eseguire il trapano tutte le volte che è necessario.

I dati del tuo carico di lavoro reale non subiscono alcun impatto.

È possibile eseguire esercitazioni di preparazione sui carichi di lavoro NFS e CIFS (SMB).

Configurare un'esercitazione di preparazione all'attacco ransomware

Prima di eseguire una simulazione, imposta un'esercitazione nella pagina Impostazioni. Accedi alla pagina Impostazioni dall'opzione Azioni nel menu in alto.

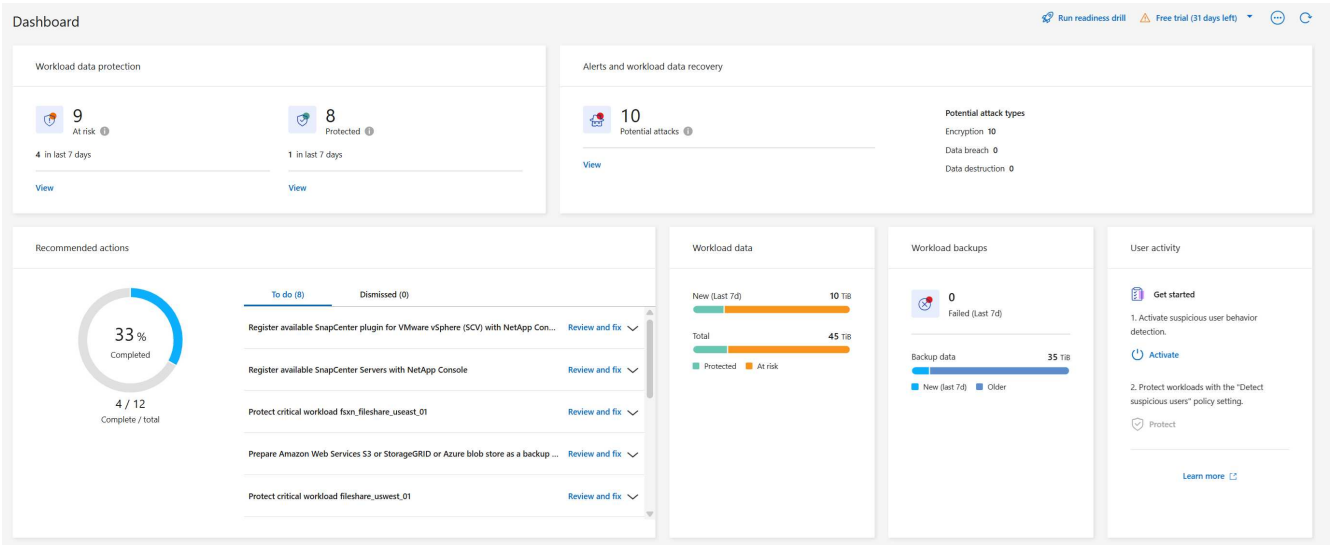
È necessario immettere un nome utente e una password nelle seguenti situazioni:

- Se si sono verificate modifiche al nome utente o alla password per la VM di archiviazione selezionata in precedenza
- Se selezioni una VM di archiviazione CIFS (SMB) diversa
- Se si immette un nome di carico di lavoro di prova diverso

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

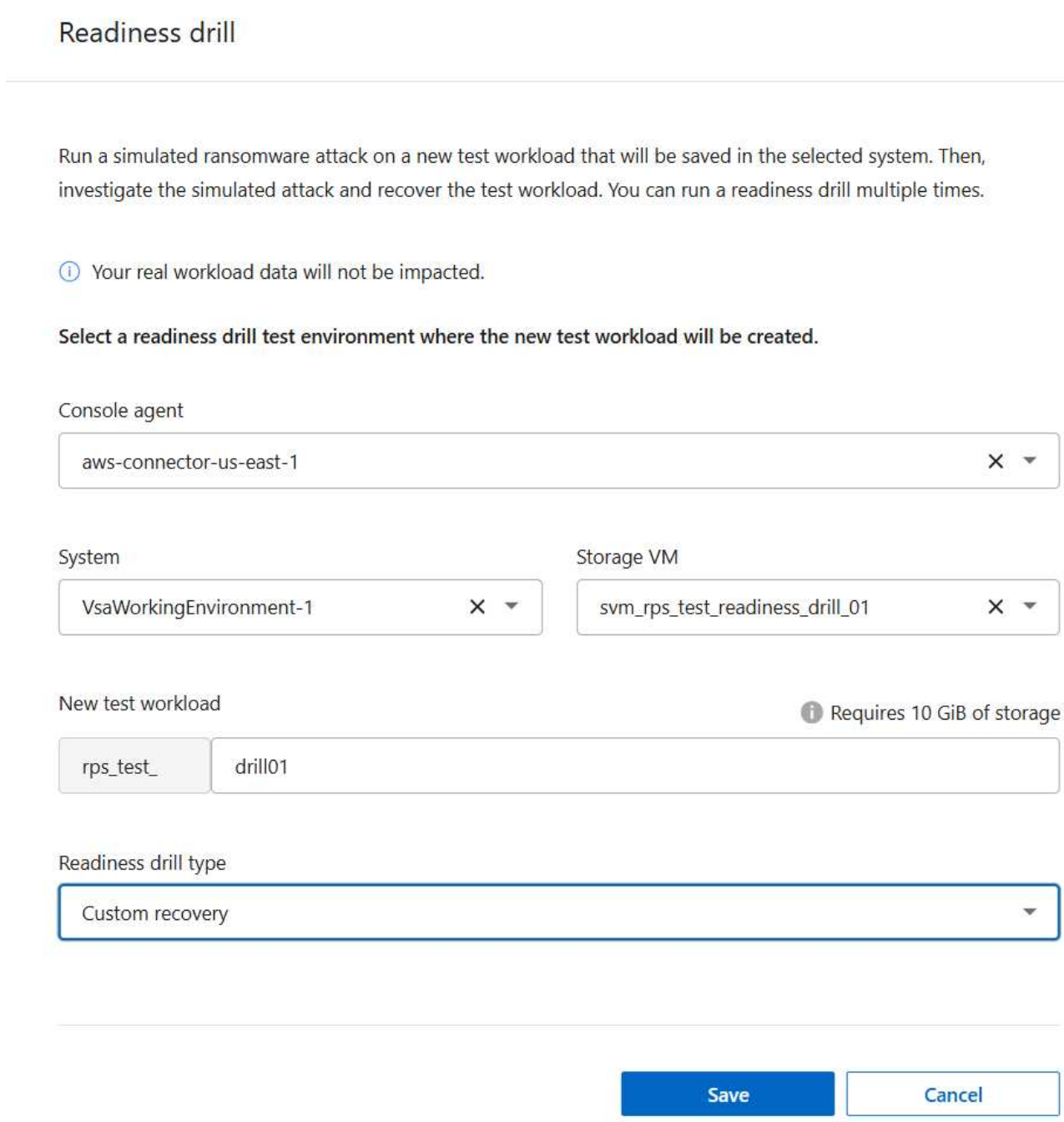
Passi

1. Dal menu NetApp Ransomware Resilience , seleziona il pulsante **Esegui esercitazione di preparazione** in alto a destra.



2. Nella scheda di esercitazione sulla prontezza nella pagina Impostazioni, seleziona **Configura**.

   La Console visualizza la pagina di configurazione dell'esercitazione di preparazione.



3. Procedi come segue:
   a. Selezionare l'agente della console che si desidera utilizzare per l'esercitazione di preparazione.
   b. Selezionare un sistema di prova.
   c. Selezionare un SVM di archiviazione di prova.
   d. Se hai selezionato una VM di archiviazione CIFS (SMB), vengono visualizzati i campi **Nome utente** e **Password**. Immettere il nome utente e la password per la VM di archiviazione.
   e. Selezionare il tipo di esercitazione di preparazione. Per un ripristino manuale da una violazione dei dati crittografati, seleziona **Ripristino personalizzato**. Per il ripristino in caso di attività sospette degli utenti, seleziona **Violazione dei dati**.

f. Immettere il nome del nuovo carico di lavoro di test da creare. Non includere trattini nel nome.

4. Seleziona **Salva**.

È possibile modificare la configurazione dell'esercitazione di preparazione in un secondo momento utilizzando la pagina Impostazioni.

Avviare un'esercitazione di preparazione

Dopo aver configurato l'esercitazione di preparazione, è possibile avviarla.

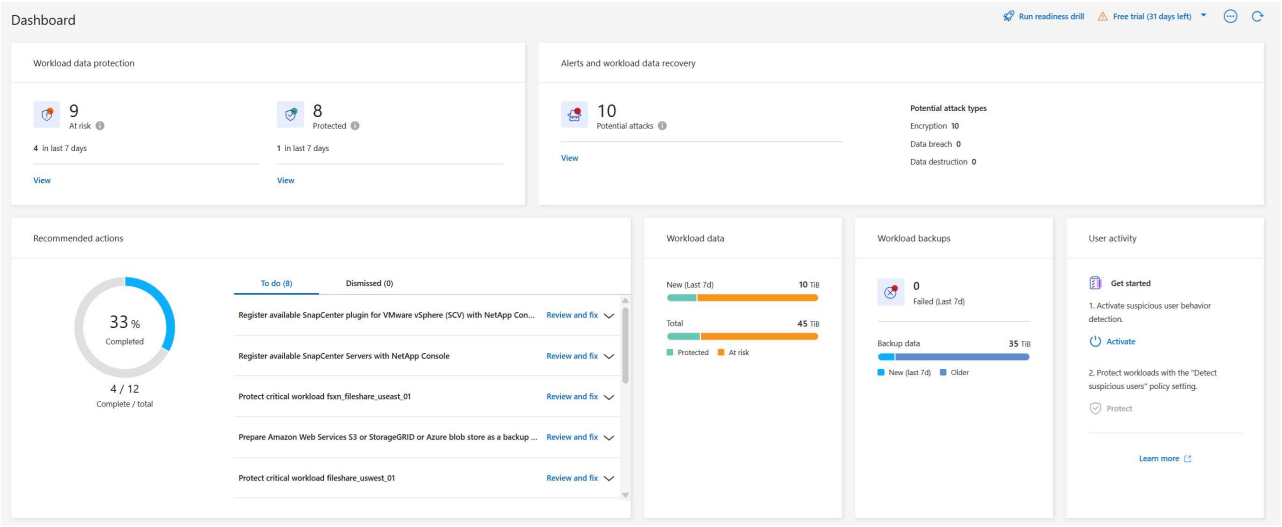
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Quando si avvia l'esercitazione di preparazione, Ransomware Resilience salta la modalità di apprendimento e avvia l'esercitazione in modalità attiva. Lo stato di rilevamento del carico di lavoro è Attivo.

Un carico di lavoro può avere uno stato di **Modalità di apprendimento** per il rilevamento ransomware quando di recente è stato assegnato un criterio di rilevamento e Ransomware Resilience esegue la scansione dei carichi di lavoro.

Passi

1. Eseguire una delle seguenti operazioni:
   - Dal menu Ransomware Resilience, seleziona il pulsante **Esegui esercitazione di preparazione** in alto a destra.



   - OPPURE, dalla pagina Impostazioni, nella scheda Esercizio di preparazione, seleziona **Avvia**.

Non è possibile modificare la configurazione dell'esercitazione di preparazione mentre l'esercitazione è in esecuzione. È possibile reimpostare il trapano per fermarlo e modificarne la configurazione.

Rispondere a un avviso di esercitazione di prontezza

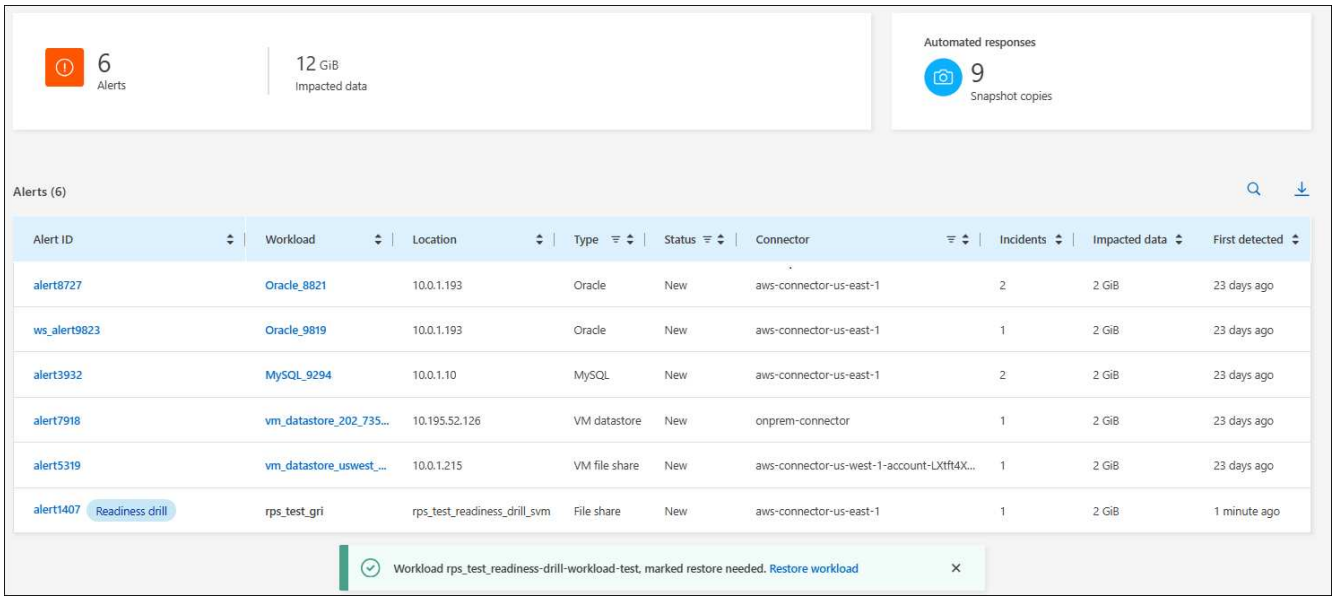
Metti alla prova la tua prontezza rispondendo a un avviso di esercitazione di prontezza.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

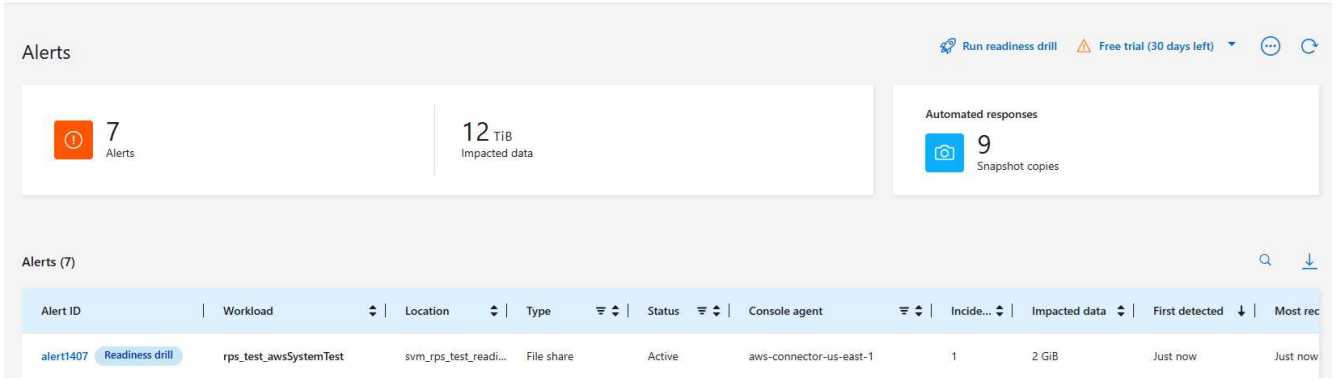
Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.

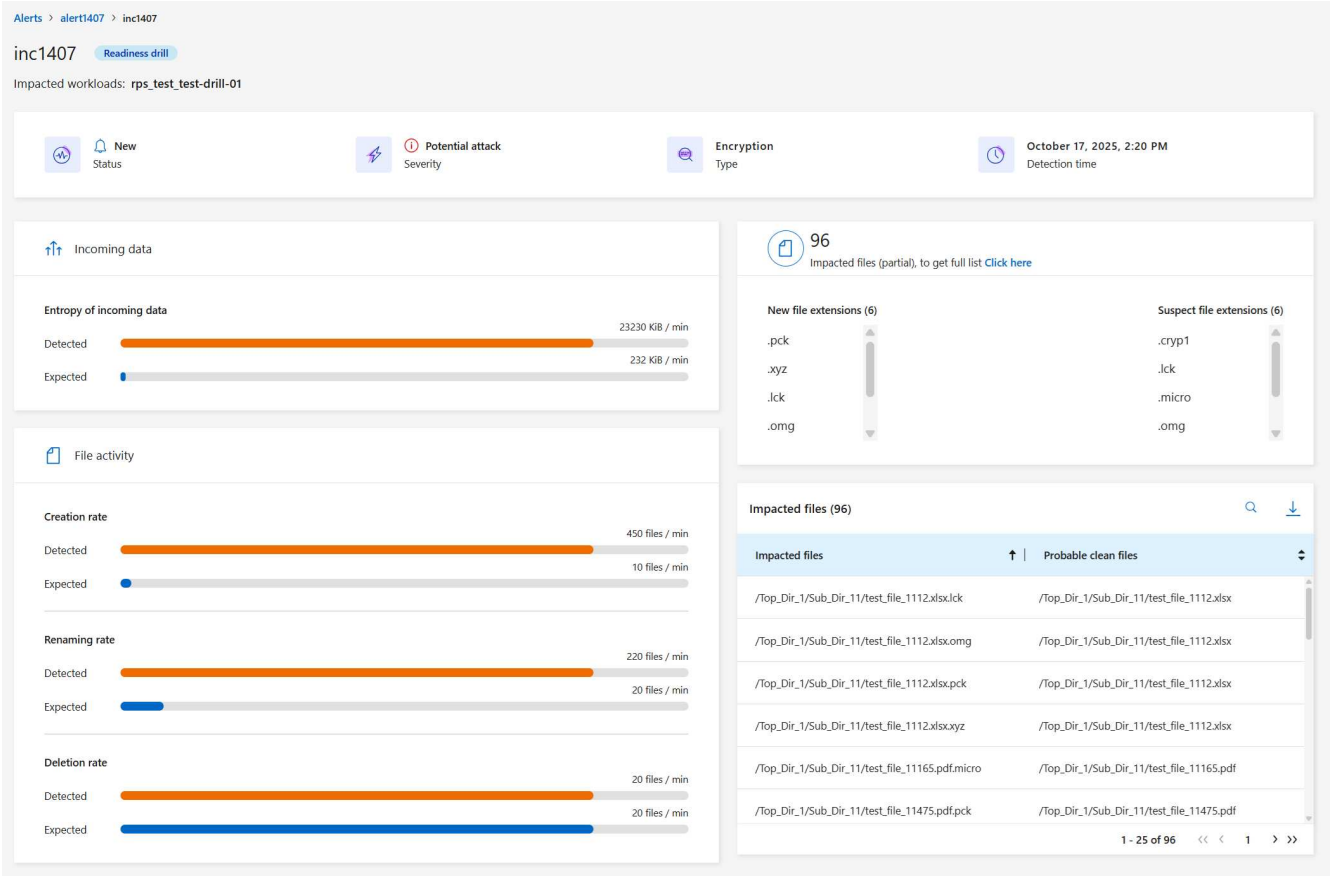
   La Console visualizza la pagina Avvisi. Nella colonna ID avviso, accanto all'ID viene visualizzato "Esercitazione di preparazione".



2. Selezionare l'avviso con l'indicazione "Esercitazione di prontezza". Nella pagina dei dettagli degli avvisi viene visualizzato un elenco degli avvisi di incidente.



3. Esaminare gli incidenti di allerta.
4. Seleziona un incidente di allerta.



Ecco alcune cose da tenere a mente:

- Osserva la potenziale gravità dell'attacco.

  Se la gravità indica che un utente è sospettato di attività dannose, rivedere il nome utente. Puoi anche"bloccare l'utente."

- Esaminare l'attività del file e i processi sospetti:
  - Confrontare i dati rilevati in arrivo con i dati previsti.
  - Confronta la velocità di creazione dei file rilevata con quella prevista.
  - Confronta la frequenza di rinominazione dei file rilevata con quella prevista.
  - Osserva il tasso di eliminazione rispetto al tasso previsto.
- Guarda l'elenco dei file interessati. Esamina le estensioni che potrebbero causare l'attacco.
- Determinare l'impatto e l'ampiezza dell'attacco esaminando il numero di file e directory interessati.

Ripristinare il carico di lavoro del test

Dopo aver esaminato l'avviso di esercitazione di preparazione, ripristinare il carico di lavoro del test, se necessario.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Torna alla pagina dei dettagli dell'avviso.
2. Se il carico di lavoro del test deve essere ripristinato, procedere come segue:
   - Seleziona **Segna come ripristino necessario**.
   - Rivedi la conferma e seleziona **Segna come ripristino necessario** nella casella di conferma.
     - Dal menu Ransomware Resilience, seleziona **Ripristino**.
     - Selezionare il carico di lavoro di prova contrassegnato con "Esercitazione di preparazione" che si desidera ripristinare.
     - Selezionare **Ripristina**.
     - Nella pagina Ripristina, fornisci le informazioni per il ripristino:
   - Selezionare la copia dello snapshot di origine.
   - Selezionare il volume di destinazione.
3. Nella pagina di revisione del ripristino, seleziona **Ripristina**.

   La Console visualizza lo stato del ripristino del drill di prontezza come "In corso" nella pagina Ripristino.

   Una volta completato il ripristino, la Console modifica lo stato del carico di lavoro in **Ripristinato**.
4. Esaminare il carico di lavoro ripristinato.

Per i dettagli sul processo di ripristino, vedere"Recuperare da un attacco ransomware (dopo che gli incidenti sono stati neutralizzati)" .

Modificare lo stato degli avvisi dopo l'esercitazione di preparazione

Dopo aver esaminato l'avviso di esercitazione di prontezza e aver ripristinato il carico di lavoro, modificare lo stato dell'avviso, se necessario.

È richiesto il ruolo Console Amministratore dell'organizzazione, Amministratore di cartelle o progetti o Amministratore di Ransomware Resilience. "Scopri di più sui ruoli di accesso alla console per tutti i servizi" .

Passi

1. Torna alla pagina dei dettagli dell'avviso.
2. Selezionare nuovamente l'avviso.
3. Indicare lo stato selezionando **Modifica stato** e cambiare lo stato in uno dei seguenti:
   - Ignorato: se sospetti che l'attività non sia un attacco ransomware, modifica lo stato in Ignorato.

     Dopo aver respinto un attacco, non è possibile ripristinarlo. Se si ignora un carico di lavoro, tutte le copie snapshot eseguite automaticamente in risposta al potenziale attacco ransomware verranno eliminate definitivamente. Se si ignora l'avviso, l'esercitazione di preparazione è considerata completata.
   - Risolto: l'incidente è stato mitigato.

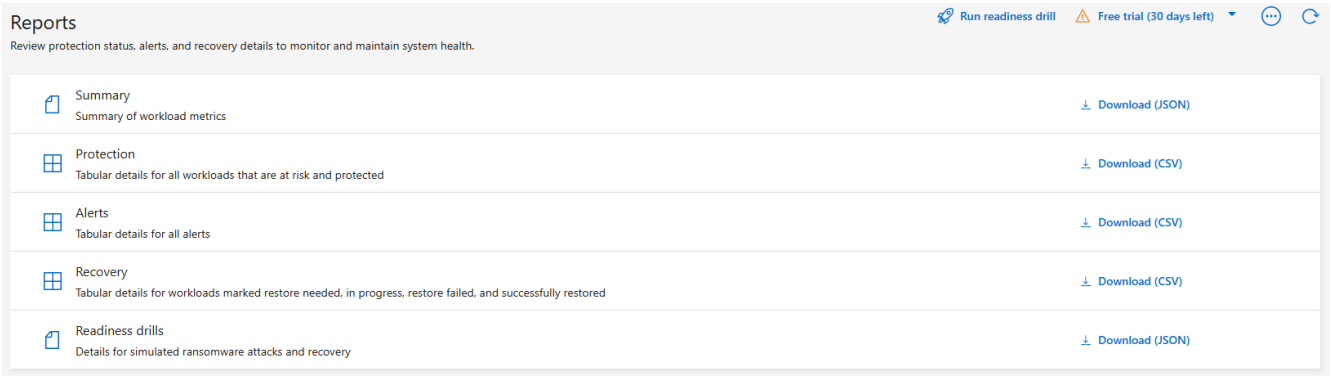
Rivedere i rapporti sull'esercitazione di preparazione

Una volta completata l'esercitazione di preparazione, potresti voler rivedere e salvare un report sull'esercitazione.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Dal menu Ransomware Resilience, seleziona **Report**.



2. Selezionare **Esercitazioni di preparazione** e **Scarica** per scaricare il report delle esercitazioni di preparazione.

Configurare le impostazioni di protezione in NetApp Ransomware Resilience

È possibile configurare destinazioni di backup, inviare dati a un sistema di sicurezza e gestione degli eventi (SIEM) esterno, eseguire un'esercitazione di preparazione agli attacchi, configurare l'individuazione del carico di lavoro o configurare il rilevamento di attività utente sospette accedendo all'opzione **Impostazioni**.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Cosa puoi fare nella pagina Impostazioni? Dalla pagina Impostazioni puoi fare quanto segue:

- Simula un attacco ransomware eseguendo un'esercitazione di preparazione e rispondendo a un avviso ransomware simulato. Per maggiori dettagli, vedere "Eseguire un'esercitazione di preparazione all'attacco ransomware" .
- Configurare l'individuazione del carico di lavoro.
- Configurare la segnalazione delle attività sospette degli utenti.
- Aggiungi una destinazione di backup.
- Collega il tuo sistema di sicurezza e gestione degli eventi (SIEM) per l'analisi e il rilevamento delle minacce. L'abilitazione del rilevamento delle minacce invia automaticamente i dati al SIEM per l'analisi delle minacce.

Accedi direttamente alla pagina Impostazioni

Puoi accedere facilmente alla pagina Impostazioni dall'opzione Azioni vicino al menu in alto.

1. Da Ransomware Resilience, seleziona la verticale  … opzione in alto a destra.
2. Dal menu a discesa, seleziona **Impostazioni**.

Simula un attacco ransomware

Eseguire un'esercitazione di preparazione al ransomware simulando un attacco ransomware su un carico di lavoro di esempio appena creato. Quindi, esaminare l'attacco simulato e recuperare il carico di lavoro di esempio. Questa funzionalità ti aiuta a sapere se sei preparato in caso di un vero e proprio attacco ransomware testando i processi di notifica degli avvisi, risposta e ripristino. È possibile eseguire più volte un'esercitazione di preparazione al ransomware.

Per i dettagli, fare riferimento a"Eseguire un'esercitazione di preparazione all'attacco ransomware" .

Configurare la scoperta del carico di lavoro

È possibile configurare l'individuazione dei carichi di lavoro per rilevare automaticamente i nuovi carichi di lavoro nel proprio ambiente.

1. Nella pagina Impostazioni, individua il riquadro **Individuazione del carico di lavoro**.
2. Nel riquadro **Individuazione carichi di lavoro**, seleziona **Individuazione carichi di lavoro**.

   Questa pagina mostra gli agenti della console con sistemi non selezionati in precedenza, gli agenti della console appena disponibili e i sistemi appena disponibili. Questa pagina non mostra i sistemi precedentemente selezionati.
3. Selezionare l'agente della console in cui si desidera rilevare i carichi di lavoro.
4. Esaminare l'elenco dei sistemi.
5. Selezionare i sistemi in cui si desidera rilevare i carichi di lavoro oppure selezionare la casella nella parte superiore della tabella per rilevare i carichi di lavoro in tutti gli ambienti di carico di lavoro rilevati.
6. Ripetere la stessa operazione per altri sistemi, se necessario.
7. Selezionare **Scopri** per fare in modo che Ransomware Resilience rilevi automaticamente i nuovi carichi di lavoro nell'agente della console selezionato.

Dalla scheda Individuazione del carico di lavoro in Impostazioni, seleziona il menu Azione … quindi **Scarica il report (JSON)** per esaminare un elenco dei carichi di lavoro supportati e non supportati nei tuoi sistemi.

Attività utente sospetta

Nella scheda Attività utente è possibile creare e gestire l'agente attività utente necessario per rilevare attività utente sospette.

Per ulteriori informazioni, consultare "Attività utente sospetta" .

Aggiungi una destinazione di backup

Ransomware Resilience è in grado di identificare i carichi di lavoro che non hanno ancora alcun backup e anche i carichi di lavoro che non hanno ancora alcuna destinazione di backup assegnata.

Per proteggere tali carichi di lavoro, è necessario aggiungere una destinazione di backup. Puoi scegliere una delle seguenti destinazioni di backup:

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

> Le destinazioni di backup non sono disponibili per i carichi di lavoro in Amazon FSx for NetApp ONTAP. Eseguire operazioni di backup utilizzando il servizio di backup FSx for ONTAP .

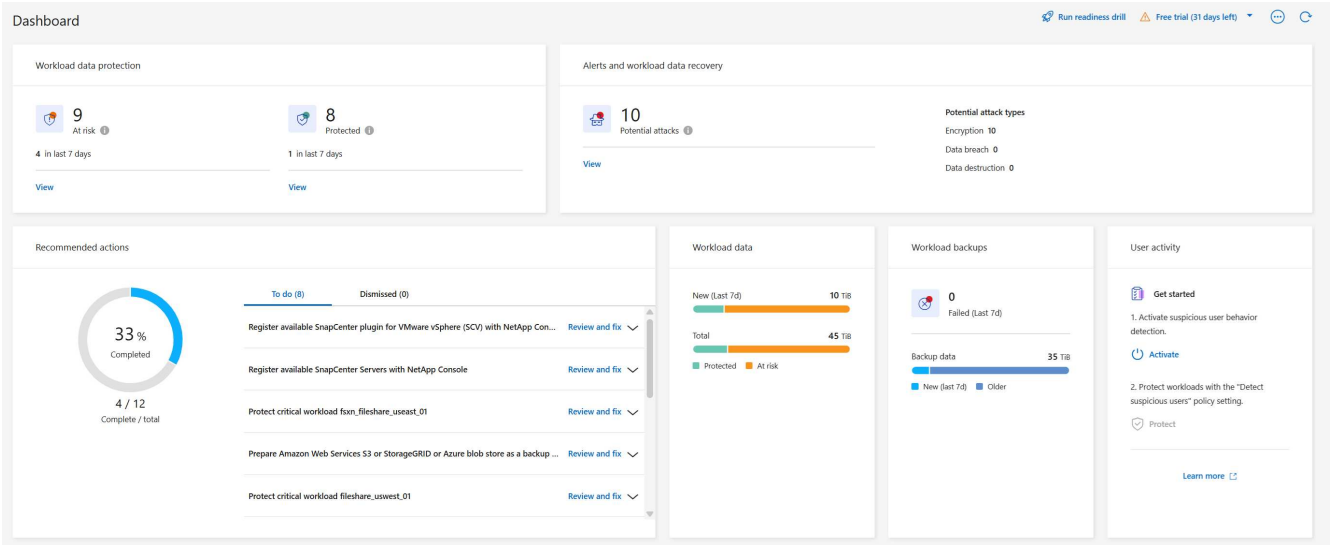
È possibile aggiungere una destinazione di backup in base a un'azione consigliata dalla Dashboard o accedendo all'opzione Impostazioni nel menu.

Accedi alle opzioni di destinazione del backup dalle azioni consigliate della Dashboard

La Dashboard fornisce numerosi suggerimenti. Un consiglio potrebbe essere quello di configurare una destinazione di backup.

Passi

1. Nella dashboard Ransomware Resilience, esamina il riquadro Azioni consigliate.



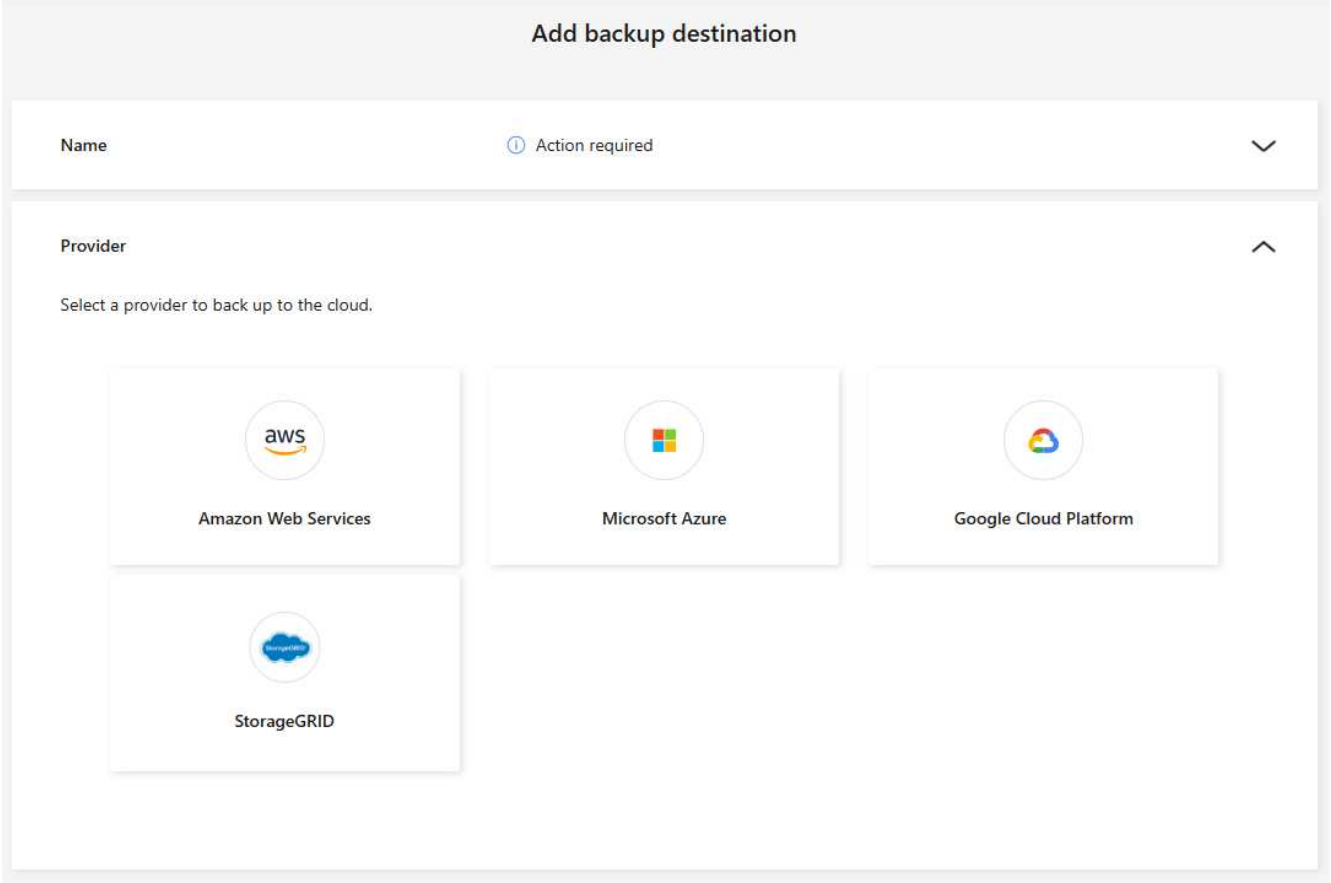
2. Dalla Dashboard, seleziona **Rivedi e correggi** per il suggerimento "Prepara <provider di backup> come destinazione di backup".
3. Proseguire con le istruzioni in base al provider di backup.

Aggiungi StorageGRID come destinazione di backup

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

Passi

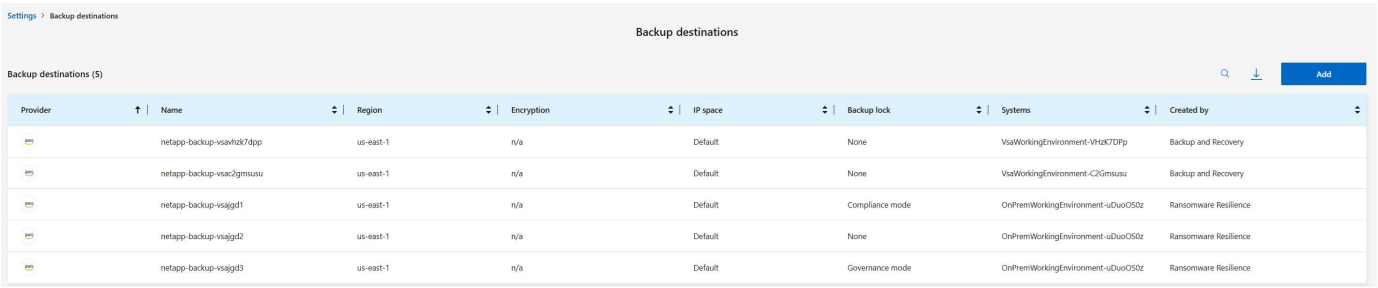
1. Nella pagina **Impostazioni > Destinazioni di backup**, seleziona **Aggiungi**.
2. Immettere un nome per la destinazione del backup.



3. Selezionare * StorageGRID*.
4. Selezionare la freccia rivolta verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni del provider**:
     - Crea un nuovo bucket o porta il tuo bucket in cui archiviare i backup.
     - Nome di dominio completo del nodo gateway StorageGRID , porta, chiave di accesso StorageGRID e credenziali della chiave segreta.
   - **Networking**: Seleziona lo spazio IP.
     - Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
5. Selezionare **Aggiungi**.

Risultato

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



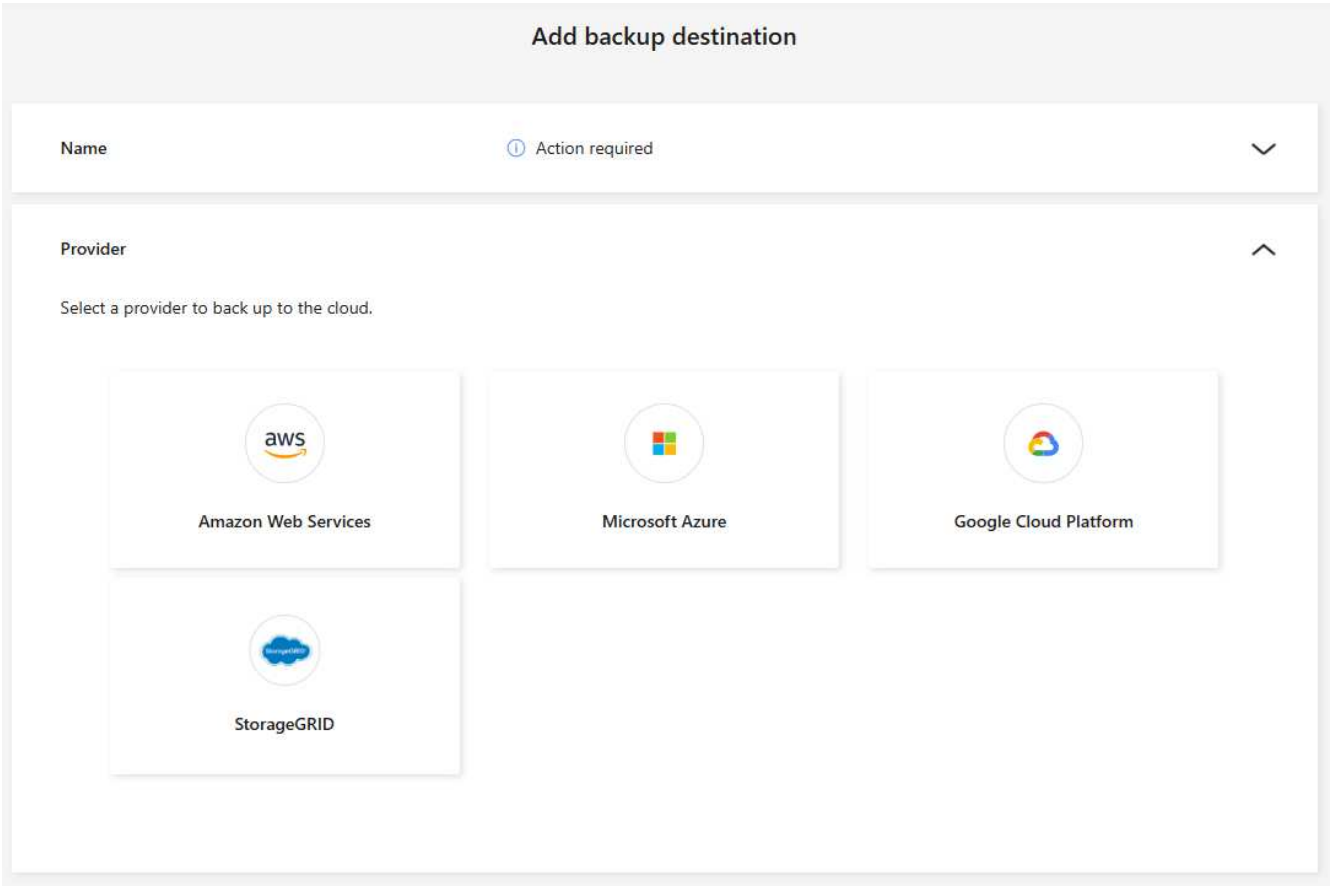
Aggiungi Amazon Web Services come destinazione di backup

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

Per i dettagli sulla gestione dell'archiviazione AWS nella Console, fare riferimento a "Gestisci i tuoi bucket Amazon S3" .

Passi

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



3. Seleziona **Amazon Web Services**.
4. Selezionare la freccia giù accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni del provider**:
     - Crea un nuovo bucket, seleziona un bucket esistente se ne esiste già uno nella Console oppure utilizza il tuo bucket in cui archiviare i backup.
     - Account AWS, regione, chiave di accesso e chiave segreta per le credenziali AWS

       "Se vuoi portare il tuo bucket, fai riferimento ad Aggiungi bucket S3" .
   - **Crittografia**: se stai creando un nuovo bucket S3, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Se hai scelto un bucket esistente, le informazioni sulla crittografia sono già disponibili.

     Per impostazione predefinita, i dati nel bucket vengono crittografati con chiavi gestite da AWS. Puoi continuare a utilizzare le chiavi gestite da AWS oppure puoi gestire la crittografia dei tuoi dati

utilizzando le tue chiavi.

- **Networking**: seleziona lo spazio IP e se utilizzerai un endpoint privato.
  - Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  - Facoltativamente, scegli se utilizzerai un endpoint privato AWS (PrivateLink) configurato in precedenza.

    Se si desidera utilizzare AWS PrivateLink, fare riferimento a "AWS PrivateLink per Amazon S3" .

- **Blocco backup**: scegli se vuoi che Ransomware Resilience protegga i backup da modifiche o eliminazioni. Questa opzione utilizza la tecnologia NetApp DataLock. Ogni backup verrà bloccato durante il periodo di conservazione, o per un minimo di 30 giorni, più un periodo di buffer fino a 14 giorni.

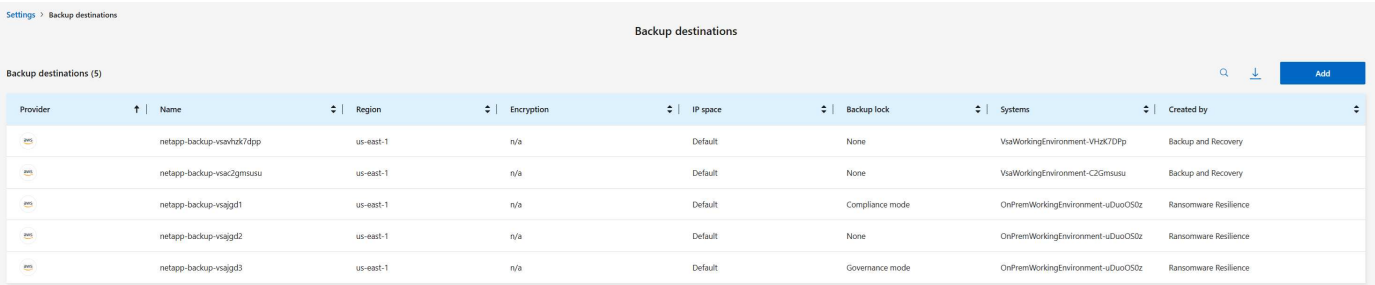
  Se si configura ora l'impostazione di blocco del backup, non sarà possibile modificarla in seguito, dopo aver configurato la destinazione del backup.

  - **Modalità di governance**: utenti specifici (con autorizzazione s3:BypassGovernanceRetention) possono sovrascrivere o eliminare i file protetti durante il periodo di conservazione.
  - **Modalità di 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

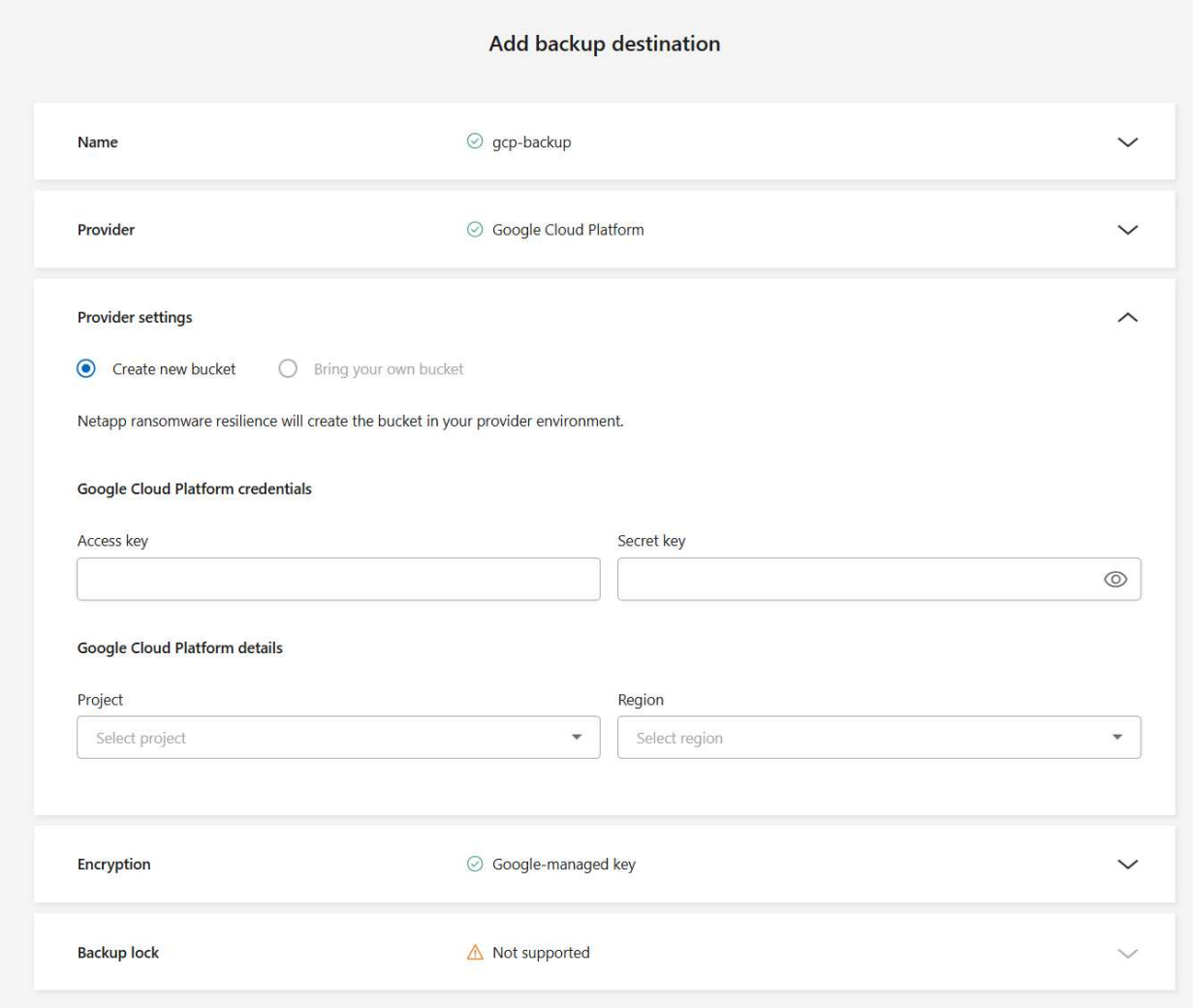
Per impostare Google Cloud Platform (GCP) come destinazione di backup, immettere le seguenti informazioni.

Per i dettagli sulla gestione dell'archiviazione GCP nella Console, fare riferimento a "Opzioni di installazione dell'agente della console in Google Cloud" .

Passi

1. Nella pagina **Impostazioni > Destinazioni di backup**, seleziona **Aggiungi**.
2. Immettere un nome per la destinazione del backup.
3. Seleziona **Google Cloud Platform**.
4. Selezionare la freccia giù accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni del provider**:

- Crea un nuovo bucket. Inserisci la chiave di accesso e la chiave segreta.
- Inserisci o seleziona il tuo progetto e la tua regione Google Cloud Platform.



- **Crittografia**: se stai creando un nuovo bucket, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Se hai scelto un bucket esistente, le informazioni sulla crittografia sono già disponibili.

  Per impostazione predefinita, i dati nel bucket vengono crittografati con chiavi gestite da Google. Puoi continuare a utilizzare le chiavi gestite da Google.

- **Networking**: seleziona lo spazio IP e se utilizzerai un endpoint privato.
  - Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  - Facoltativamente, scegli se utilizzerai un endpoint privato GCP (PrivateLink) configurato in precedenza.

5. Selezionare **Aggiungi**.

Risultato

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

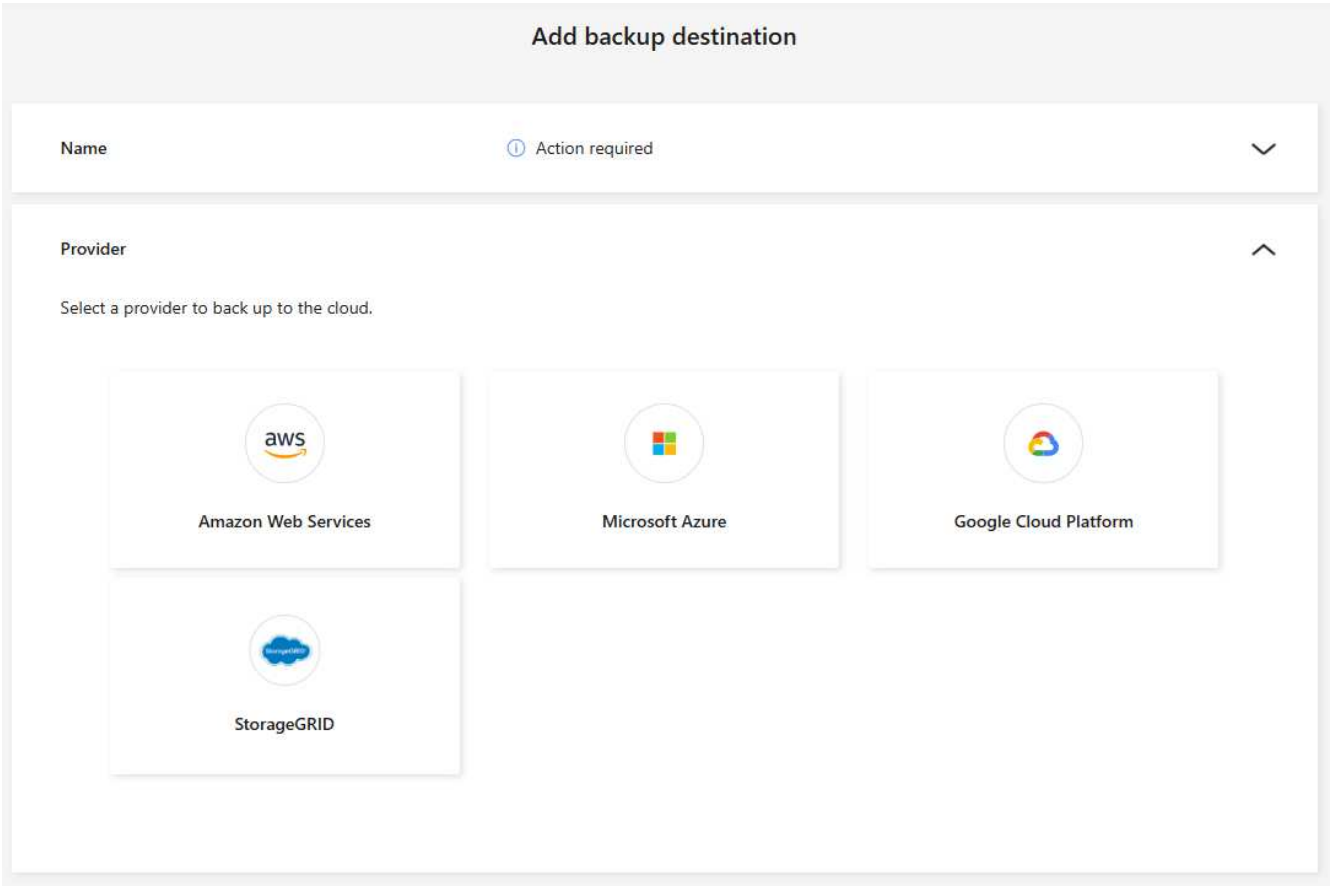
Aggiungi Microsoft Azure come destinazione di backup

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

Per informazioni dettagliate sulla gestione delle credenziali di Azure e degli abbonamenti al marketplace nella console, fare riferimento a "Gestisci le tue credenziali di Azure e gli abbonamenti al marketplace" .

Passi

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



3. Selezionare **Azure**.
4. Selezionare la freccia giù accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni del provider**:
     - Crea un nuovo account di archiviazione, selezionane uno esistente se ne esiste già uno nella Console oppure utilizza il tuo account di archiviazione che memorizzerà i backup.
     - Sottoscrizione, regione e gruppo di risorse di Azure per le credenziali di Azure

       "Se si desidera utilizzare il proprio account di archiviazione, fare riferimento ad Aggiungere account di archiviazione BLOB di Azure" .
   - **Crittografia**: se stai creando un nuovo account di archiviazione, inserisci le informazioni sulla chiave di crittografia fornite dal provider. Se hai scelto un account esistente, le informazioni di crittografia sono già disponibili.

     Per impostazione predefinita, i dati nell'account vengono crittografati con chiavi gestite da Microsoft.

Puoi continuare a utilizzare le chiavi gestite da Microsoft oppure puoi gestire la crittografia dei tuoi dati utilizzando le tue chiavi.

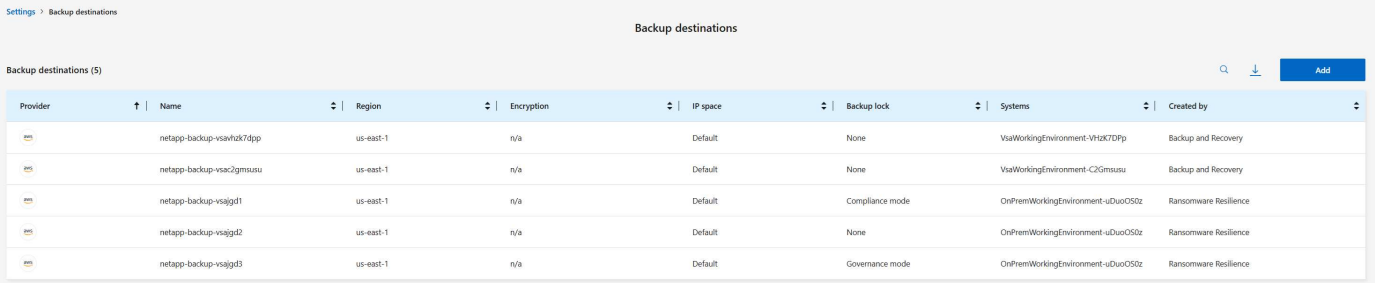
- **Networking**: seleziona lo spazio IP e se utilizzerai un endpoint privato.
  - Lo spazio IP è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. I LIF intercluster per questo spazio IP devono avere accesso a Internet in uscita.
  - Facoltativamente, scegli se utilizzerai un endpoint privato di Azure configurato in precedenza.

    Se si desidera utilizzare Azure PrivateLink, fare riferimento a "Azure PrivateLink" .

5. Selezionare **Aggiungi**.

Risultato

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



Connettersi a un sistema di gestione della sicurezza e degli eventi (SIEM) per l'analisi e il rilevamento delle minacce

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

Prima di abilitare SIEM in Ransomware Resilience, è necessario configurare il sistema SIEM.

Informazioni sui dati dell'evento inviati a un SIEM

Ransomware Resilience può inviare i seguenti dati sugli eventi al tuo sistema SIEM:

- **contesto**:
  - **os**: Questa è una costante con il valore di ONTAP.
  - **os_version**: la versione di ONTAP in esecuzione sul sistema.
  - **connector_id**: ID dell'agente della console che gestisce il sistema.
  - **cluster_id**: ID del cluster segnalato da ONTAP per il sistema.
  - **svm_name**: Nome dell'SVM in cui è stato trovato l'avviso.
  - **volume_name**: Nome del volume su cui si trova l'avviso.
  - **volume_id**: ID del volume segnalato da ONTAP per il sistema.
- **incidente**:
  - **incident_id**: ID incidente generato da Ransomware Resilience per il volume sottoposto ad attacco in Ransomware Resilience.
  - **alert_id**: ID generato da Ransomware Resilience per il carico di lavoro.

- **gravità**: Uno dei seguenti livelli di allerta: "CRITICO", "ALTO", "MEDIO", "BASSO".
- **descrizione**: Dettagli sull'avviso rilevato, ad esempio "Un potenziale attacco ransomware rilevato sul carico di lavoro arp_learning_mode_test_2630"

Configurare AWS Security Hub per il rilevamento delle minacce

Prima di abilitare AWS Security Hub in Ransomware Resilience, è necessario eseguire i seguenti passaggi generali in AWS Security Hub:

- Imposta le autorizzazioni in AWS Security Hub.
- Imposta la chiave di accesso all'autenticazione e la chiave segreta in AWS Security Hub. (Questi passaggi non sono forniti qui.)

Passaggi per impostare le autorizzazioni in AWS Security Hub

1. Vai alla **console AWS IAM**.
2. Selezionare **Politiche**.
3. Crea una policy 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"
      ]
    }
  ]
}
```

Configurare Microsoft Sentinel per il rilevamento delle minacce

Prima di abilitare Microsoft Sentinel in Ransomware Resilience, è necessario eseguire i seguenti passaggi generali in Microsoft Sentinel:

- **Prerequisiti**
  - Abilita Microsoft Sentinel.
  - Crea un ruolo personalizzato in Microsoft Sentinel.
- **Registrazione**

    - Registra Ransomware Resilience per ricevere eventi da Microsoft Sentinel.
    - Crea un segreto per la registrazione.
- **Autorizzazioni**: assegna le autorizzazioni all'applicazione.
- **Autenticazione**: immettere le credenziali di autenticazione per l'applicazione.

Passaggi per abilitare Microsoft Sentinel

1. Vai a Microsoft Sentinel.
2. Creare un'**area di lavoro di Log Analytics**.
3. Abilita Microsoft Sentinel per utilizzare l'area di lavoro Log Analytics appena creata.

Passaggi per creare un ruolo personalizzato in Microsoft Sentinel

1. Vai a Microsoft Sentinel.
2. Selezionare **Abbonamento** > **Controllo accessi (IAM)**.
3. Inserisci un nome di ruolo personalizzato. Utilizzare il nome **Ransomware Resilience Sentinel Configurator**.
4. Copia il seguente JSON e incollalo nella scheda **JSON**.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Rivedi e salva le tue impostazioni.

Passaggi per registrare Ransomware Resilience per ricevere eventi da Microsoft Sentinel

1. Vai a Microsoft Sentinel.
2. Selezionare **Entra ID** > **Applicazioni** > **Registrazioni app**.
3. Per il **Nome visualizzato** dell'applicazione, immettere "**Ransomware Resilience**".
4. Nel campo **Tipo di account supportato**, seleziona **Solo account in questa directory organizzativa**.
5. Selezionare un **Indice predefinito** in cui verranno inviati gli eventi.
6. Seleziona **Recensione**.
7. Seleziona **Registra** per salvare le tue impostazioni.

   Dopo la registrazione, l'interfaccia di amministrazione di Microsoft Entra visualizza il riquadro Panoramica dell'applicazione.

Passaggi per creare un segreto per la registrazione

1. Vai a Microsoft Sentinel.
2. Selezionare **Certificati e segreti** > **Segreti client** > **Nuovo segreto client**.

3. Aggiungi una descrizione per il segreto della tua applicazione.
4. Seleziona una **Scadenza** per il segreto oppure specifica una durata personalizzata.

   La durata del segreto del cliente è limitata a due anni (24 mesi) o meno. Microsoft consiglia di impostare un valore di scadenza inferiore a 12 mesi.

5. Seleziona **Aggiungi** per creare il tuo segreto.
6. Registrare il segreto da utilizzare nella fase di autenticazione. Una volta che avrai abbandonato questa pagina, il segreto non verrà più visualizzato.

Passaggi per assegnare le autorizzazioni all'applicazione

1. Vai a Microsoft Sentinel.
2. Selezionare **Abbonamento** > **Controllo accessi (IAM)**.
3. Selezionare **Aggiungi** > **Aggiungi assegnazione ruolo**.
4. Per il campo **Ruoli di amministratore privilegiato**, selezionare **Ransomware Resilience Sentinel Configurator**.

   Questo è il ruolo personalizzato che hai creato in precedenza.

5. Selezionare **Avanti**.
6. Nel campo **Assegna accesso a**, seleziona **Utente, gruppo o entità servizio**.
7. Seleziona **Seleziona membri**. Quindi, seleziona **Ransomware Resilience Sentinel Configurator**.
8. Selezionare **Avanti**.
9. Nel campo **Cosa può fare l'utente**, seleziona **Consenti all'utente di assegnare tutti i ruoli eccetto i ruoli di amministratore con privilegi Proprietario, UAA, RBAC (consigliato)**.
10. Selezionare **Avanti**.
11. Selezionare **Rivedi e assegna** per assegnare le autorizzazioni.

Passaggi per immettere le credenziali di autenticazione per l'applicazione

1. Vai a Microsoft Sentinel.
2. Inserisci le credenziali:
   a. Immettere l'ID tenant, l'ID applicazione client e il segreto dell'applicazione client.
   b. Fare clic su **Autentica**.

      Una volta completata l'autenticazione, verrà visualizzato il messaggio "Autenticato".

3. Immettere i dettagli dell'area di lavoro di Log Analytics per l'applicazione.
   a. Selezionare l'ID dell'abbonamento, il gruppo di risorse e l'area di lavoro Log Analytics.

Configurare Splunk Cloud per il rilevamento delle minacce

Prima di abilitare Splunk Cloud in Ransomware Resilience, è necessario eseguire i seguenti passaggi generali in Splunk Cloud:

- Abilita un HTTP Event Collector in Splunk Cloud per ricevere dati sugli eventi tramite HTTP o HTTPS dalla Console.

- Crea un token Event Collector in Splunk Cloud.

Passaggi per abilitare un HTTP Event Collector in Splunk

1. Vai a Splunk Cloud.
2. Selezionare **Impostazioni** > **Inserimento dati**.
3. Selezionare **HTTP Event Collector** > **Impostazioni globali**.
4. Nel menu a discesa Tutti i token, seleziona **Abilitato**.
5. Per fare in modo che Event Collector ascolti e comunichi tramite HTTPS anziché HTTP, selezionare **Abilita SSL**.
6. Immettere una porta in **Numero porta HTTP** per HTTP Event Collector.

Passaggi per creare un token Event Collector in Splunk

1. Vai a Splunk Cloud.
2. Selezionare **Impostazioni** > **Aggiungi dati**.
3. Selezionare **Monitor** > **HTTP Event Collector**.
4. Inserisci un nome per il token e seleziona **Avanti**.
5. Selezionare un **Indice predefinito** in cui verranno inviati gli eventi, quindi selezionare **Revisiona**.
6. Verificare che tutte le impostazioni per l'endpoint siano corrette, quindi selezionare **Invia**.
7. Copia il token e incollalo in un altro documento per averlo pronto per la fase di autenticazione.

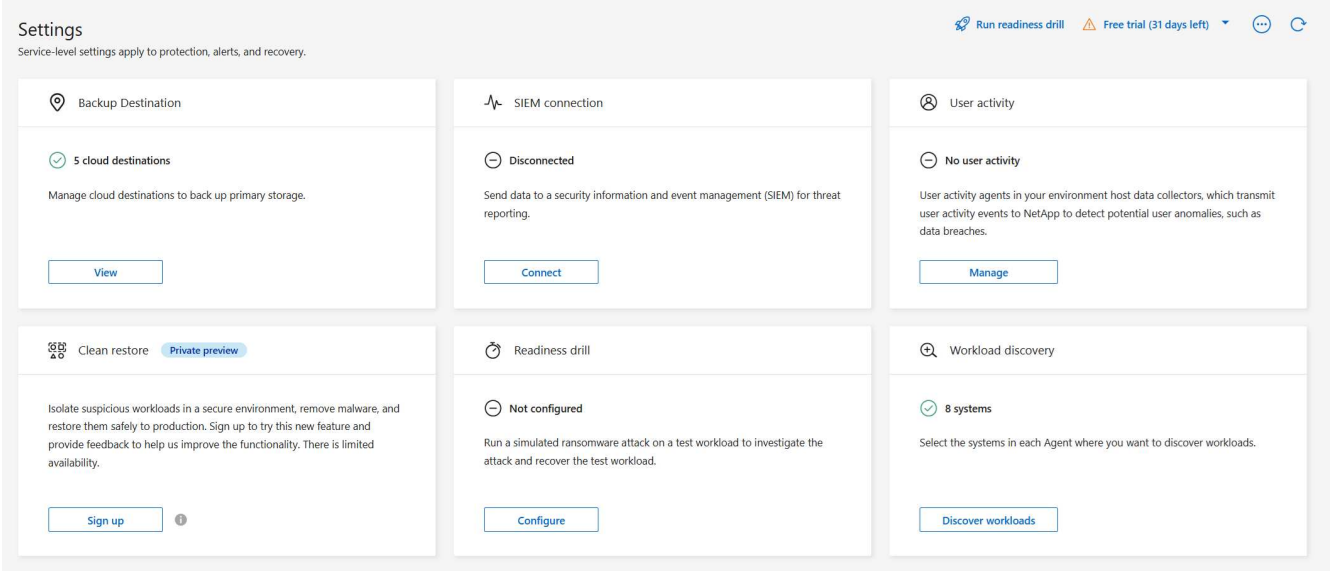
Connetti SIEM alla resilienza del ransomware

Abilitando SIEM, i dati da Ransomware Resilience vengono inviati al server SIEM per l'analisi e la segnalazione delle minacce.

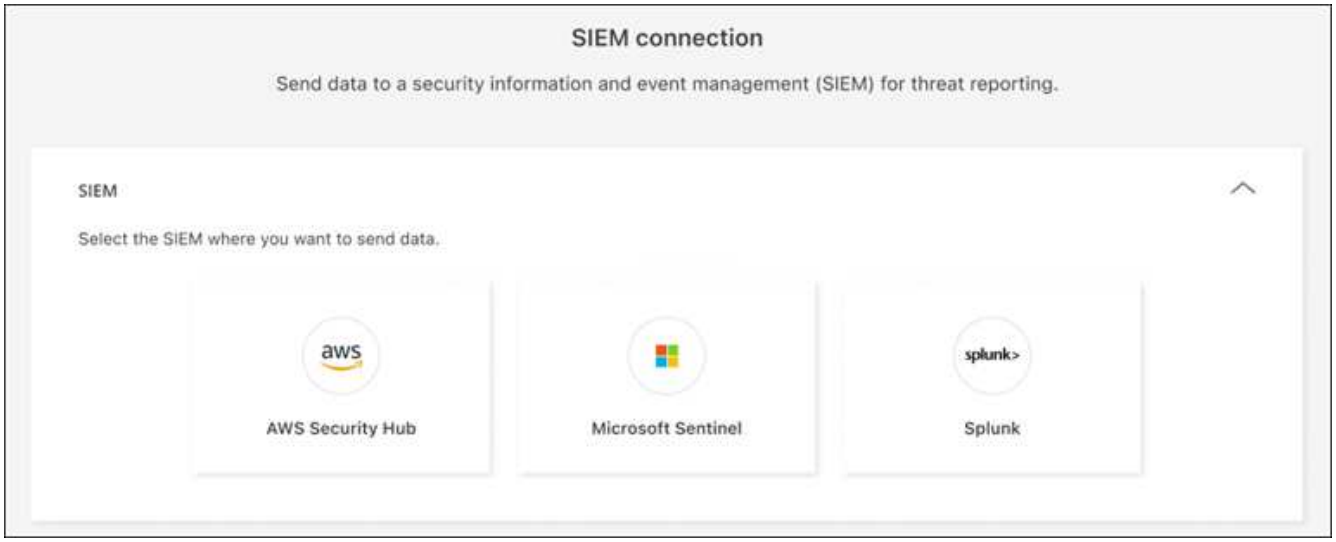
Passi

1. Dal menu Console, seleziona **Protezione** > **Ransomware Resilience**.
2. Dal menu Ransomware Resilience, seleziona la verticale … opzione in alto a destra.
3. Selezionare **Impostazioni**.

   Viene visualizzata la pagina Impostazioni.



4. Nella pagina Impostazioni, seleziona **Connetti** nel riquadro Connessione SIEM.



5. Scegli uno dei sistemi SIEM.
6. Inserisci il token e i dettagli di autenticazione configurati in AWS Security Hub o Splunk Cloud.

   Le informazioni da immettere dipendono dal SIEM selezionato.

7. Selezionare **Abilita**.

   Nella pagina Impostazioni viene visualizzato "Connesso".

Configura il rilevamento dell'attività dell'utente

Scopri il rilevamento delle attività degli utenti in NetApp Ransomware Resilience

NetApp Ransomware Resilience supporta il rilevamento di comportamenti sospetti degli utenti, consentendo di affrontare gli incidenti ransomware a livello di utente.

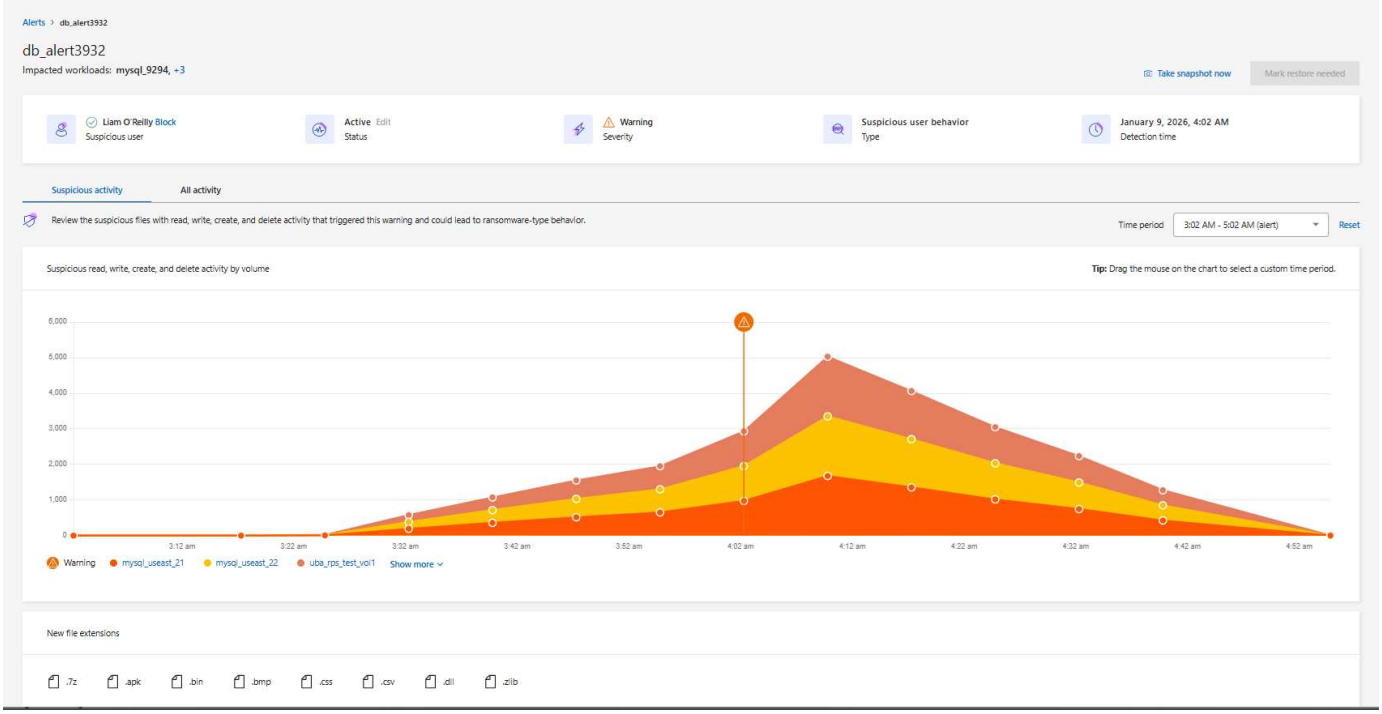
NetApp Ransomware Resilience offre un rilevamento delle violazioni dei dati basato sull'intelligenza artificiale monitorando le attività sospette degli utenti. Forti aumenti dell'attività di lettura e dei modelli di accesso all'attività di lettura vengono utilizzati per determinare l'intento malevolo. Una volta rilevato, Ransomware Resilience genera automaticamente avvisi nella NetApp Console, via e-mail e in qualsiasi ecosistema di sicurezza configurato (ad esempio, SIEM).

Grazie al rilevamento e all'invio di avvisi in caso di comportamenti sospetti degli utenti, Ransomware Resilience ti avvisa di tentativi e modelli di violazione e distruzione dei dati che sembrano sospetti. In ogni avviso, Ransomware Resilience identifica un utente che puoi bloccare.

Ransomware Resilience rileva le attività sospette degli utenti analizzando gli eventi di attività degli utenti generati da FPolicy in ONTAP. Per raccogliere dati sull'attività dell'utente, è necessario distribuire uno o più agenti di attività dell'utente. L'agente è un server Linux o una macchina virtuale con connettività ai dispositivi del tuo tenant.

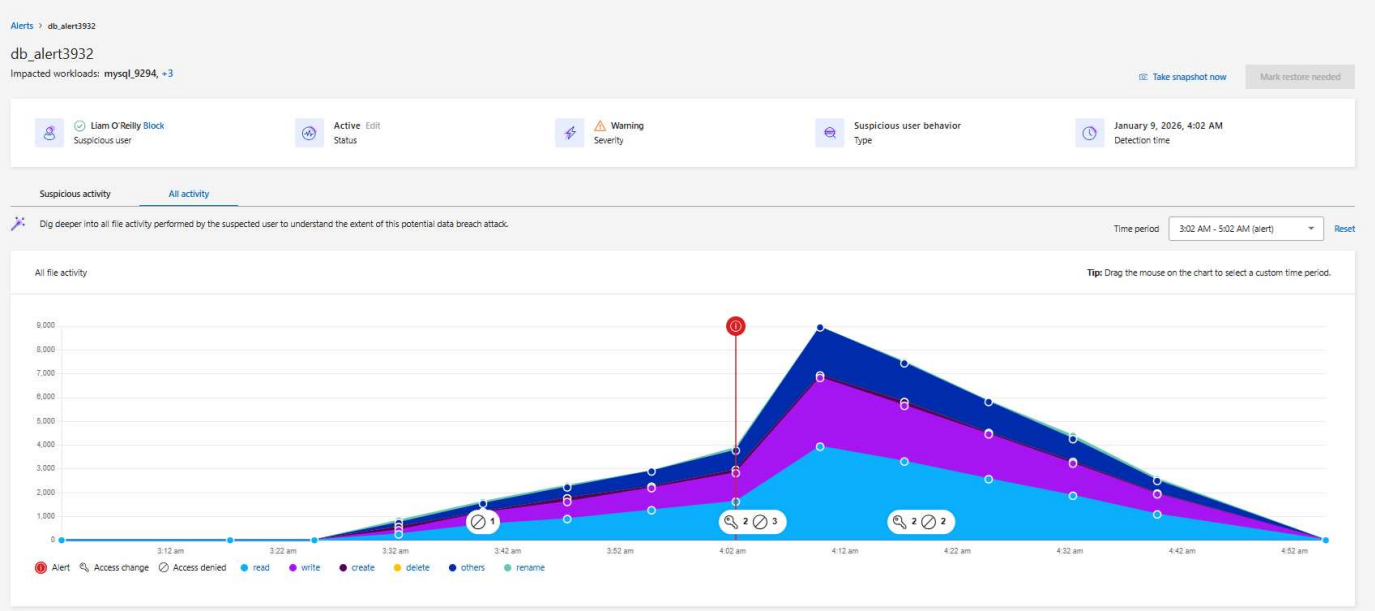
Analisi forense delle attività sospette degli utenti

Ransomware Resilience offre forensics per i comportamenti degli utenti: elenchi e grafici che mostrano quando si sono verificate attività sospette e quando sono state inviate notifiche. Questi dettagliano la frequenza delle attività sospette su file, directory, volumi e carichi di lavoro nel tempo per aiutare a tracciare gli eventi. Puoi anche osservare la comparsa di nuove estensioni di file.



.

È possibile confrontare le attività sospette con una visualizzazione di tutte le attività. Nella visualizzazione di tutte le attività, è possibile osservare eventi di lettura, scrittura, ridenominazione, spostamento, creazione ed eliminazione, oltre a eventi di modifica dell'accesso e di accesso negato.



.

Componenti

Ci sono tre componenti chiave nel rilevamento dell'attività sospetta degli utenti in Ransomware Resilience.

- L'**agente di attività utente** è un ambiente eseguibile per i raccoglitori di dati. È necessario configurare l'agente di attività utente.
- Il **collettore dati** condivide gli eventi di attività dell'utente con Ransomware Resilience. Il collettore dati viene creato automaticamente quando abilita una strategia di protezione dal ransomware con rilevamento delle attività sospette degli utenti.
- Il **connettore directory utente** consente la mappatura tra nomi utente e ID utente, garantendo maggiore chiarezza nella risposta a comportamenti sospetti degli utenti. È necessario configurare il connettore directory utente.

NetApp Ransomware Resilience e Data Infrastructure Insights

Il rilevamento del comportamento sospetto degli utenti di Ransomware Resilience è un'integrazione con Data Infrastructure Insights (DII) Workload Security e utilizza "Endpoint DII". Non è necessaria alcuna configurazione DII per abilitare il rilevamento del comportamento degli utenti in Ransomware Resilience. Per abilitare il rilevamento del comportamento degli utenti, "crea l'agente e i collettori richiesti e abilita la strategia di protezione ransomware appropriata".

Se stai già utilizzando NetApp Data Infrastructure Insights (DII) Workload Security, è consigliato utilizzare gli stessi agenti Workload Security per Ransomware Resilience. Non è necessario distribuire agenti Workload Security separati per Ransomware Resilience, tuttavia, l'utilizzo degli stessi agenti Workload Security richiede una relazione di associazione tra l'organizzazione Ransomware Resilience Console e il tenant DII Storage Workload Security. Contatta il tuo rappresentante di account per abilitare questa associazione.

Prossimi passi

- "Requisiti per il rilevamento dell'attività comportamentale dell'utente"
- "Configura gli agenti e i rilevatori di attività comportamentale degli utenti"

Requisiti per il rilevamento del comportamento dell'utente in NetApp Ransomware Resilience

Prima di creare un agente di attività utente e altri collettori, è necessario assicurarsi di soddisfare i requisiti delineati per il sistema operativo, il server e la rete.

Supporto del cloud provider

Supporto del provider cloud

I dati sulle attività sospette degli utenti possono essere archiviati in AWS e Azure nelle seguenti regioni:

Fornitore di cloud	Regione
AWS	• Asia Pacifico (Sydney) (ap-southeast-2) • Europa (Francoforte) (eu-central-1) • Stati Uniti orientali (Virginia settentrionale) (us-east-1)
Azzurro	Stati Uniti orientali

Requisiti del sistema operativo

Il rilevamento di comportamenti sospetti degli utenti è supportato con i seguenti sistemi operativi:

Sistema operativo	Versioni supportate
AlmaLinux	Da 9.4 (64 bit) a 9.5 (64 bit) e 10 (64 bit), incluso SELinux
CentOS	CentOS Stream 9 (64 bit)
Debian	11 (64 bit), 12 (64 bit), incluso SELinux
OpenSUSE Leap	Da 15.3 (64 bit) a 15.6 (64 bit)
Oracle Linux	8.10 (64 bit) e 9.1 (64 bit) fino a 9.6 (64 bit), incluso SELinux
Cappello rosso	8.10 (64 bit), 9.1 (64 bit) fino a 9.6 (64 bit) e 10 (64 bit), incluso SELinux
Roccioso	Rocky 9.4 (64 bit) fino a 9.6 (64 bit), incluso SELinux
SUSE Enterprise Linux	15 SP4 (64 bit) fino a 15 SP6 (64 bit), incluso SELinux
Ubuntu	20.04 LTS (64 bit), 22.04 LTS (64 bit) e 24.04 LTS (64 bit)

L'ordinateur que vous utilisez pour l'agent d'activité de l'utilisateur ne doit pas exécuter d'autres logiciels au niveau de l'application. Si consiglia un server dedicato.

IL `unzip` il comando è necessario per l'installazione. IL `sudo su -` Il comando è necessario per l'installazione, l'esecuzione degli script e la disinstallazione.

Requisiti del server

Il server deve soddisfare i seguenti requisiti minimi:

- **CPU**: 4 core
- **RAM**: 16 GB di RAM
- **Spazio su disco**: 36 GB di spazio libero su disco

Raccomandazioni per il server

- Assegnare spazio extra sul disco per consentire la creazione del file system. Assicurarsi che ci siano almeno 35 GB di spazio libero nel file system. + Se `/opt` è una cartella montata da un archivio NAS, gli utenti locali devono avere accesso a questa cartella. La creazione dell'agente di attività utente può fallire se gli utenti locali non dispongono delle autorizzazioni necessarie.
- Si consiglia di installare l'agente di attività utente su un sistema separato dall'ambiente Ransomware Resilience. Se si installano entrambi sulla stessa macchina, è necessario prevedere da 50 a 55 GB di spazio su disco. Per Linux, allocare 25-30 GB di spazio a `/opt/netapp` e 25 GB a `var/log/netapp`.
- Si consiglia di sincronizzare l'ora sia sul sistema ONTAP sia sulla macchina dell'agente di attività utente utilizzando il protocollo NTP (Network Time Protocol) o il protocollo SNTP (Simple Network Time Protocol).

Regole di accesso alla rete cloud

Esamina le regole di accesso alla rete cloud per la tua area geografica di riferimento (Asia Pacifico, Europa o Stati Uniti).

Durante l'installazione iniziale, sostituire l' `<site_name>` con un'autorizzazione con carattere jolly (`*`). Dopo che l'agente è attivato e completamente operativo, è possibile sostituire l'autorizzazione con il nome del sito. Contattare il proprio rappresentante NetApp per il nome del sito.

L'agente di attività utente utilizza NetApp Data Insights Infrastructure technology, da cui l'utilizzo di `cloudinsights` endpoints. Per ulteriori informazioni, vedere

Distribuzioni di agenti di attività utente con sede in APAC

Protocollo	Porta	Fonte	Destinazione	Descrizione
HTTPS (TCP)	443	Agente di attività dell'utente	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	Accesso alla resilienza del ransomware

Distribuzioni di agenti di attività utente con sede in Europa

Protocollo	Porta	Fonte	Destinazione	Descrizione
HTTPS (TCP)	443	Agente di attività dell'utente	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accesso alla resilienza del ransomware

Distribuzioni di agenti di attività utente con sede negli Stati Uniti

Protocollo	Porta	Fonte	Destinazione	Descrizione
HTTPS (TCP)	443	Agente di attività dell'utente	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	Accesso alla resilienza del ransomware

Regole in-network

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agente di attività dell'utente	URL del server LDAP	Connettiti a LDAP
HTTPS (TCP)	443	Agente di attività dell'utente	Indirizzo IP di gestione del cluster o SVM (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000 - 55000	Indirizzi IP LIF dei dati SVM	Agente di attività dell'utente	Comunicazione da ONTAP all'agente di attività dell'utente per gli eventi Fpolicy. Queste porte devono essere aperte verso l'agente di attività utente affinché ONTAP possa inviargli eventi, incluso qualsiasi firewall sull'agente di attività utente stesso (se presente). + **NOTA:** Non è necessario riservare **tutte** queste porte, ma le porte riservate a questo scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando 100 porte e di aumentarle se necessario.

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000-55000	IP di gestione del cluster	Agente di attività dell'utente	Comunicazione dall'IP di gestione del cluster ONTAP all'agente di attività dell'utente per **eventi EMS**. Queste porte devono essere aperte verso l'agente di attività utente affinché ONTAP possa inviargli eventi EMS, incluso qualsiasi firewall sull'agente di attività utente stesso. + **NOTA:** Non è necessario riservare **tutte** queste porte, ma le porte riservate a questo scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando 100 porte e di aumentarle se necessario.
SSH	22	Agente di attività dell'utente	Gestione dei cluster	Necessario per il blocco degli utenti CIFS/SMB.

Passaggio successivo

- "Configura gli agenti e i raccoglitori di attività utente"

Configurare agenti e collettori per il rilevamento delle attività degli utenti in NetApp Ransomware Resilience

Per abilitare il rilevamento di comportamenti sospetti degli utenti in NetApp Ransomware Resilience, è necessario installare almeno un agente di attività utente. Quando si attiva la funzionalità di rilevamento di comportamenti sospetti degli utenti dalla dashboard di Ransomware Resilience, è necessario fornire le informazioni sull'host dell'agente di attività utente.

Un agente può ospitare più raccoglitori di dati. I raccoglitori di dati inviano i dati a una posizione SaaS per l'analisi. Esistono due tipi di collezionisti:

- Il **collettore dati** raccoglie i dati sull'attività degli utenti da ONTAP.
- Il **connettore directory utente** si connette alla tua directory per mappare gli ID utente ai nomi utente.

I collettori vengono configurati nelle impostazioni di Resilienza ransomware.

> Se stai già utilizzando NetApp Data Infrastructure Insights (DII) Workload Security, è consigliato utilizzare gli stessi agenti Workload Security per Ransomware Resilience. Non è necessario distribuire agenti Workload Security separati per Ransomware Resilience, tuttavia, l'utilizzo degli stessi agenti Workload Security richiede una relazione di associazione tra l'organizzazione Ransomware Resilience Console e il tenant DII Storage Workload Security. Contatta il tuo rappresentante di account per abilitare questa associazione.

+ Se non stai già utilizzando DII, procedi con le istruzioni di configurazione qui.

Prima di iniziare

- Assicurati di soddisfare i "requisiti del sistema operativo, del server e della rete".

Ruolo Console obbligatorio Per attivare il rilevamento di attività utente sospette, è necessario il ruolo **Organization admin role**. Per le successive configurazioni di attività utente sospette, è necessario il ruolo **Ransomware Resilience user behavior admin role**. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console".

Assicurarsi che ogni ruolo venga applicato a livello di organizzazione.

Creare un agente di attività utente

Gli agenti di attività utente sono ambienti eseguibili per "raccoglitori di dati"; i raccoglitori di dati condividono gli eventi di attività utente con Ransomware Resilience. È necessario creare almeno un agente di attività utente per abilitare il rilevamento di attività utente sospette.

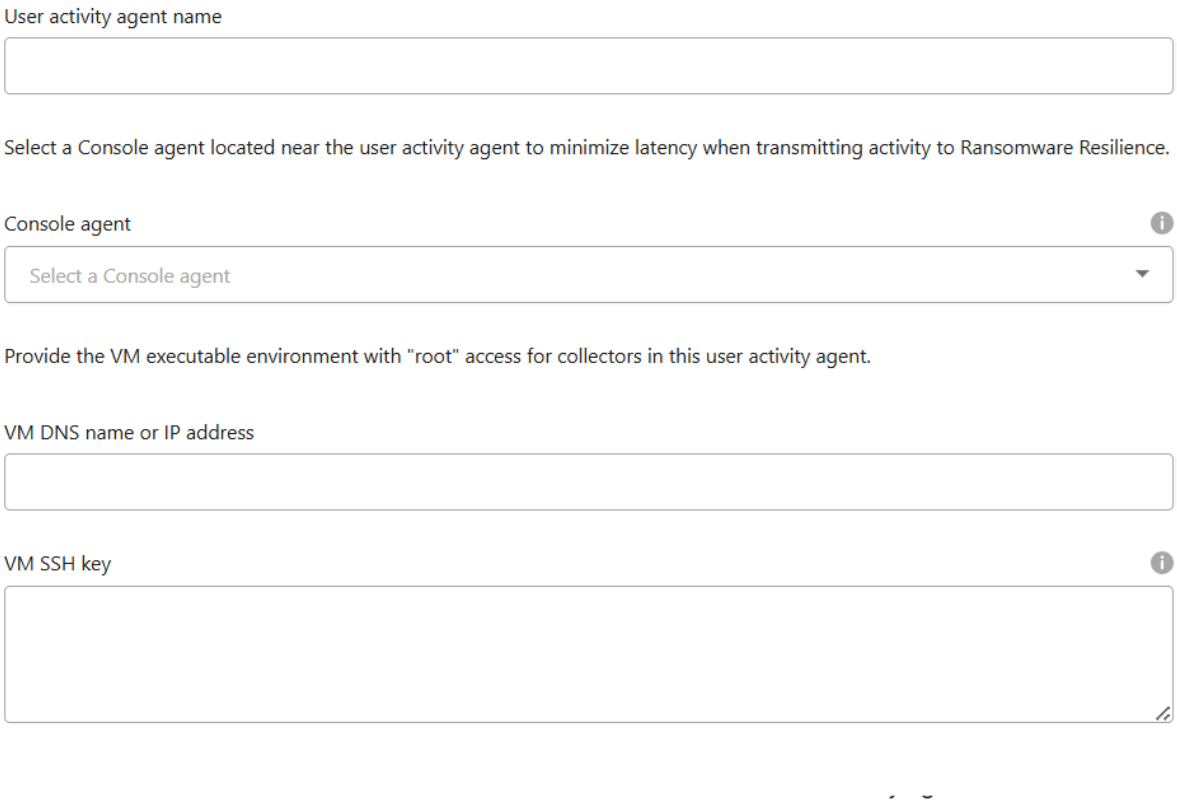
Passi

1. Se è la prima volta che crei un agente di attività utente, vai alla **Dashboard**. Nel riquadro **Attività utente**, seleziona **Attiva**.

   Se vuoi aggiungere un ulteriore agente di attività utente, vai su **Impostazioni**, individua il riquadro **Attività utente**, quindi seleziona **Gestisci**. Nella schermata Attività utente, seleziona la scheda **Agenti attività utente**, quindi **Aggiungi**.

2. Seleziona un **fornitore cloud**, quindi una **regione**. Selezionare **Avanti**.
3. Fornire i dettagli dell'agente di attività dell'utente:
   - **Nome dell'agente di attività dell'utente**
   - **Agente console** - L'agente console deve trovarsi nella stessa rete dell'agente di attività utente e disporre di connettività SSH all'indirizzo IP dell'agente di attività utente.
   - **Nome DNS o indirizzo IP della VM**
   - **Chiave SSH VM** - Inserisci la chiave SSH utilizzando questo formato:

     ```
     -----BEGIN OPENSSH PRIVATE KEY-----
     private-key-contents
     -----END OPENSSH PRIVATE KEY-----
     ```



4. Selezionare **Avanti**.
5. Rivedi le tue impostazioni. Selezionare **Attiva** per completare l'aggiunta dell'agente di attività utente.
6. Conferma che l'agente di attività utente è stato creato correttamente. Nel riquadro Attività utente, una distribuzione riuscita viene visualizzata come **Running**.

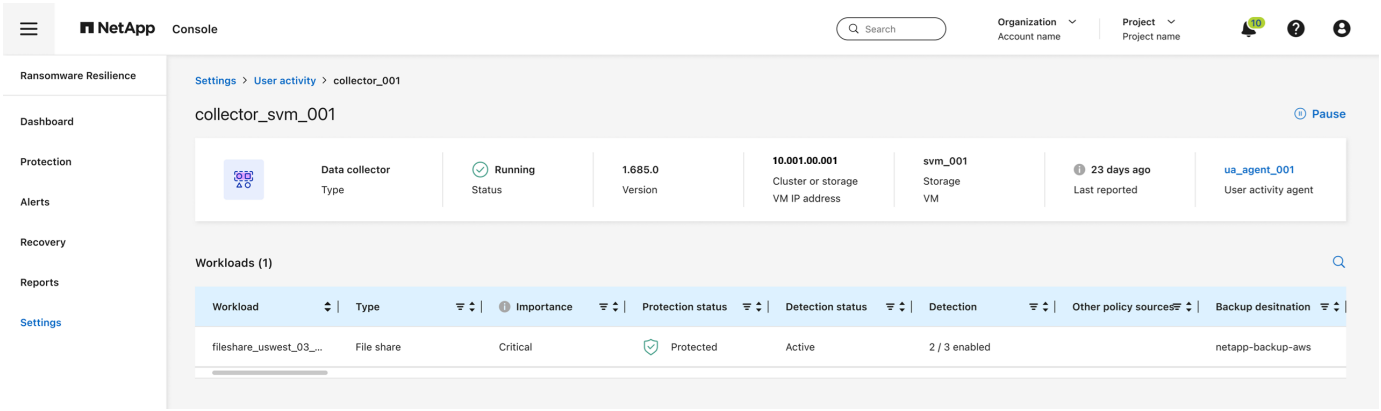
Risultato

Dopo che l'agente di attività utente è stato creato correttamente, torna al menu **Impostazioni** e seleziona **Gestisci** nel riquadro Attività utente. Seleziona la scheda **Agenti di attività utente** e poi seleziona l'agente di attività utente per visualizzare i dettagli relativi, inclusi i collettori di dati e i connettori della directory utente.

Aggiungi un raccoglitore di dati

I collettori di dati vengono creati automaticamente quando si attiva una strategia di protezione dal ransomware con rilevamento delle attività sospette degli utenti. Per maggiori informazioni, vedere aggiungere una politica di rilevamento.

È possibile visualizzare i dettagli del raccoglitore dati. Da Impostazioni, seleziona **Gestisci** nel riquadro Attività utente. Selezionare la scheda **Raccolta dati**, quindi selezionare la raccolta dati per visualizzarne i dettagli o metterla in pausa.



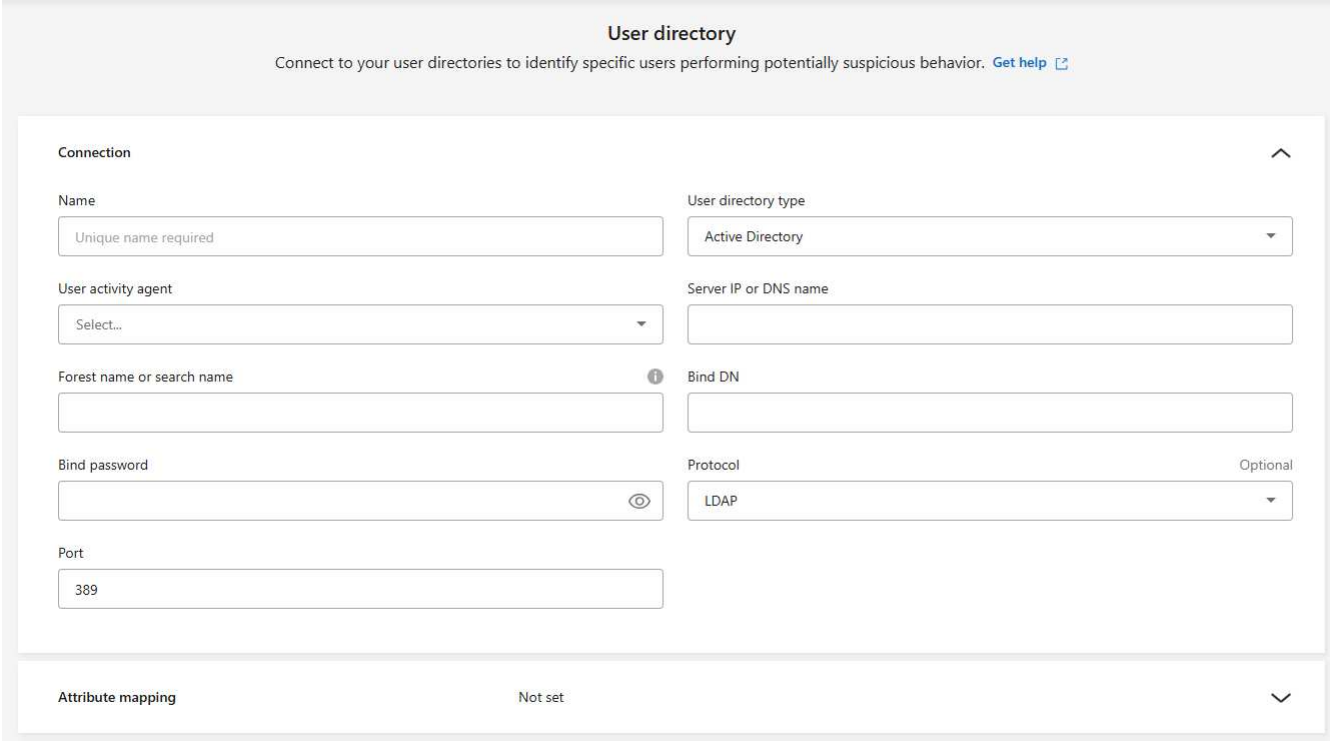
Crea un connettore di directory utente

Per mappare gli ID utente ai nomi utente, è necessario creare un connettore di directory utente.

Passi

1. In Ransomware Resilience, vai su **Impostazioni**.
2. Nel riquadro Attività utente, seleziona **Gestisci**.
3. Selezionare la scheda **Connettori directory utente**, quindi **Aggiungi**.
4. Configurare la connessione. Inserisci le informazioni richieste per ogni campo.

Campo	Descrizione
Nome	Inserisci un nome univoco per il connettore della directory utente
Tipo di directory utente	Il tipo di directory
Indirizzo IP del server o nome di dominio	L'indirizzo IP o il nome di dominio completo (FQDN) del server che ospita la connessione
Nome della foresta o nome della ricerca	È possibile specificare il livello di foresta della struttura della directory come nome di dominio diretto (ad esempio `unit.company.com`) o un insieme di nomi distinti relativi (ad esempio: `DC=unit,DC=company,DC=com`). Puoi anche inserire un `OU` per filtrare per unità organizzativa o per `CN` per limitare a un utente specifico (ad esempio: `CN=user,OU=engineering,DC=unit,DC=company,DC=com`).
LEGA DN	Il BIND DN è un account utente autorizzato a effettuare ricerche nella directory, ad esempio utente@dominio.com. L'utente necessita dell'autorizzazione di sola lettura del dominio.
Password BIND	La password per l'utente fornita in BIND DN
Protocollo	Il campo protocollo è facoltativo. È possibile utilizzare LDAP, LDAPS o LDAP su StartTLS.
Porta	Inserisci il numero di porta scelto



Fornire i dettagli della mappatura degli attributi:

- **Nome da visualizzare**
- **SID** (se si utilizza LDAP)
- **Nome utente**
- **ID Unix** (se stai utilizzando NFS)
- Se selezioni **Includi attributi facoltativi**, puoi anche aggiungere un indirizzo email, un numero di telefono, un ruolo, uno stato, un paese, un reparto, una foto, il nome del responsabile o dei gruppi. Selezionare **Avanzate** per aggiungere una query di ricerca facoltativa.

5. Selezionare **Aggiungi**.
6. Torna alla scheda dei connettori della directory utente per controllare lo stato del connettore della directory utente. Se la creazione avviene correttamente, lo stato del connettore della directory utente viene visualizzato come **In esecuzione**.

Elimina un connettore di directory utente

1. In Ransomware Resilience, vai su **Impostazioni**.
2. Individua il riquadro Attività utente e seleziona **Gestisci**.
3. Selezionare la scheda **Connettore directory utente**.
4. Identifica il connettore della directory utente che desideri eliminare. Nel menu azioni alla fine della riga, seleziona i tre punti ... quindi **Elimina**.
5. Nella finestra di dialogo pop-up, seleziona **Delete** per confermare.

Rispondere agli avvisi di attività sospette degli utenti

Dopo aver configurato il rilevamento delle attività sospette degli utenti, è possibile monitorare gli eventi nella pagina degli avvisi. Per ulteriori informazioni, vedere "Rileva attività dannose e comportamenti sospetti degli

utenti".

[1] Sebbene sia possibile che un attacco passi inosservato, la nostra ricerca indica che la tecnologia NetApp ha portato a un elevato grado di rilevamento per alcuni attacchi ransomware basati sulla crittografia dei file.

Utilizzare la resilienza del ransomware

Monitora lo stato del carico di lavoro utilizzando la dashboard NetApp Ransomware Resilience

La dashboard NetApp Ransomware Resilience fornisce informazioni immediate sullo stato di protezione dei tuoi carichi di lavoro. È possibile determinare rapidamente i carichi di lavoro a rischio o protetti, identificare i carichi di lavoro interessati da un incidente o in fase di ripristino e valutare l'entità della protezione esaminando la quantità di spazio di archiviazione protetto o a rischio.

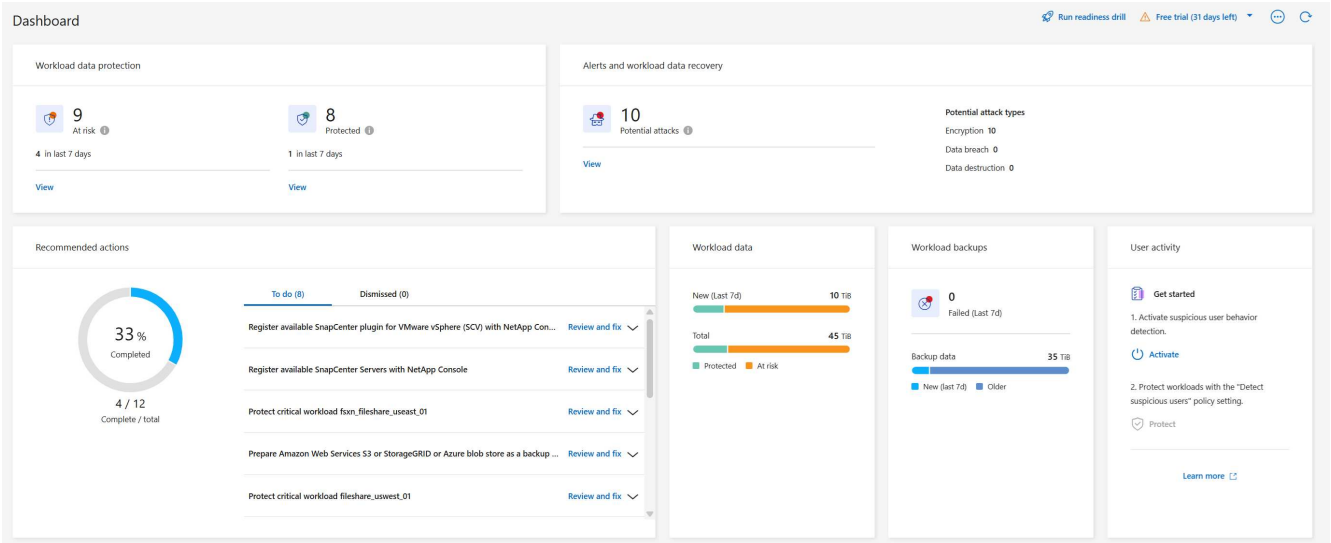
Utilizzare la Dashboard per rivedere i suggerimenti di protezione, modificare le impostazioni e scaricare i report.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Esaminare lo stato del carico di lavoro utilizzando la Dashboard

Passi

1. Dopo che la Console rileva i carichi di lavoro, la dashboard Ransomware Resilience visualizza lo stato di protezione dei dati del carico di lavoro.



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

    - **Protezione dei dati del carico di lavoro**: seleziona **Visualizza tutto** per visualizzare tutti i carichi di lavoro a rischio o protetti nella pagina Protezione. I carichi di lavoro sono a rischio quando i livelli di protezione non corrispondono a una policy di protezione. Fare riferimento a "Proteggere i carichi di lavoro" .

Selezionare il suggerimento "i" per visualizzare suggerimenti su questi dati. Per aumentare il limite del carico di lavoro, seleziona **Aumenta limite del carico di lavoro** all'interno di questa nota. Selezionando questa opzione verrai indirizzato alla pagina di supporto della console, dove potrai creare un ticket di assistenza.

- **Avvisi e ripristino dei dati del carico di lavoro**: seleziona **Visualizza tutto** per visualizzare gli incidenti attivi che hanno avuto un impatto sul tuo carico di lavoro, sono pronti per il ripristino dopo la neutralizzazione degli incidenti o sono in fase di ripristino. Fare riferimento a "Rispondere a un avviso rilevato" .
  - Un incidente è classificato in uno dei seguenti stati:
    - Nuovo
    - Licenziato
    - Licenziamento
    - Risolto
  - Un avviso può avere uno dei seguenti stati:
    - Nuovo
    - Inattivo
  - Un carico di lavoro può avere uno dei seguenti stati di ripristino:
    - Ripristino necessario
    - In corso
    - Restaurato
    - Fallito
- **Azioni consigliate**: per aumentare la protezione, rivedi ogni raccomandazione, quindi seleziona **Rivedi e correggi**.

  Vedere "Esaminare i suggerimenti di protezione sulla Dashboard" O "Proteggere i carichi di lavoro" .

  Ransomware Resilience visualizza per 24 ore i nuovi suggerimenti dall'ultima visita alla Dashboard con il tag "Nuovo". Le azioni vengono visualizzate in ordine di priorità, con la più importante in cima. Esamina, agisci o ignora ogni raccomandazione.

Il numero totale di azioni non include le azioni che hai ignorato.

- **Dati sul carico di lavoro**: monitora le modifiche nella copertura di protezione negli ultimi 7 giorni.
- **Backup del carico di lavoro**: monitora le modifiche nei backup del carico di lavoro creati da Ransomware Resilience che non sono riusciti o sono stati completati correttamente negli ultimi 7 giorni.

Esaminare le raccomandazioni di protezione sulla Dashboard

Ransomware Resilience valuta la protezione dei tuoi carichi di lavoro e consiglia azioni per migliorarla.

È possibile rivedere una raccomandazione e agire di conseguenza, modificando lo stato della raccomandazione in Completata. Oppure, se vuoi agire in seguito, puoi ignorarlo. Quando si ignora un'azione, la raccomandazione viene spostata in un elenco di azioni ignorate, che è possibile rivedere in seguito.

Ecco alcuni esempi di consigli offerti da Ransomware Resilience.

Raccomandazione	Descrizione	Come risolvere
Aggiungere una policy di protezione dal ransomware.	Al momento il carico di lavoro non è protetto.	Assegnare una policy al carico di lavoro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Connettiti al SIEM per la segnalazione delle minacce.	Inviare dati a un sistema di gestione della sicurezza e degli eventi (SIEM) per l'analisi e il rilevamento delle minacce.	Immettere i dettagli del server SIEM/XDR per abilitare il rilevamento delle minacce. Fare riferimento a "Configurare le impostazioni di protezione" .
Abilita la protezione coerente con il carico di lavoro per le applicazioni o VMware.	Questi carichi di lavoro non sono gestiti da SnapCenter Software o SnapCenter Plug-in for VMware vSphere.	Per farli gestire da SnapCenter, abilitare la protezione coerente con il carico di lavoro. Fare riferimento a "Proteggere il carico di lavoro dagli attacchi ransomware" .
Migliorare la sicurezza del sistema	NetApp Digital Advisor ha identificato almeno un rischio per la sicurezza elevato o critico.	Esamina tutti i rischi per la sicurezza in NetApp Digital Advisor. Fare riferimento a "Documentazione Digital Advisor" .
Rendere più forte una politica.	Alcuni carichi di lavoro potrebbero non avere una protezione sufficiente. Rafforza la protezione dei carichi di lavoro con una policy.	Aumenta la conservazione, aggiungi backup, applica backup immutabili, blocca estensioni di file sospette, abilita il rilevamento su storage secondario e molto altro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Preparare <provider di backup> come destinazione di backup per eseguire il backup dei dati del carico di lavoro.	Al momento il carico di lavoro non ha destinazioni di backup.	Aggiungi destinazioni di backup a questo carico di lavoro per proteggerlo. Fare riferimento a "Configurare le impostazioni di protezione" .
Proteggi i carichi di lavoro delle applicazioni critiche o molto importanti dal ransomware.	La pagina Proteggi visualizza i carichi di lavoro delle applicazioni critici o molto importanti (in base al livello di priorità assegnato) che non sono protetti.	Assegnare una policy a questi carichi di lavoro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Proteggi i carichi di lavoro di condivisione file critici o molto importanti dal ransomware.	La pagina Protezione visualizza i carichi di lavoro critici o molto importanti di tipo Condivisione file o Datastore che non sono protetti.	Assegnare una policy a ciascun carico di lavoro. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Registra il plugin SnapCenter disponibile per VMware vSphere (SCV) con la Console	Un carico di lavoro VM non è protetto.	Assegnare una protezione coerente con la VM al carico di lavoro della VM abilitando il plug-in SnapCenter per VMware vSphere. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .

Raccomandazione	Descrizione	Come risolvere
Registra il server SnapCenter disponibile con la console	Un'applicazione non è protetta.	Assegnare una protezione coerente con l'applicazione al carico di lavoro abilitando SnapCenter Server. Fare riferimento a "Proteggere i carichi di lavoro dagli attacchi ransomware" .
Esamina i nuovi avvisi.	Sono presenti nuovi avvisi.	Esamina i nuovi avvisi. Fare riferimento a "Rispondere a un avviso di ransomware rilevato" .

Passi

1. Dal riquadro Azioni consigliate in Ransomware Resilience, seleziona una raccomandazione, quindi **Esamina e correggi**.
2. Per ignorare l'azione e rimandarla a dopo, seleziona **Ignora**.

   La raccomandazione viene eliminata dall'elenco delle cose da fare e visualizzata nell'elenco delle cose ignorate.

   In seguito potrai trasformare un elemento ignorato in un elemento da fare. Quando si contrassegna un elemento come completato o si trasforma un elemento ignorato in un'azione Da fare, il totale delle azioni aumenta di 1.

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

Esporta i dati di protezione in file CSV

È possibile esportare dati e scaricare file CSV che mostrano dettagli su protezione, avvisi e ripristino.

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

- **Protezione**: contiene lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale di carichi di lavoro che Ransomware Resilience contrassegna come protetti o a rischio.
- **Avvisi**: include lo stato e i dettagli di tutti gli avvisi, tra cui il numero totale di avvisi e snapshot automatici.
- **Ripristino**: include lo stato e i dettagli di tutti i carichi di lavoro che devono essere ripristinati, incluso il numero totale di carichi di lavoro che Ransomware Resilience contrassegna come "Ripristino necessario", "In corso", "Ripristino non riuscito" e "Ripristino riuscito".

Scaricando un file CSV da una pagina vengono inclusi solo i dati di quella pagina.

I file CSV includono dati per tutti i carichi di lavoro su tutti i sistemi Console.

Passi

1. Dalla dashboard Ransomware Resilience, seleziona **Aggiorna** opzione in alto a destra per aggiornare i dati che appariranno nei file.
2. Eseguire una delle seguenti operazioni:
   - Dalla pagina, seleziona **Download** opzione.

- Dal menu Ransomware Resilience, seleziona **Report**.

3. Se hai selezionato l'opzione **Report**, seleziona uno dei file preconfigurati con nome, quindi seleziona **Scarica (CSV)** o **Scarica (JSON)**.

Accedi alla documentazione tecnica

È possibile accedere alla documentazione tecnica di Ransomware Resilience da"docs.netapp.com" o dall'interno di Ransomware Resilience.

Passi

1. Dalla dashboard Ransomware Resilience, seleziona la verticale *Azioni*  opzione.
2. Seleziona una di queste opzioni:
   - **Novità** per visualizzare informazioni sulle funzionalità delle versioni attuali o precedenti nelle Note di rilascio.
   - **Documentazione** per visualizzare la documentazione di Ransomware Resilience nella home page e questa documentazione.

Proteggere i carichi di lavoro

Proteggi i carichi di lavoro con le strategie di protezione NetApp Ransomware Resilience

È possibile proteggere i carichi di lavoro dagli attacchi ransomware abilitando una protezione coerente con il carico di lavoro o creando strategie di protezione ransomware in NetApp Ransomware Resilience.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Comprendere le strategie di protezione dal ransomware

Le strategie di protezione dal ransomware comprendono *rilevamento*, *protezione* e *replica*.

- **Le policy di rilevamento** identificano le minacce ransomware
- **Le policy di protezione** includono policy di snapshot e backup. In una strategia di protezione sono necessarie policy di rilevamento e snapshot. Le policy di backup sono facoltative.

  Se utilizzi altri prodotti NetApp per proteggere il tuo carico di lavoro, Ransomware Resilience li rileva e ti offre la possibilità di:

  - utilizzare una policy di rilevamento ransomware e continuare a utilizzare le policy di snapshot e backup create da altri strumenti NetApp , oppure
  - utilizzare Ransomware Resilience per gestire rilevamento, snapshot e backup.
- **I criteri di replica** consentono di replicare gli snapshot da Ransomware Resilience a un sito secondario. Le pianificazioni di replicazione possono essere impostate su frequenze orarie, giornaliere, settimanali o mensili.

Attualmente è possibile replicare gli snapshot solo nell'archiviazione ONTAP locale.

Per una migliore gestione e protezione del tuo patrimonio di dati, puoi creare"condivisioni di file di gruppo" per proteggere collettivamente i volumi con un'unica strategia.

Politiche di protezione con altri servizi gestiti NetApp

Oltre a Ransomware Resilience, è possibile utilizzare i seguenti servizi per gestire la protezione:

- NetApp Backup and Recovery per condivisioni di file, condivisioni di file VM
- SnapCenter per VMware per datastore VM
- SnapCenter per Oracle

Le informazioni sulla protezione da questi servizi vengono visualizzate in Ransomware Resilience. È possibile aggiungere criteri di rilevamento a questi servizi con Ransomware Resilience. L'aggiunta di una policy di protezione con Ransomware Resilience sostituisce le policy di protezione esistenti.

Se una policy di rilevamento ransomware è gestita da Autonomous Ransomware Protection (ARP o ARP/AI, a seconda della versione ONTAP) e FPolicy in ONTAP, tali carichi di lavoro sono protetti e continueranno a essere gestiti da ARP e FPolicy.

Le destinazioni di backup non sono disponibili per i carichi di lavoro in Amazon FSx for NetApp ONTAP. Eseguire operazioni di backup utilizzando il servizio di backup FSx for ONTAP . Le policy di backup per i carichi di lavoro vengono impostate in FSx per ONTAP in AWS, non in Ransomware Resilience. Le policy di backup vengono visualizzate in Ransomware Resilience e rimangono invariate rispetto ad AWS.

Criteri di protezione per carichi di lavoro non protetti dalle applicazioni NetApp

Se il carico di lavoro non è gestito da Backup and Recovery, Ransomware Resilience, SnapCenter o SnapCenter Plug-in for VMware vSphere, potrebbero essere presenti snapshot acquisiti come parte di ONTAP o di altri prodotti. Se è attiva la protezione FPolicy ONTAP , è possibile modificarla utilizzando ONTAP.

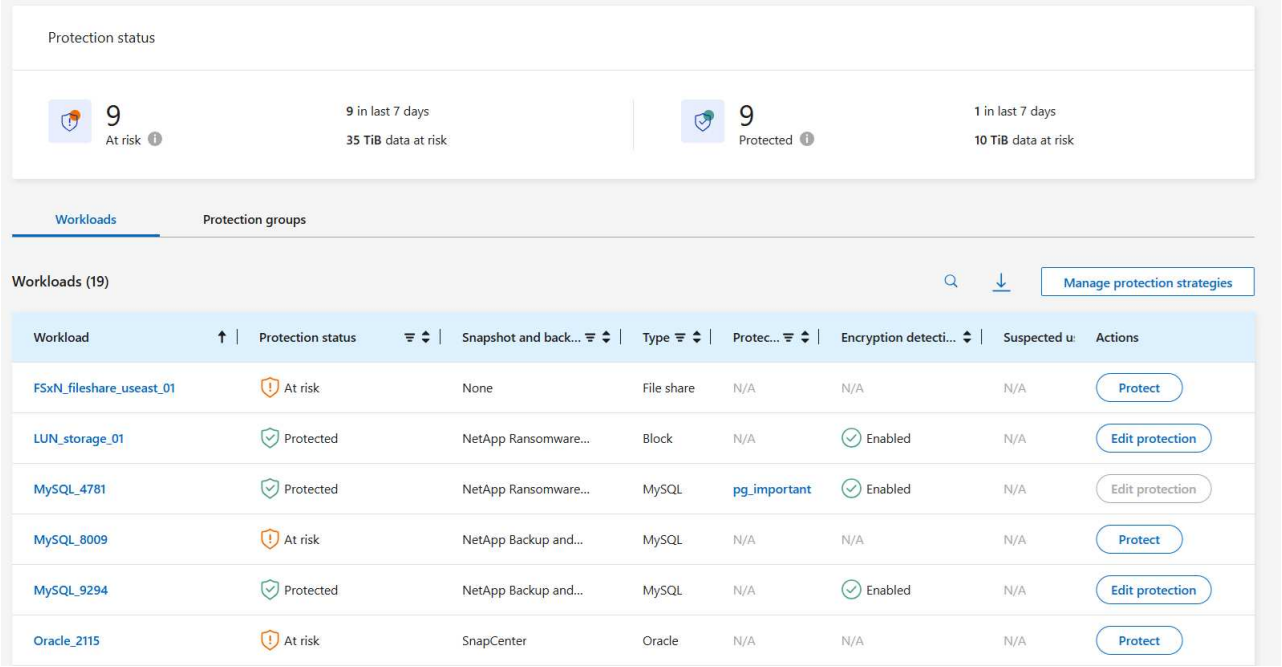
Visualizza la protezione ransomware su un carico di lavoro

Uno dei primi passi per proteggere i carichi di lavoro è visualizzare i carichi di lavoro correnti e il loro stato di protezione. È possibile visualizzare i seguenti tipi di carichi di lavoro:

- Carichi di lavoro applicativi
- Carichi di lavoro a blocchi
- Carichi di lavoro di condivisione file
- Carichi di lavoro VM

Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.
2. Eseguire una delle seguenti operazioni:
   - Dal riquadro Protezione dati nella Dashboard, seleziona **Visualizza tutto**.
   - Dal menu, seleziona **Protezione**.



3. Da questa pagina è possibile visualizzare e modificare i dettagli di protezione per il carico di lavoro.

> Vedere"Aggiungi una strategia di protezione dal ransomware" per scoprire come utilizzare Ransomware Resilience quando è presente una policy di protezione con SnapCenter o Backup and Recovery.

Comprendere la pagina Protezione

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

Stato di protezione: un carico di lavoro può mostrare uno dei seguenti stati di protezione per indicare se una policy è applicata o meno:

- **Protetto**: è stata applicata una policy. ARP (o ARP/AI a seconda della versione ONTAP) è abilitato su tutti i volumi correlati al carico di lavoro.
- **A rischio**: non viene applicata alcuna politica. Se un carico di lavoro non ha un criterio di rilevamento primario abilitato, è "a rischio" anche se ha un criterio di snapshot e backup abilitato.
- **In corso**: una policy è in fase di applicazione ma non è ancora stata completata.
- **Non riuscito**: un criterio è stato applicato ma non funziona.

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

- **Apprendimento**: di recente è stata assegnata una policy di rilevamento ransomware al carico di lavoro e Ransomware Resilience sta eseguendo la scansione dei carichi di lavoro.
- **Attivo**: è assegnata una policy di protezione contro il rilevamento del ransomware.
- **Non impostato**: non è assegnato alcun criterio di protezione contro il rilevamento del ransomware.
- **Errore**: è stato assegnato un criterio di rilevamento ransomware, ma Ransomware Resilience ha riscontrato un errore.

Quando la protezione è abilitata in Ransomware Resilience, il rilevamento degli avvisi e la segnalazione iniziano dopo che lo stato della policy di rilevamento ransomware passa dalla modalità di apprendimento alla modalità attiva.

Le attività sospette relative al comportamento dell'utente e le attività FPolicy (estensioni di file sospette) vengono elencate separatamente dallo stato di rilevamento.

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

Destinazione di replica: se hai configurato la replica degli snapshot, vengono elencati i nomi delle VM e dei sistemi di archiviazione di destinazione. Se non c'è replica, questo campo visualizza "Nessuno".

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

- Gestito da SnapCenter
- Gestito dal SnapCenter Plug-in for VMware vSphere
- Gestito da Backup e Ripristino
- Nome della policy di protezione ransomware che regola gli snapshot e i backup
- Nessuno

Importanza del carico di lavoro

Ransomware Resilience assegna un'importanza o una priorità a ciascun carico di lavoro durante la fase di individuazione, basandosi su un'analisi di ciascun carico di lavoro. L'importanza del carico di lavoro è determinata dalle seguenti frequenze di snapshot:

- **Critico**: vengono eseguite più copie snapshot all'ora (programma di protezione molto aggressivo)
- **Importante**: le copie degli snapshot vengono create meno frequentemente di ogni ora ma più frequentemente di ogni giorno
- **Standard**: le copie snapshot vengono eseguite più di una volta al giorno

Criteri di rilevamento predefiniti

È possibile scegliere una delle seguenti policy predefinite di Ransomware Resilience, in base all'importanza del carico di lavoro.

Il criterio **Estensione utente crittografia** è l'unico criterio predefinito che supporta il rilevamento di comportamenti sospetti degli utenti.

+ La **Criterio di replica critica** è l'unica politica predefinita che supporta la replica degli snapshot su ONTAP.

Livello di politica	Istantanea	Frequenza	Conservazione (giorni)	Numero di copie snapshot	Numero massimo di copie snapshot
Politica sui carichi di lavoro critici	Ogni quarto d'ora	Ogni 15 minuti	3	288	309
	Quotidiano	Ogni 1 giorno	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni	60	2	309
Importante politica sul carico di lavoro	Ogni quarto d'ora	Ogni 30 minuti	3	144	165
	Quotidiano	Ogni 1 giorno	14	14	165
	Settimanale	Ogni 1 settimana	35	5	165
	Mensile	Ogni 30 giorni	60	2	165
Politica standard del carico di lavoro	Ogni quarto d'ora	Ogni 30 minuti	3	72	93
	Quotidiano	Ogni 1 giorno	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93
Estensione utente crittografia	Ogni quarto d'ora	Ogni 30 minuti	3	72	93
	Quotidiano	Ogni 1 giorno	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93

Livello di politica	Istantanea	Frequenza	Conservazione (giorni)	Numero di copie snapshot	Numero massimo di copie snapshot
Estensione utente crittografia	Ogni quarto d'ora	Ogni 30 minuti	3	72	93
	Quotidiano	Ogni 1 giorno	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93
Politica di replicazione critica	Ogni quarto d'ora	Ogni 15 minuti	3	288	309
	Quotidiano	Ogni 1 giorno	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni	60	2	309

Abilita la protezione coerente con l'applicazione o la VM con SnapCenter

Abilitando la protezione coerente con l'applicazione o la macchina virtuale, è possibile proteggere i carichi di lavoro dell'applicazione o della macchina virtuale in modo coerente, ottenendo uno stato di quiescenza e coerenza per evitare potenziali perdite di dati in un secondo momento, qualora fosse necessario un ripristino.

Questo processo avvia la registrazione di SnapCenter Software Server per le applicazioni o SnapCenter Plug-in for VMware vSphere per le VM che utilizzano Backup e Ripristino.

Dopo aver abilitato la protezione coerente con il carico di lavoro, puoi gestire le strategie di protezione in Ransomware Resilience. La strategia di protezione include le policy di snapshot e backup gestite altrove, insieme a una policy di rilevamento ransomware gestita in Ransomware Resilience.

Per informazioni sulla registrazione SnapCenter o SnapCenter Plug-in for VMware vSphere tramite Backup e ripristino, fare riferimento alle seguenti informazioni:

- "Registra il software SnapCenter Server"
- "Registra il SnapCenter Plug-in for VMware vSphere"

Passi

1. Dal menu Ransomware Resilience, seleziona **Dashboard**.
2. Dal riquadro Raccomandazioni, individua una delle seguenti raccomandazioni e seleziona **Rivedi e correggi**:
   - Registra SnapCenter Server disponibile con la NetApp Console
   - Registra il SnapCenter Plug-in for VMware vSphere (SCV) con la NetApp Console
3. Seguire le informazioni per registrare SnapCenter o SnapCenter Plug-in for VMware vSphere tramite

Backup e ripristino.

4. Ritorno alla resilienza del ransomware.
5. Da Ransomware Resilience, vai alla Dashboard e avvia nuovamente il processo di individuazione.
6. Da Ransomware Resilience, seleziona **Protezione** per visualizzare la pagina Protezione.
7. Esaminare i dettagli nella colonna delle policy di snapshot e backup nella pagina Protezione per verificare che le policy siano gestite altrove.

Aggiungi una strategia di protezione dal ransomware

Esistono tre approcci per aggiungere una strategia di protezione dal ransomware:

- **Creare una strategia di protezione dal ransomware se non si dispone di policy di snapshot o backup.**

  La strategia di protezione dal ransomware include:

  - Politica di snapshot
  - Criterio di rilevamento del ransomware
  - Politica di backup
- **Sostituisci le policy di snapshot o backup esistenti di SnapCenter o la protezione di Backup e Recovery con strategie di protezione gestite da Ransomware Resilience.**

  La strategia di protezione dal ransomware include:

  - Politica di snapshot
  - Criterio di rilevamento del ransomware
  - Politica di backup
- **Creare una policy di rilevamento per i carichi di lavoro con policy di snapshot e backup esistenti gestite in altri prodotti o servizi NetApp .**

  La policy di rilevamento non modifica le policy gestite in altri prodotti.

  La policy di rilevamento abilita la protezione autonoma contro i ransomware e la protezione FPolicy se sono già attivate in altri servizi. Scopri di più su"Protezione autonoma dal ransomware" ,"Backup e ripristino" , E"Politica ONTAP" .

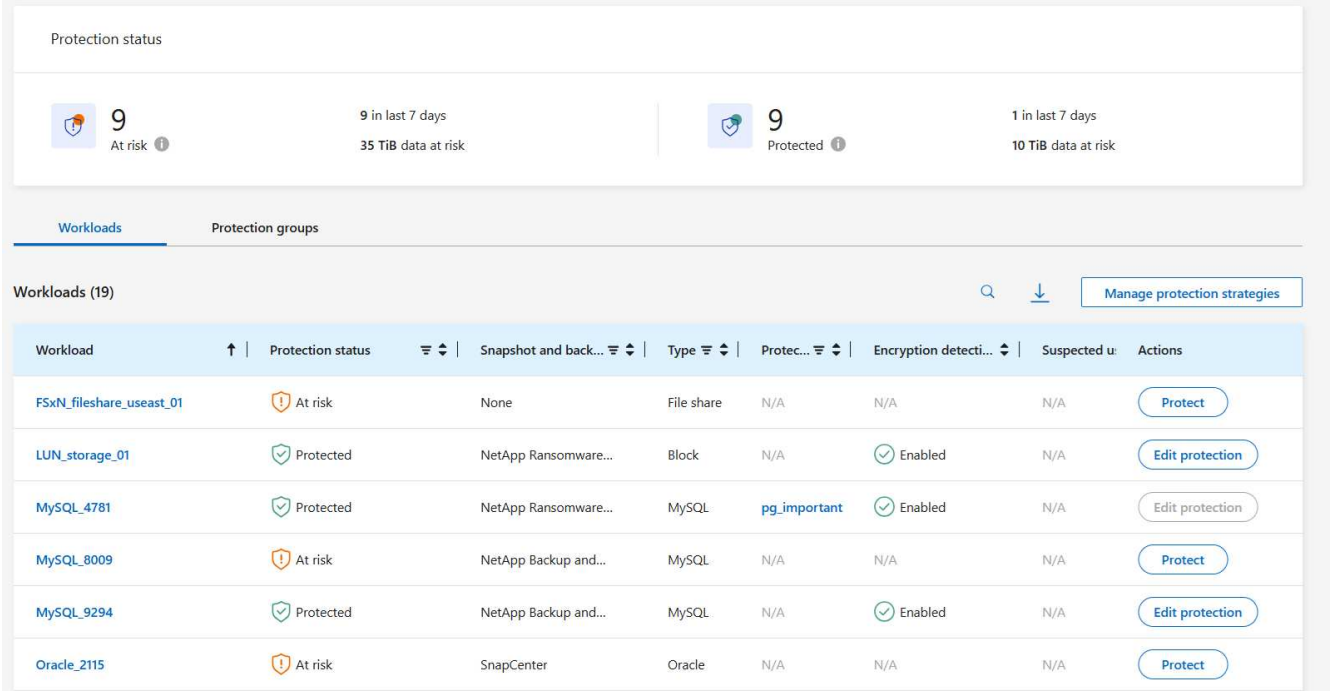
Creare una strategia di protezione dal ransomware (se non si dispone di snapshot o policy di backup)

Se nel carico di lavoro non sono presenti policy di snapshot o backup, è possibile creare una strategia di protezione dal ransomware, che può includere le seguenti policy create in Ransomware Resilience:

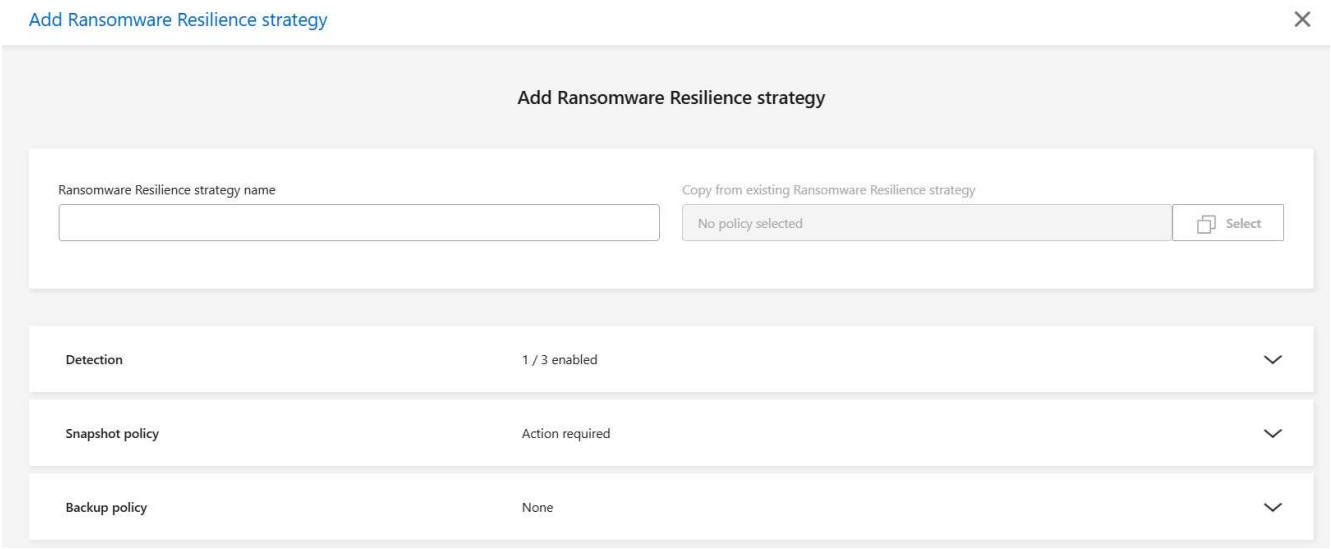
- Politica di snapshot
- Politica di backup
- Criterio di rilevamento del ransomware
- Replicazione secondaria a ONTAP

Passaggi per creare una strategia di protezione dal ransomware

1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona un carico di lavoro, quindi **Proteggi**.
3. Nella pagina Strategie di protezione dal ransomware, seleziona **Aggiungi**.



4. Inserisci un nuovo nome per la strategia oppure inserisci un nome esistente per copiarlo. Se inserisci un nome esistente, scegli quale copiare e seleziona **Copia**.

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

5. Per ogni elemento, seleziona la **freccia giù**.
   - **Politica di rilevamento**:
     - **Criterio**: scegliere uno dei criteri di rilevamento predefiniti.

        - **Rilevamento primario**: abilita Ransomware Resilience per rilevare potenziali attacchi ransomware.
        - **Rilevamento del comportamento sospetto dell'utente**: abilita il rilevamento del comportamento dell'utente per trasmettere gli eventi delle attività dell'utente a Ransomware Resilience e rilevare eventi sospetti, come violazioni dei dati.
        - **Blocca estensioni file**: abilita Ransomware Resilience per bloccare le estensioni di file sospette note. Ransomware Resilience esegue automaticamente copie snapshot quando il rilevamento primario è abilitato.

          Se si desidera modificare le estensioni dei file bloccati, modificarle in Gestione sistema.

    - **Politica di snapshot**:
        - **Nome base policy snapshot**: seleziona una policy oppure seleziona **Crea** e inserisci un nome per la policy snapshot.
        - **Blocco snapshot**: abilita questa opzione per bloccare le copie snapshot sull'archiviazione primaria in modo che non possano essere modificate o eliminate per un determinato periodo di tempo, anche se un attacco ransomware riesce a raggiungere la destinazione dell'archiviazione di backup. Questo è anche chiamato *archiviazione immutabile*. Ciò consente tempi di ripristino più rapidi.

          Quando uno snapshot è bloccato, la data di scadenza del volume viene impostata sulla data di scadenza della copia dello snapshot.

    Il blocco della copia snapshot è disponibile con ONTAP 9.12.1 e versioni successive. Per saperne di più su SnapLock, fare riferimento a "SnapLock in ONTAP" .

    - **Pianificazioni snapshot**: scegli le opzioni di pianificazione, il numero di copie snapshot da conservare e seleziona per abilitare la pianificazione.
        - **Politica di replicazione**:
    - **Nome base della policy di replicazione**: immettere un nuovo nome o sceglierne uno esistente. Il nome base è il prefisso aggiunto a tutti gli snapshot.
    - **Pianificazioni di replicazione**: attiva/disattiva le frequenze che desideri abilitare (oraria, giornaliera, settimanale o mensile) e imposta il valore di conservazione (il numero di snapshot replicati da conservare) per ogni pianificazione abilitata.
        - **Politica di backup**:
    - **Nome base della policy di backup**: inserisci un nuovo nome o scegline uno esistente.
    - **Pianificazioni di backup**: scegli le opzioni di pianificazione per l'archiviazione secondaria e abilita la pianificazione.

    Per abilitare il blocco del backup sull'archiviazione secondaria, configura le destinazioni di backup utilizzando l'opzione **Impostazioni**. Per maggiori dettagli, vedere "Configurare le impostazioni" .

6. Selezionare **Aggiungi**.

Aggiungere un criterio di rilevamento ai carichi di lavoro con criteri di snapshot e backup esistenti gestiti da SnapCenter o Backup and Recovery

Ransomware Resilience consente di assegnare una policy di rilevamento o una policy di protezione ai carichi di lavoro con protezione snapshot e backup esistente gestita in altri prodotti o servizi NetApp . Altri servizi, come Backup and Recovery e SnapCenter, utilizzano policy che regolano gli snapshot, la replica su storage

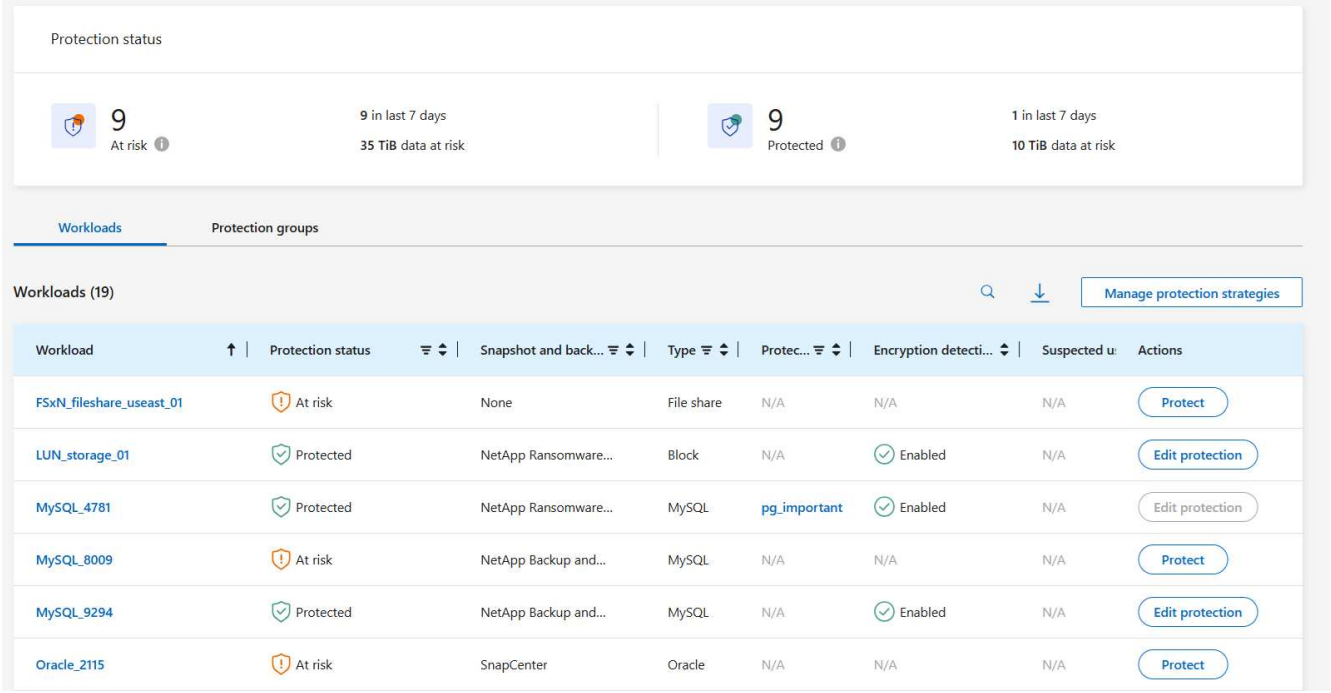
secondario o i backup su storage di oggetti.

Aggiungere una policy di rilevamento ai carichi di lavoro con policy di backup o snapshot esistenti

Se disponi di policy di snapshot o backup esistenti con Backup and Recovery o SnapCenter, puoi aggiungere una policy per rilevare gli attacchi ransomware. Per gestire la protezione e il rilevamento con Ransomware Resilience, vedereProteggiti con la resilienza del ransomware .

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona un carico di lavoro, quindi seleziona **Proteggi**.
3. Ransomware Resilience rileva se sono presenti policy SnapCenter o Backup and Recovery attive.
4. Per mantenere in vigore i criteri di Backup e ripristino o SnapCenter esistenti e applicare solo un criterio di *rilevamento*, lasciare deselezionata la casella **Sostituisci criteri esistenti**.
5. Per visualizzare i dettagli delle policy SnapCenter , seleziona la **freccia giù**.
6. Seleziona le impostazioni di rilevamento desiderate: **Rilevamento crittografia Rilevamento comportamento utente sospetto Blocca estensioni di file sospette**
7. Selezionare **Avanti**.
8. Se hai selezionato **Rilevamento comportamento utente sospetto** come impostazione di rilevamento, seleziona l'agente Attività utente o "o crearne uno".

   L'agente di attività utente ospita i nuovi collettori di dati. Ransomware Resilience crea automaticamente il raccoglitore dati per trasmettere gli eventi di attività dell'utente a Ransomware Resilience per rilevare comportamenti anomali dell'utente.

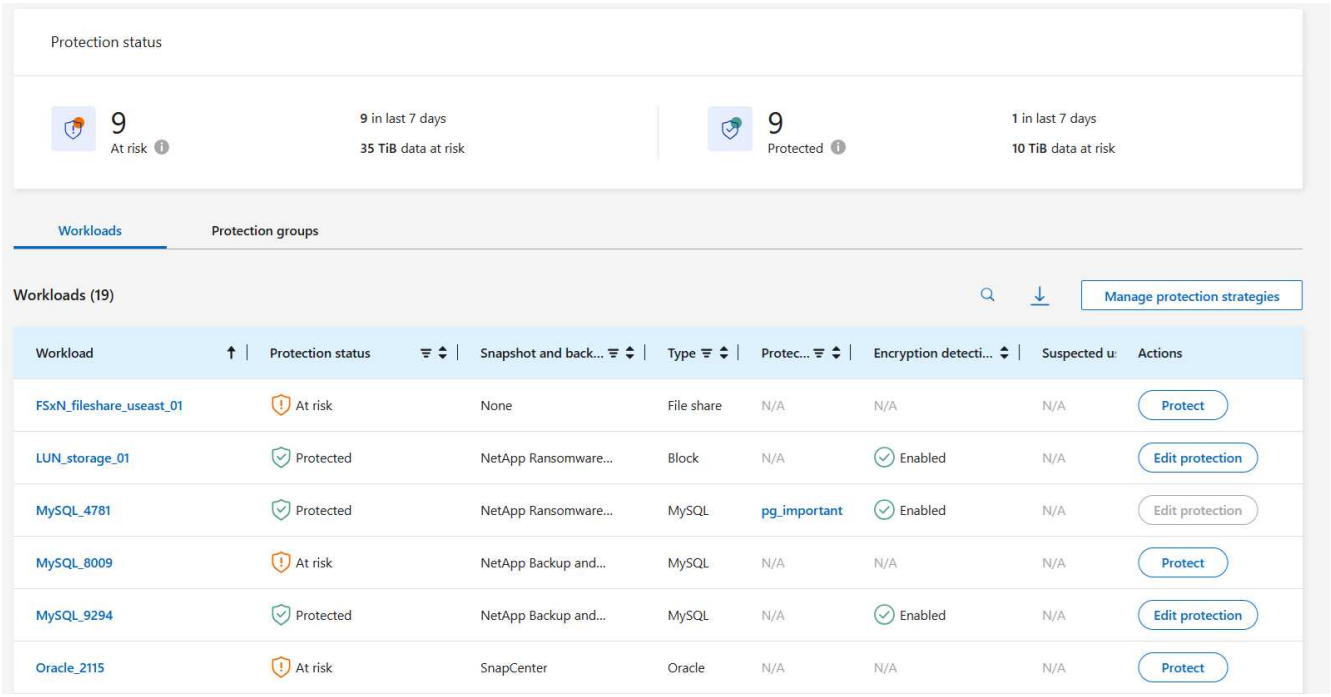
9. Selezionare **Avanti**.
10. Rivedi le tue scelte. Selezionare **Crea** per attivare il rilevamento.
11. Nella pagina Protezione, controlla lo **Stato di rilevamento** per confermare che il rilevamento sia Attivo.

Sostituisci le policy di backup o snapshot esistenti con una strategia di protezione dal ransomware

È possibile sostituire le policy di backup o snapshot esistenti con una strategia di protezione dal ransomware. Questo approccio rimuove la protezione gestita esternamente e configura il rilevamento e la protezione in Ransomware Resilience.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona un carico di lavoro, quindi seleziona **Proteggi**.
3. Ransomware Resilience rileva se sono presenti policy attive di Backup e Recovery o SnapCenter . Per sostituire i criteri di Backup e ripristino o SnapCenter esistenti, selezionare la casella **Sostituisci criteri esistenti**. Selezionando la casella, Ransomware Resilience sostituisce l'elenco dei criteri di rilevamento con i criteri di rilevamento.
4. Scegli una polizza di protezione. Se non esiste alcuna policy di protezione, seleziona **Aggiungi** per crearne una nuova. Per informazioni sulla creazione di una policy, vedereCreare una politica di protezione . Selezionare **Avanti**.
5. Se la strategia prevede la replica, selezionare **Sistema di destinazione** e **VM di archiviazione di destinazione**. Selezionare **Avanti**.
6. Seleziona una destinazione di backup o creane una nuova. Selezionare **Avanti**.
   a. Se la strategia di protezione prevede il rilevamento del comportamento dell'utente, selezionare un agente di attività utente nel proprio ambiente per ospitare i nuovi raccoglitori di dati. Ransomware Resilience crea automaticamente il raccoglitore dati per trasmettere gli eventi di attività dell'utente a Ransomware Resilience per rilevare comportamenti anomali dell'utente.
7. Esaminare la nuova strategia di protezione, quindi selezionare **Proteggi** per applicarla.
8. Nella pagina Protezione, controlla lo **Stato di rilevamento** per confermare che il rilevamento sia Attivo.

Assegna una politica diversa

È possibile sostituire la policy esistente con una diversa.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, nella riga del carico di lavoro, seleziona **Modifica protezione**.
3. Se il carico di lavoro ha una policy di Backup e ripristino o SnapCenter esistente che si desidera mantenere, deselezionare **Sostituisci policy esistenti**. Per sostituire le policy esistenti, seleziona **Sostituisci policy esistenti**.
4. Nella pagina Criteri, seleziona la freccia rivolta verso il basso per il criterio che desideri assegnare per esaminarne i dettagli.
5. Seleziona la policy che vuoi assegnare.
6. Selezionare **Proteggi** per completare la modifica.

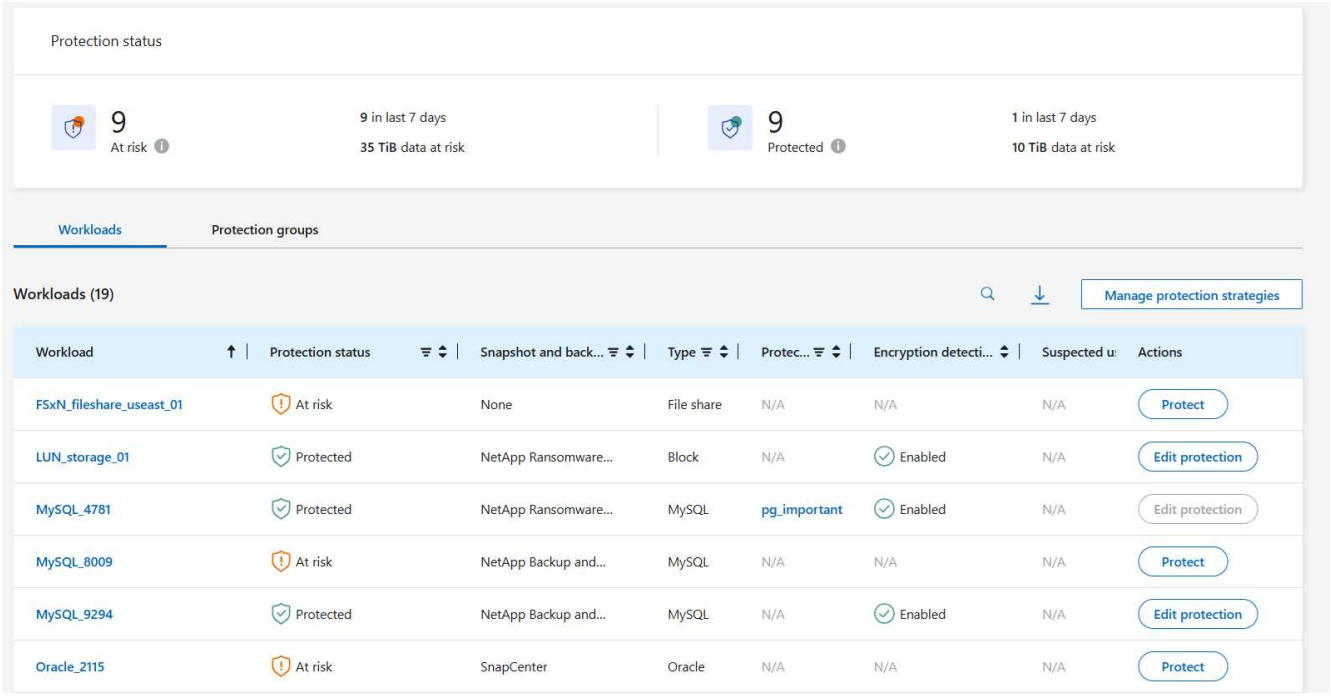
Crea un gruppo di protezione

Raggruppare le condivisioni file in un gruppo di protezione semplifica la protezione del patrimonio di dati. Ransomware Resilience può proteggere tutti i volumi di un gruppo contemporaneamente, anziché proteggere ciascun volume separatamente.

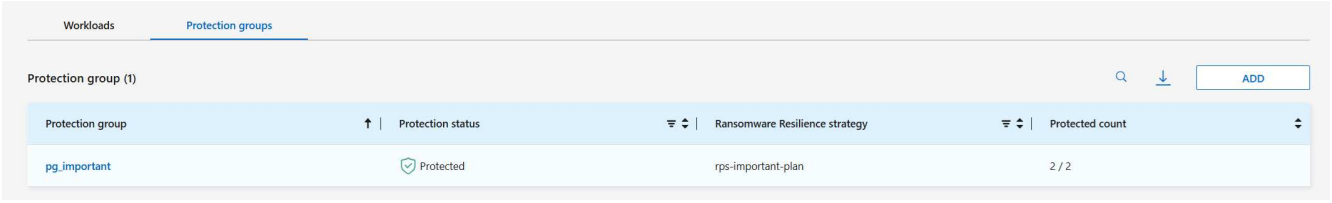
È possibile creare gruppi indipendentemente dal loro stato di protezione (ovvero gruppi non protetti e gruppi protetti). Quando si aggiunge un criterio di protezione a un gruppo di protezione, il nuovo criterio di protezione sostituisce tutti i criteri esistenti, compresi quelli gestiti da SnapCenter e NetApp Backup and Recovery.

Passi

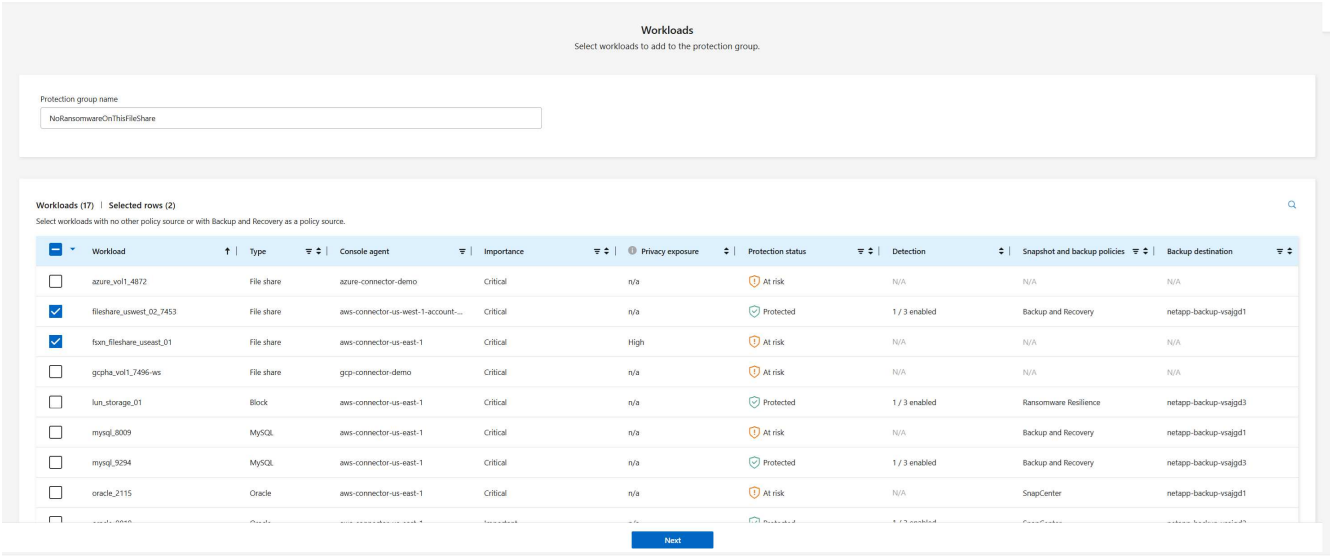
1. Dal menu Ransomware Resilience, seleziona **Protezione**.



2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**.



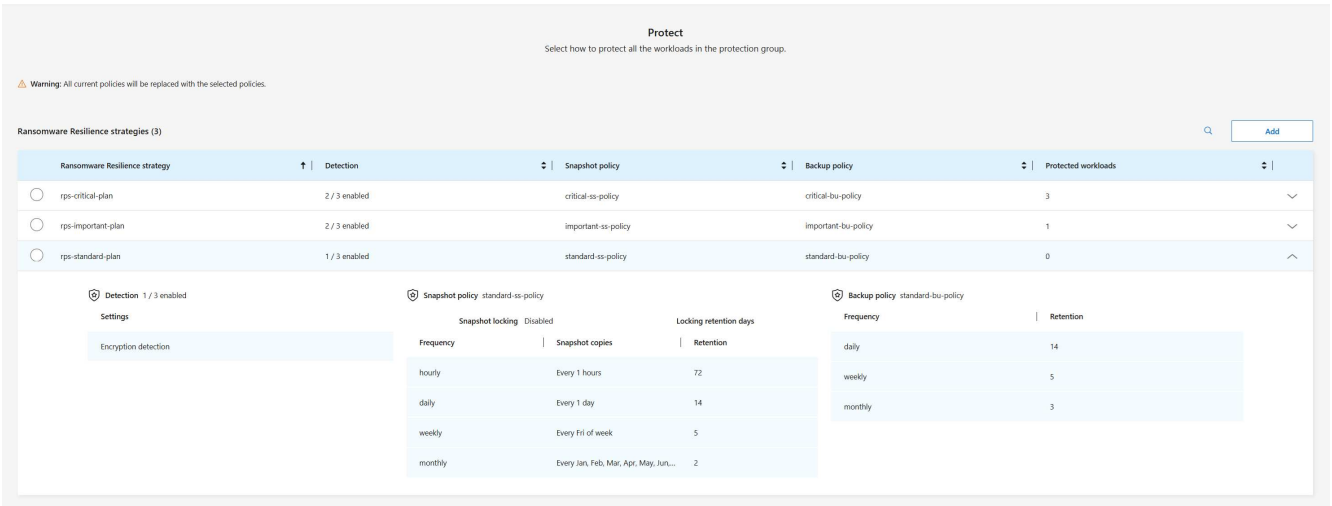
3. Selezionare **Aggiungi**.



4. Immettere un nome per il gruppo di protezione.
5. Seleziona i carichi di lavoro da aggiungere al gruppo.

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

6. Selezionare **Avanti**.



7. Selezionare il criterio per gestire la protezione di questo gruppo. Per confermare, selezionare **Avanti**.
8. Se la strategia di protezione include la replica, rivedere le impostazioni di replica.
   a. Per replicare tutti gli snapshot nella stessa destinazione, seleziona **Usa la stessa destinazione per ogni carico di lavoro**. Selezionare un **Sistema di destinazione** e una **VM di archiviazione di**

destinazione per i carichi di lavoro nella sezione Agente console. + Per utilizzare destinazioni diverse, deselezionare la casella. Esaminare ciascun carico di lavoro in ciascun agente della console e assegnare un **Sistema di destinazione** e una **VM di archiviazione di destinazione** per ciascun carico di lavoro. Selezionare **Avanti**.

9. Per configurare un criterio di backup, selezionarne uno, quindi selezionare **Avanti**.
10. Se la policy di rilevamento include il rilevamento del comportamento dell'utente, seleziona il raccoglitore dati che desideri utilizzare, quindi **Avanti**.
11. Rivedere le selezioni per il gruppo di protezione.
12. Per finalizzare la creazione del gruppo di protezione, selezionare **Aggiungi**.

Modifica protezione gruppo

È possibile modificare i criteri di rilevamento per un gruppo esistente.

Passi

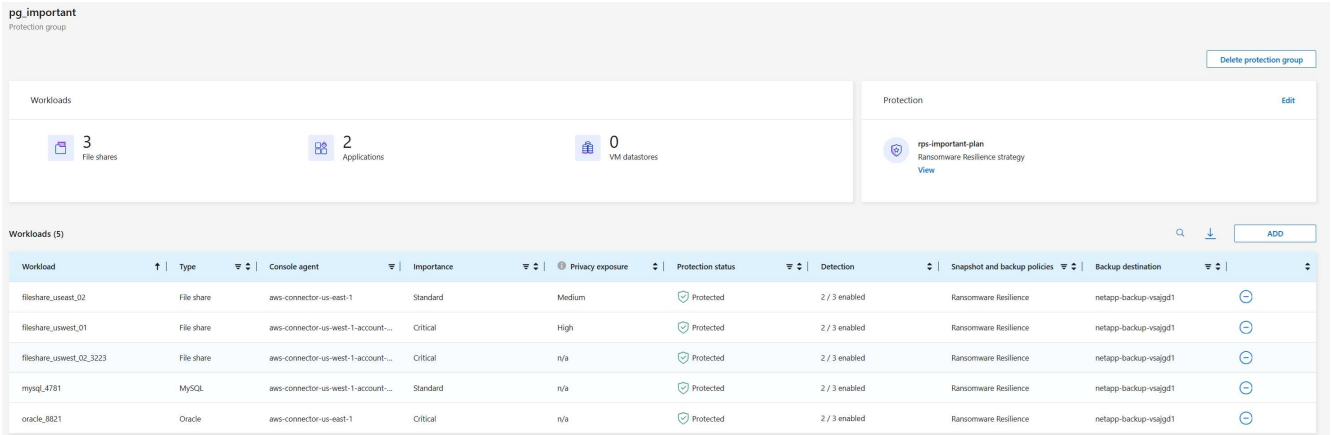
1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**, quindi seleziona il gruppo di cui desideri modificare la policy.
3. Dalla pagina di panoramica del gruppo di protezione, seleziona **Modifica protezione**.
4. Selezionare un criterio di protezione esistente da applicare oppure selezionare **Aggiungi** per creare un nuovo criterio di protezione. Per ulteriori informazioni sull'aggiunta di una policy di protezione, vedere,Creare una politica di protezione . Quindi seleziona **Salva**.
5. Nella panoramica della destinazione di backup, seleziona una destinazione di backup esistente oppure **Aggiungi una nuova destinazione di backup**.
6. Seleziona **Avanti** per rivedere le modifiche.

Rimuovere carichi di lavoro da un gruppo

Potrebbe essere necessario in seguito rimuovere carichi di lavoro da un gruppo esistente.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**.
3. Seleziona il gruppo da cui desideri rimuovere uno o più carichi di lavoro.



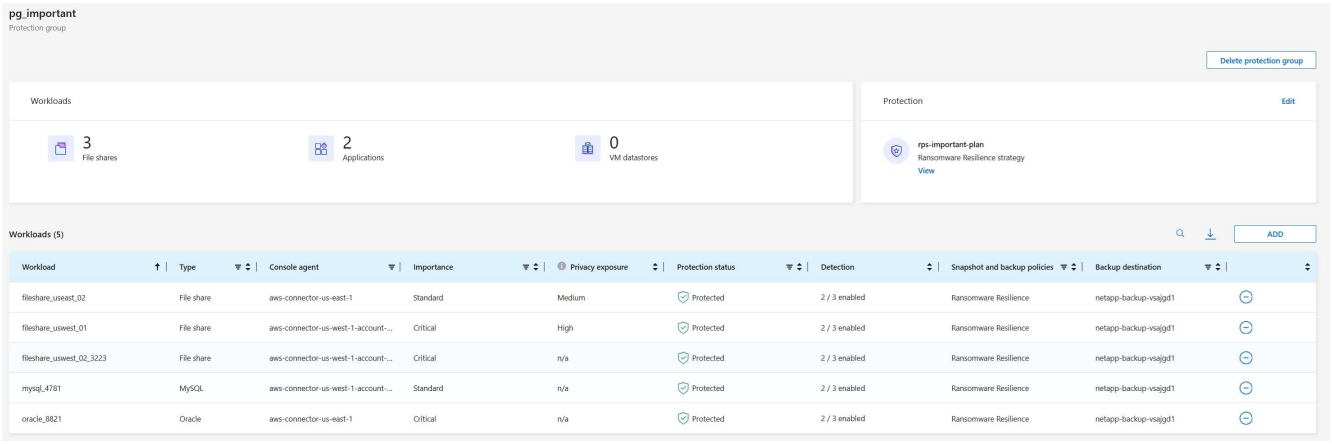
4. Dalla pagina del gruppo di protezione selezionato, seleziona il carico di lavoro che desideri rimuovere dal gruppo e seleziona *Azioni* opzione.
5. Dal menu Azioni, seleziona **Rimuovi carico di lavoro**.
6. Conferma di voler rimuovere il carico di lavoro e seleziona **Rimuovi**.

Elimina il gruppo di protezione

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

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Dalla pagina Protezione, seleziona la scheda **Gruppi di protezione**.
3. Seleziona il gruppo da cui desideri rimuovere uno o più carichi di lavoro.



4. Nella pagina del gruppo di protezione selezionato, in alto a destra, seleziona **Elimina gruppo di protezione**.
5. Conferma di voler eliminare il gruppo e seleziona **Elimina**.

Gestire le strategie di protezione dal ransomware

È possibile eliminare una strategia ransomware.

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

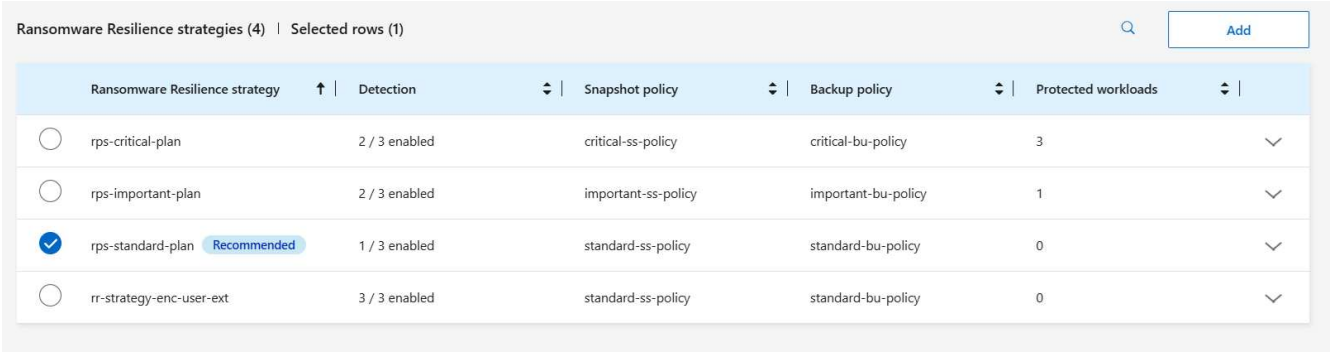
Prima di eliminare una strategia di protezione ransomware, potrebbe essere opportuno verificare quali carichi di lavoro sono protetti da tale strategia.

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

Passaggi per visualizzare le strategie

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, seleziona **Gestisci strategie di protezione**.

   La pagina Strategie di protezione dal ransomware mostra un elenco di strategie.



3. Nella pagina Strategie di protezione ransomware, nella colonna Carichi di lavoro protetti, seleziona la freccia rivolta verso il basso alla fine della riga.

Eliminare una strategia di protezione ransomware

È possibile eliminare una strategia di protezione che al momento non è associata ad alcun carico di lavoro.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, seleziona **Gestisci strategie di protezione**.
3. Nella pagina Gestisci strategie, seleziona *Azioni* ••• opzione per la strategia che vuoi eliminare.
4. Dal menu Azioni, seleziona **Elimina criterio**.

Scansiona le informazioni di identificazione personale con NetApp Data Classification in Ransomware Resilience

All'interno di NetApp Ransomware Resilience, puoi utilizzare NetApp Data Classification per analizzare e classificare i dati in un carico di lavoro di condivisione file. La classificazione dei dati aiuta a determinare se il set di dati include informazioni di identificazione personale (PII), che possono aumentare i rischi per la sicurezza. Data Classification è un componente fondamentale della NetApp Console ed è disponibile senza costi aggiuntivi.

"Classificazione dei dati"utilizza l'elaborazione del linguaggio naturale basata sull'intelligenza artificiale per l'analisi e la categorizzazione dei dati contestuali, fornendo informazioni fruibili sui dati per soddisfare i requisiti di conformità, rilevare vulnerabilità di sicurezza, ottimizzare i costi e accelerare la migrazione.

Questo processo può influire sull'importanza del carico di lavoro per garantire la protezione adeguata.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Identificare l'esposizione alla privacy con la classificazione dei dati

Prima di utilizzare la classificazione dei dati all'interno di Ransomware Resilience, è necessario"per abilitare la classificazione dei dati per analizzare i tuoi dati" .

È possibile implementare la classificazione dei dati nella pagina Protezione di Ransomware Resilience.

Seguire la procedura per identificare l'esposizione alla privacy. Quando selezioni **Identifica esposizione**, se non hai ancora implementato la classificazione dei dati, una finestra di dialogo ti consente di abilitarla.

Per ulteriori informazioni sulla classificazione dei dati, vedere:

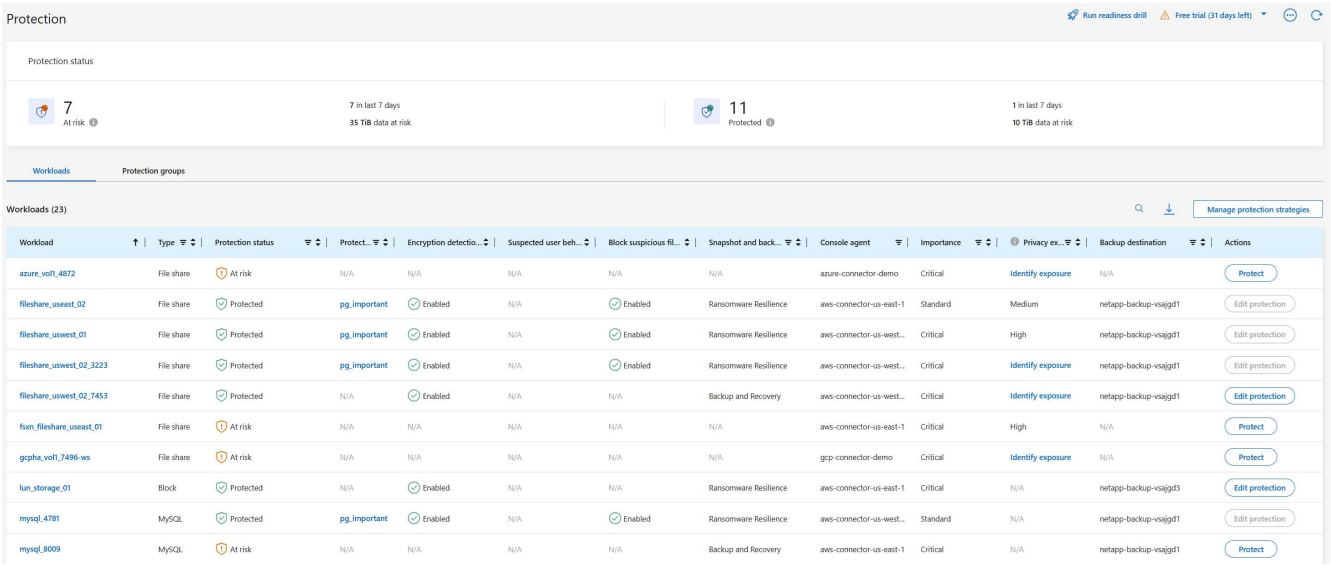
- "Scopri di più sulla classificazione dei dati"
- "Categorie di dati privati"
- "Esamina i dati archiviati nella tua organizzazione"

Prima di iniziare

La scansione dei dati PII in Ransomware Resilience è disponibile se hai"Classificazione dei dati distribuita" . La classificazione dei dati è disponibile come parte della Console senza costi aggiuntivi e può essere distribuita in locale o nel cloud del cliente.

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, individua un carico di lavoro di condivisione file nella colonna Carico di lavoro.



3. Per consentire alla Classificazione dei dati di analizzare i dati alla ricerca di informazioni personali identificabili (PII), nella colonna **Esposizione alla privacy**, selezionare **Identifica esposizione**.

> Se non hai distribuito Data CCasification, selezionando **Identifica esposizione** si apre una finestra di dialogo per distribuire Data Classification. Selezionare **Distribuisci**. Dopo aver implementato la classificazione dei dati, puoi tornare alla pagina Protezione e selezionare **Identifica esposizione**.

Risultato

La scansione può richiedere diversi minuti, a seconda delle dimensioni e del numero dei file. Durante la scansione, la pagina Protezione indica che sta identificando i file e ne fornisce il conteggio. Una volta completata la scansione, la colonna Esposizione privacy classifica il livello di esposizione come Basso, Medio o Alto.

Esaminare l’esposizione alla privacy

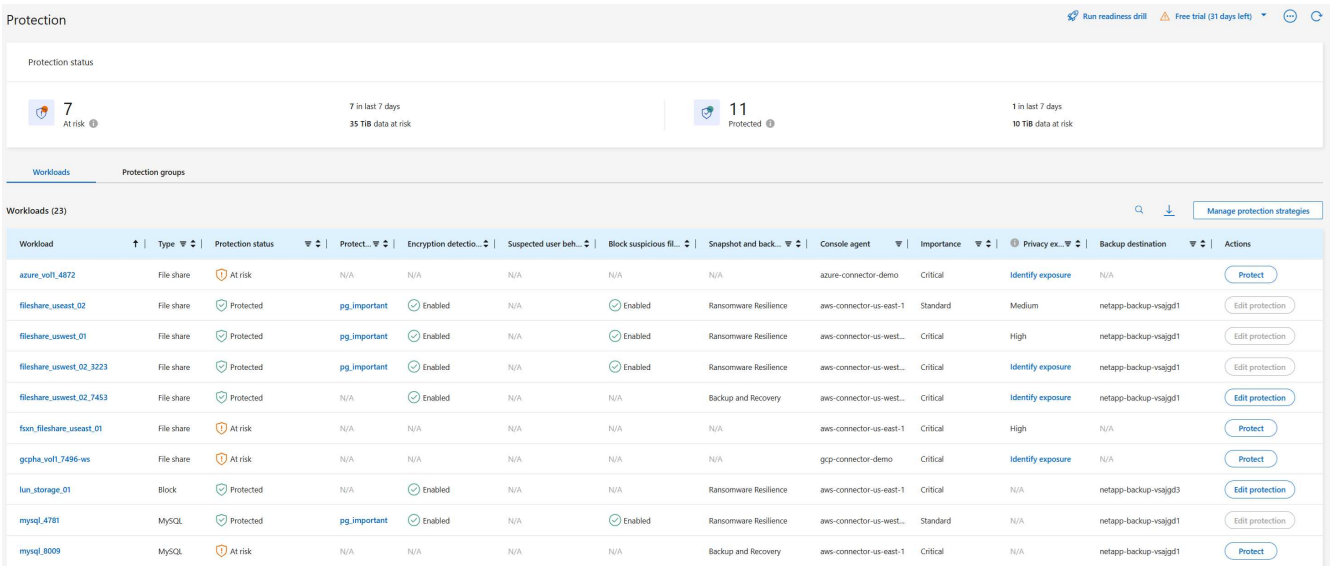
Dopo aver eseguito le scansioni di classificazione dei dati per individuare le informazioni personali identificabili, valutare il rischio.

I dati PII sono classificati in una delle tre designazioni:

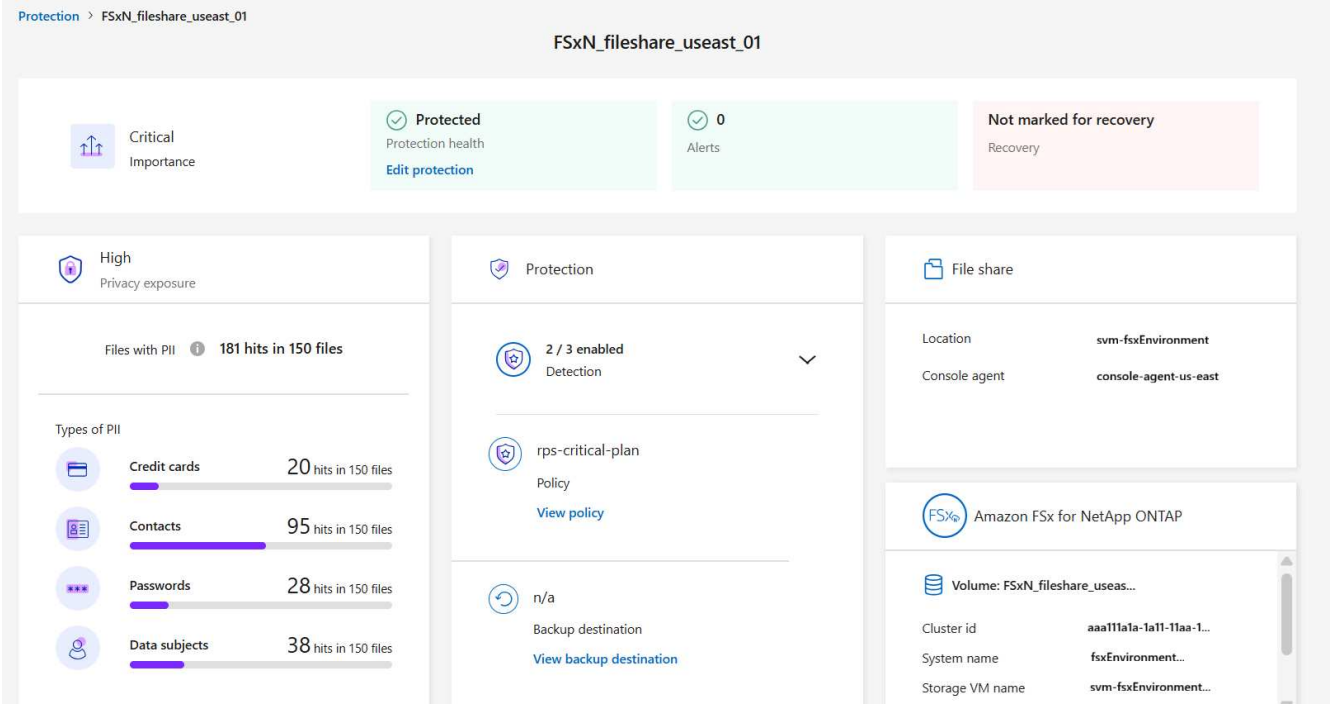
- **Alto**: oltre il 70% dei file contiene PII
- **Medio**: più del 30% e meno del 70% dei file contengono PII
- **Basso**: maggiore dello 0% e inferiore al 30% dei file contiene PII

Passi

1. Dal menu Ransomware Resilience, seleziona **Protezione**.
2. Nella pagina Protezione, individua il carico di lavoro di condivisione file nella colonna Carico di lavoro che mostra uno stato nella colonna Esposizione alla privacy.



3. Selezionare il collegamento al carico di lavoro nella colonna Carico di lavoro per visualizzarne i dettagli.



4. Nella pagina Dettagli carico di lavoro, esamina i dettagli nel riquadro Esposizione alla privacy.

Impatto dell'esposizione alla privacy sull'importanza del carico di lavoro

Le modifiche all'esposizione alla privacy possono influire sull'importanza del carico di lavoro.

Quando l'esposizione alla privacy:	Da questa esposizione alla privacy:	A questa esposizione della privacy:	Quindi, l'importanza del carico di lavoro fa questo: .
Diminuisce	Alto, medio o basso	Medio, Basso o Nessuno	Rimane lo stesso
Aumenta	Nessuno	Basso	Rimane allo standard
	Basso	Medio	Modifiche da Standard a Importante
	Basso o medio	Alto	Modifiche da Standard o Importante a Critico

Per maggiori informazioni

Per maggiori dettagli sulla classificazione dei dati, fare riferimento alla documentazione sulla classificazione dei dati:

- "Scopri di più sulla classificazione dei dati"
- "Categorie di dati privati"
- "Esamina i dati archiviati nella tua organizzazione"

Gestisci gli avvisi in NetApp Ransomware Resilience

Quando NetApp Ransomware Resilience rileva un possibile attacco, visualizza un avviso nella Dashboard e nell'area Notifiche. Ransomware Resilience esegue immediatamente uno snapshot. Esaminare il rischio potenziale nella scheda **Avvisi** di Ransomware Resilience.

Se Ransomware Resilience rileva un possibile attacco, viene visualizzata una notifica nelle impostazioni di notifica della Console e viene inviata un'email agli indirizzi configurati. L'email include informazioni sulla gravità, sul workload interessato e un collegamento all'alert nella scheda **Alerts** di Ransomware Resilience.

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

Se si ignora l'avviso, Ransomware Resilience apprende questo comportamento, lo associa alle normali operazioni e non avvia più un avviso.

Per iniziare a recuperare i dati, contrassegna l'avviso come pronto per il recupero, in modo che l'amministratore dell'archiviazione possa avviare il processo di recupero.

Ogni avviso potrebbe includere più incidenti su volumi e stati diversi. Esaminare tutti gli incidenti.

Ransomware Resilience fornisce informazioni, denominate *prove*, su ciò che ha causato l'emissione dell'avviso, come ad esempio:

- Le estensioni dei file sono state create o modificate
- Creazione di file con un confronto tra i tassi rilevati e quelli previsti
- Eliminazione dei file con un confronto tra i tassi rilevati e quelli previsti
- Quando la crittografia è elevata, senza modifiche all'estensione del file

Un avviso è classificato come segue:

- **Potenziale attacco**: viene generato un avviso quando Autonomous Ransomware Protection rileva una nuova estensione e l'evento si ripete più di 20 volte nelle ultime 24 ore (comportamento predefinito).
- **Avviso**: un avviso si verifica in base ai seguenti comportamenti:
  - Non è mai stata identificata prima una nuova estensione e lo stesso comportamento non si ripete abbastanza volte da poter essere considerato un attacco.
  - Si osserva un'elevata entropia.
  - L'attività di lettura, scrittura, ridenominazione o eliminazione dei file è raddoppiata rispetto ai livelli normali.

Per gli ambienti SAN, gli avvisi si basano solo sull'entropia elevata.

Le prove si basano sulle informazioni di Autonomous Ransomware Protection in ONTAP. Per i dettagli, fare riferimento a "Panoramica sulla protezione autonoma dal ransomware" .

Un avviso può avere uno dei seguenti stati:

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

Un incidente di allerta può avere i seguenti stati:

- **Nuovo**: tutti gli incidenti vengono contrassegnati come "nuovi" quando vengono identificati per la prima volta.
- **In revisione**: puoi contrassegnare un incidente come in revisione mentre lo valuti.
- **Ignorato**: se sospetti che l'attività non sia un attacco ransomware, puoi modificare lo stato in "Ignorato".

> Dopo aver respinto un attacco, non è possibile ripristinarne lo stato. Se si ignora un carico di lavoro, tutte le copie snapshot eseguite automaticamente in risposta al potenziale attacco ransomware verranno eliminate definitivamente.

- **In fase di archiviazione**: L'incidente è in fase di archiviazione.
- **Risolto**: l'incidente è stato risolto.
- **Risoluzione automatica**: per gli avvisi a bassa priorità, l'incidente viene risolto automaticamente se non viene intrapresa alcuna azione entro cinque giorni.

> Se hai configurato un sistema di sicurezza e gestione degli eventi (SIEM) in Ransomware Resilience nella pagina Impostazioni, Ransomware Resilience invia i dettagli dell'avviso al tuo sistema SIEM.

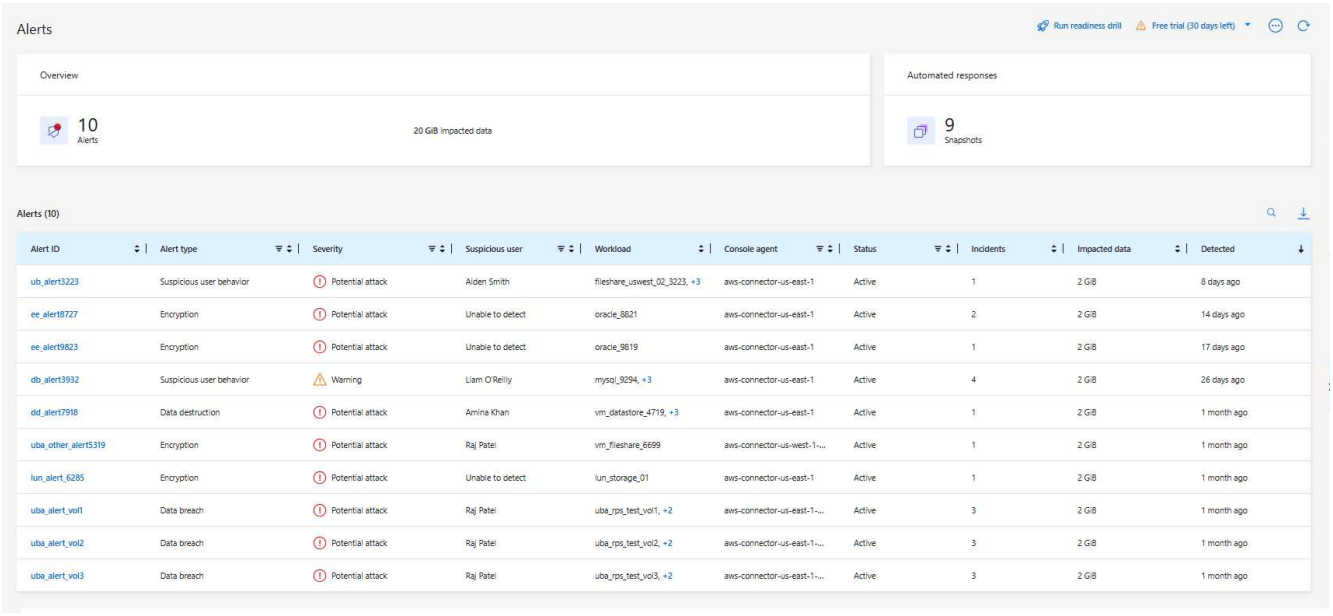
Visualizza avvisi

È possibile accedere agli avvisi dalla Ransomware Resilience Dashboard o dalla scheda **Avvisi**.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Nella Dashboard di Resilienza Ransomware, esamina il riquadro Avvisi.
2. Selezionare **Visualizza tutto** sotto uno degli stati.
3. Selezionare un avviso per esaminare tutti gli incidenti su ciascun volume per ciascun avviso.
4. Per rivedere altri avvisi, seleziona **Avviso** nel breadcrumb in alto a sinistra.
5. Esaminare gli avvisi nella pagina Avvisi.



6. Continua con una delle seguenti opzioni:
   - Rileva attività dannose e comportamenti anomali degli utenti .
   - Contrassegna gli incidenti ransomware come pronti per il ripristino (dopo che gli incidenti sono stati neutralizzati) .
   - Ignorare gli incidenti che non sono potenziali attacchi .

Rispondere a un'e-mail di avviso

Quando Ransomware Resilience rileva un potenziale attacco, invia una notifica via email agli utenti iscritti, in base alle preferenze di notifica di iscrizione configurate nelle impostazioni della NetApp Console. L'email contiene informazioni sull'avviso, tra cui la gravità e le risorse interessate.

Per impostare le notifiche e-mail nella NetApp Console, vedere "Imposta le impostazioni di notifica via email".

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Visualizza l'email.
2. Nell'e-mail, seleziona **Visualizza avviso** e accedi a Ransomware Resilience.

   Viene visualizzata la pagina Avvisi.

3. Esaminare tutti gli incidenti su ciascun volume per ciascun avviso.
4. Per rivedere altri avvisi, clicca su **Avviso** nel breadcrumb in alto a sinistra.
5. Continua con una delle seguenti opzioni:
   - Rileva attività dannose e comportamenti anomali degli utenti .
   - Contrassegna gli incidenti ransomware come pronti per il ripristino (dopo che gli incidenti sono stati neutralizzati) .

- Ignorare gli incidenti che non sono potenziali attacchi .

Rileva attività dannose e comportamenti anomali degli utenti

Nella scheda Avvisi è possibile verificare se si è verificata un'attività dannosa o un comportamento anomalo da parte dell'utente.

È necessario aver configurato un agente di attività utente e abilitato una policy di protezione con rilevamento del comportamento utente per visualizzare gli avvisi a livello utente. La colonna **Utente sospetto** viene visualizzata nella dashboard Avvisi solo quando il rilevamento del comportamento utente è abilitato. Per abilitare il rilevamento degli utenti sospetti, vedere "Attività utente sospetta".

Visualizza attività dannose

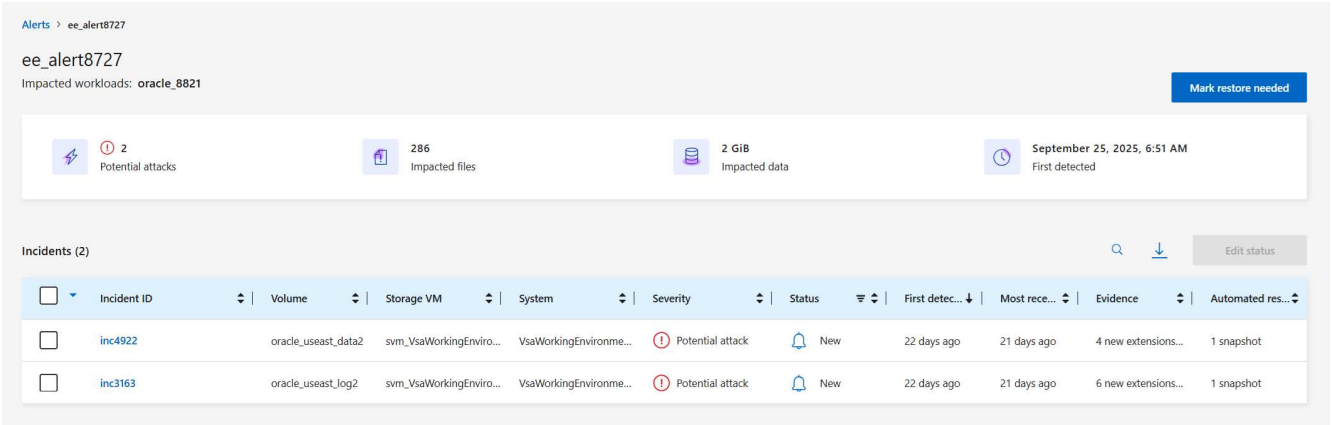
Quando Autonomous Ransomware Protection attiva un avviso in Ransomware Resilience, puoi visualizzare i seguenti dettagli:

- Entropia dei dati in arrivo
- Tasso di creazione previsto di nuovi file rispetto al tasso rilevato
- Tasso di eliminazione previsto dei file rispetto al tasso rilevato
- Frequenza di ridenominazione prevista dei file rispetto alla frequenza rilevata
- File e directory interessati

Questi dettagli sono visualizzabili per i carichi di lavoro NAS. Per gli ambienti SAN sono disponibili solo i dati sull'entropia.

Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.
2. Seleziona un avviso.
3. Esaminare gli incidenti nell'avviso.



4. Seleziona un incidente per esaminarne i dettagli.

Visualizza il comportamento anomalo dell'utente

Se hai configurato il rilevamento degli utenti sospetti per visualizzare comportamenti anomali degli utenti, puoi visualizzare i dati a livello di utente e bloccare utenti specifici. Per abilitare le impostazioni utente sospette,

vedere"Configurare le impostazioni di resilienza al ransomware" .

Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.
2. Seleziona un avviso.
3. Esaminare gli incidenti nell'avviso.
4. Per bloccare un utente sospetto nel tuo ambiente, seleziona **Blocca** sotto il nome dell'utente.

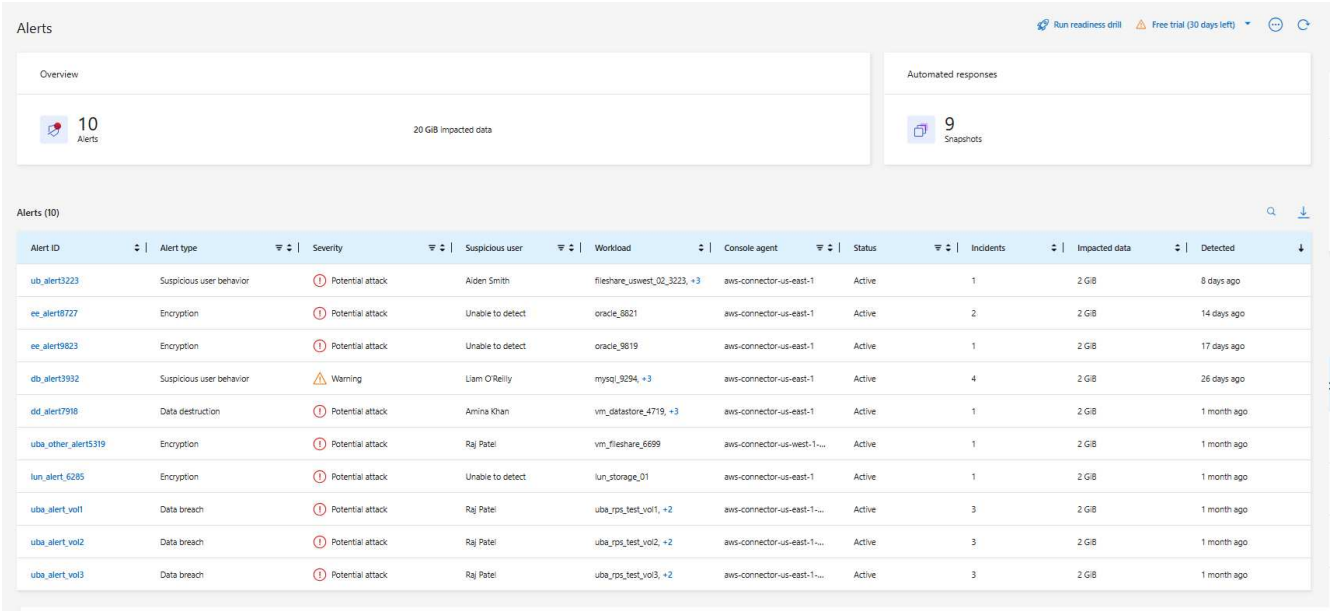
Contrassegna gli incidenti ransomware come pronti per il ripristino (dopo che gli incidenti sono stati neutralizzati)

Dopo aver fermato l'attacco, informa l'amministratore dello storage che i dati sono pronti così che possa avviare il processo di ripristino.

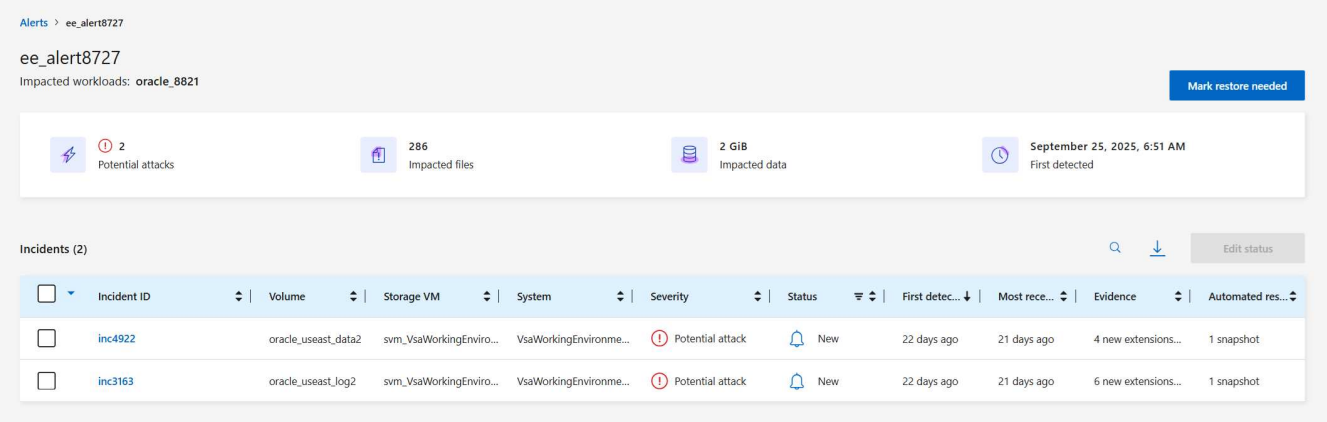
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.



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



4. Se si determina che gli incidenti sono pronti per il ripristino, selezionare **Segna come ripristino necessario**.
5. Conferma l'azione e seleziona **Segna come ripristino necessario**.
6. Per avviare il ripristino del carico di lavoro, selezionare **Recupera** carico di lavoro nel messaggio oppure selezionare la scheda **Ripristino**.

Risultato

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

Ignorare gli incidenti che non sono potenziali attacchi

Dopo aver esaminato gli incidenti, è necessario stabilire se si tratta di potenziali attacchi. Se non si tratta di minacce reali, possono essere ignorate.

Puoi ignorare i falsi positivi o decidere di recuperare immediatamente i tuoi dati. Se si ignora l'avviso, Ransomware Resilience apprende questo comportamento e lo associa alle normali operazioni, senza più avviare un avviso per tale comportamento.

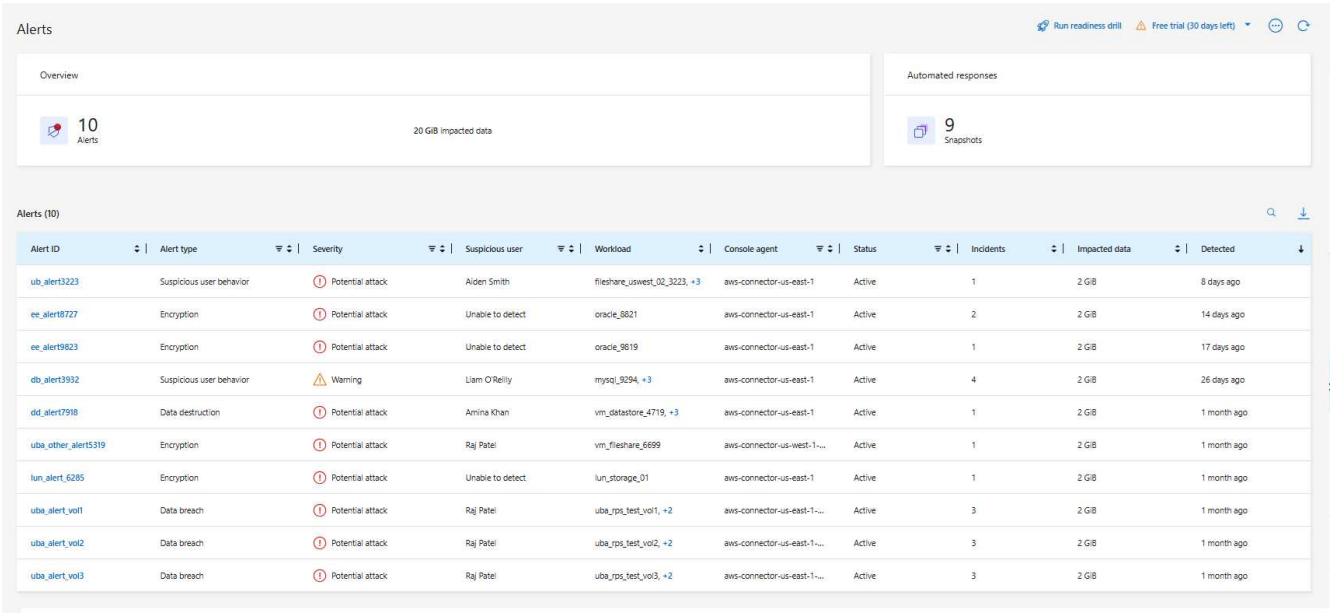
Se si elimina un carico di lavoro, tutte le copie snapshot eseguite automaticamente in risposta a un potenziale attacco ransomware vengono eliminate definitivamente.

Se si ignora un avviso, non è possibile modificarne lo stato né annullare la modifica.

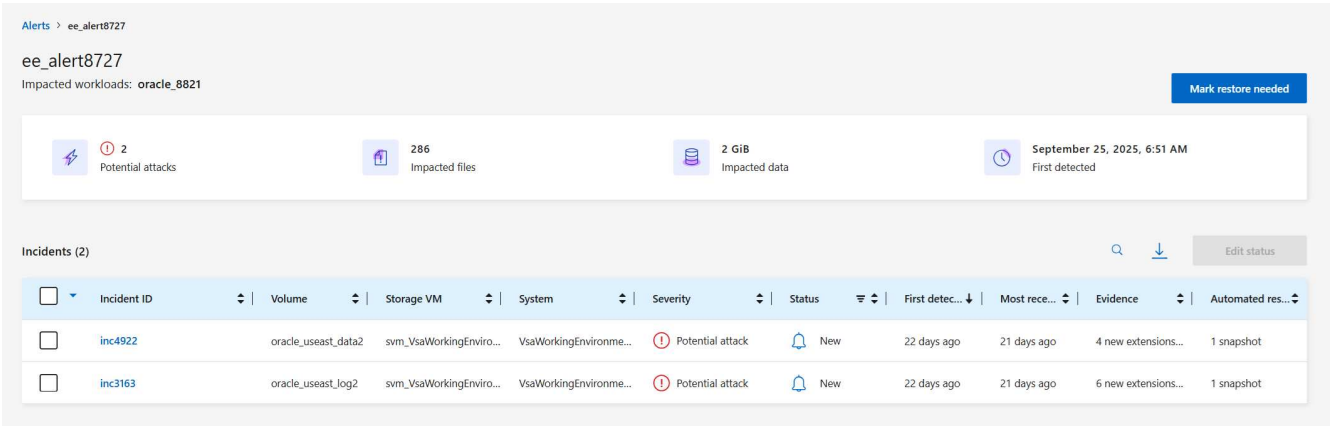
Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

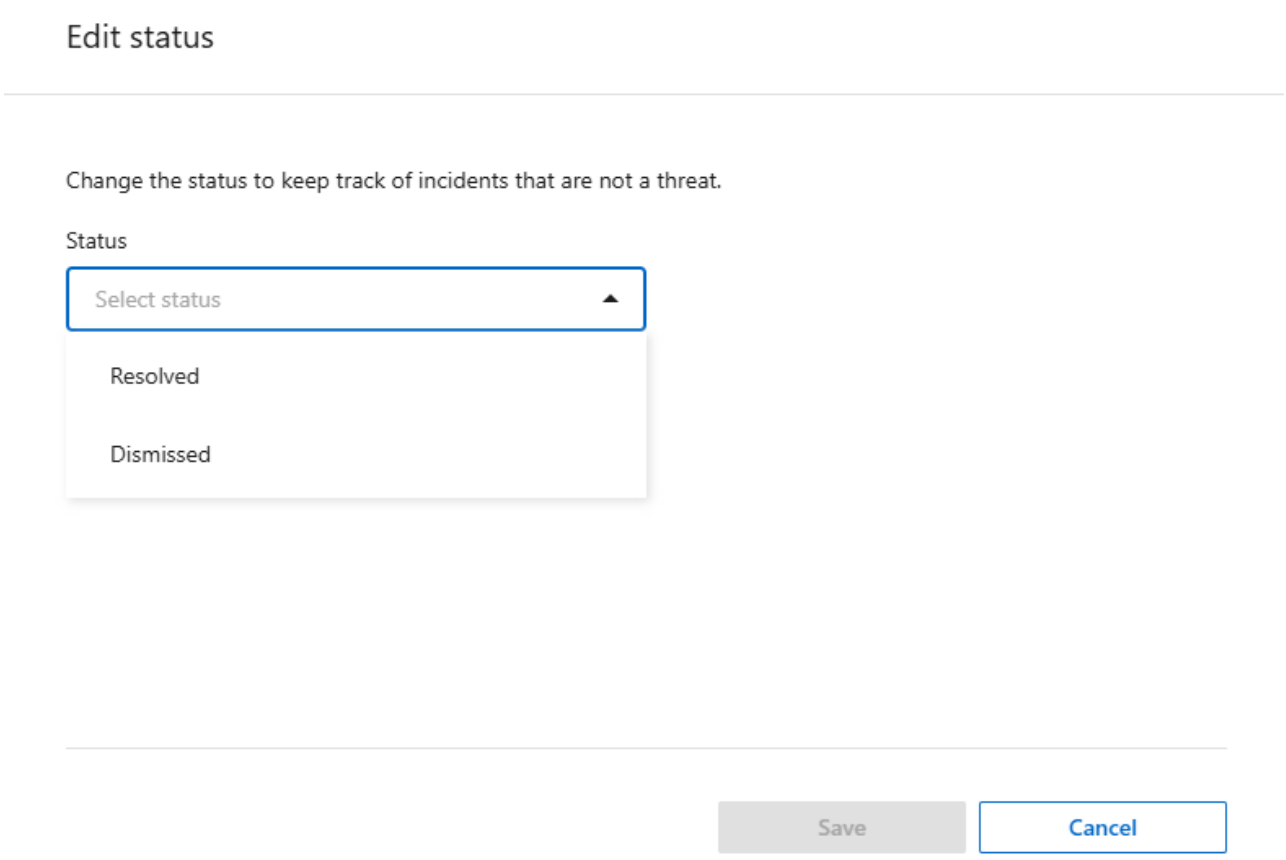
1. Dal menu Ransomware Resilience, seleziona **Avvisi**.



2. Nella pagina Avvisi, seleziona l'avviso.



3. Seleziona uno o più incidenti. In alternativa, selezionare tutti gli incidenti selezionando la casella ID incidente in alto a sinistra della tabella.
4. Se stabilisci che l'incidente non rappresenta una minaccia, scartalo come falso positivo:
   - Seleziona l'incidente.
   - Selezionare il pulsante **Modifica stato** sopra la tabella.



5. Dalla casella Modifica stato, seleziona lo stato **Ignorato**.

   Vengono visualizzate informazioni aggiuntive sul carico di lavoro e sulle copie snapshot eliminate.

6. Seleziona **Salva**.

   Lo stato dell'incidente o degli incidenti cambia in "Ignorato".

Visualizza un elenco dei file interessati

Prima di ripristinare il carico di lavoro di un'applicazione a livello di file, è possibile visualizzare un elenco dei file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco dei file interessati. Quindi utilizzare la pagina Recupero per caricare l'elenco e scegliere quali file ripristinare.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

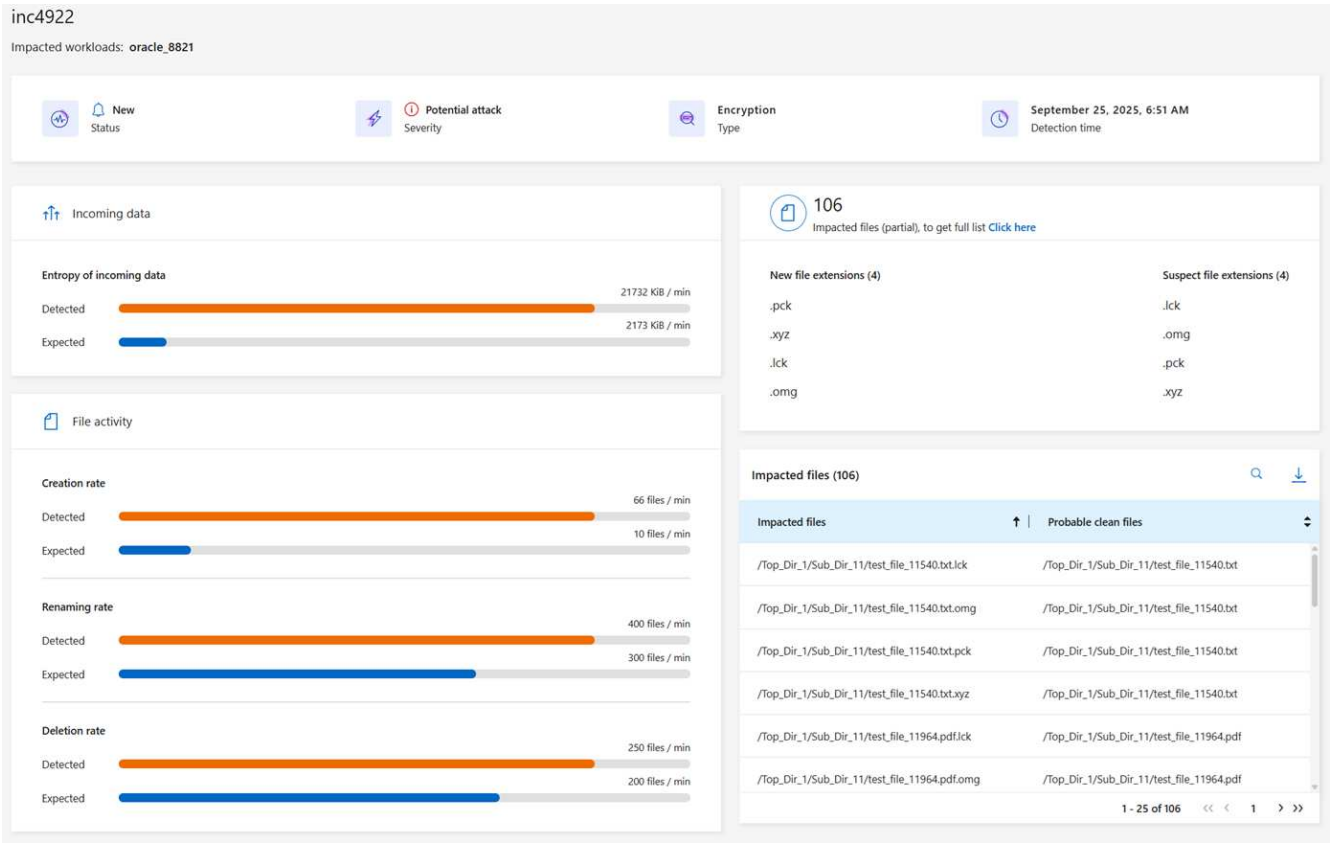
Passi

Utilizzare la pagina Avvisi per recuperare l'elenco dei file interessati.

Se un volume presenta più avvisi, potrebbe essere necessario scaricare l'elenco CSV dei file interessati per ciascun avviso.

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.

2. Nella pagina Avvisi, ordina i risultati in base al carico di lavoro per visualizzare gli avvisi per il carico di lavoro dell'applicazione che desideri ripristinare.
3. Dall'elenco degli avvisi per quel carico di lavoro, seleziona un avviso.
4. Per quell'avviso, seleziona un singolo incidente.



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

Recupera da un attacco ransomware (dopo che gli incidenti sono stati neutralizzati) con NetApp Ransomware Resilience

Dopo che i carichi di lavoro sono stati contrassegnati come "Ripristino necessario", NetApp Ransomware Resilience consiglia un punto di ripristino effettivo (RPA) e orchestra il flusso di lavoro per un ripristino a prova di crash.

- Se l'applicazione o la VM è gestita da SnapCenter, Ransomware Resilience ripristina l'applicazione o la VM allo stato precedente e all'ultima transazione utilizzando il processo coerente con l'applicazione o con la VM. Il ripristino coerente con l'applicazione o la macchina virtuale aggiunge ai dati nel volume tutti i dati che non sono stati archiviati, ad esempio i dati nella cache o in un'operazione di I/O.
- Se l'applicazione o la VM non è gestita da SnapCenter ma da NetApp Backup and Recovery o Ransomware Resilience, Ransomware Resilience esegue un ripristino coerente con l'arresto anomalo, in cui tutti i dati presenti nel volume nello stesso momento vengono ripristinati, ad esempio, in caso di arresto anomalo del sistema.

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

Il ripristino del carico di lavoro può avere un impatto sui carichi di lavoro in esecuzione. Dovresti coordinare i processi di recupero con le parti interessate appropriate.

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

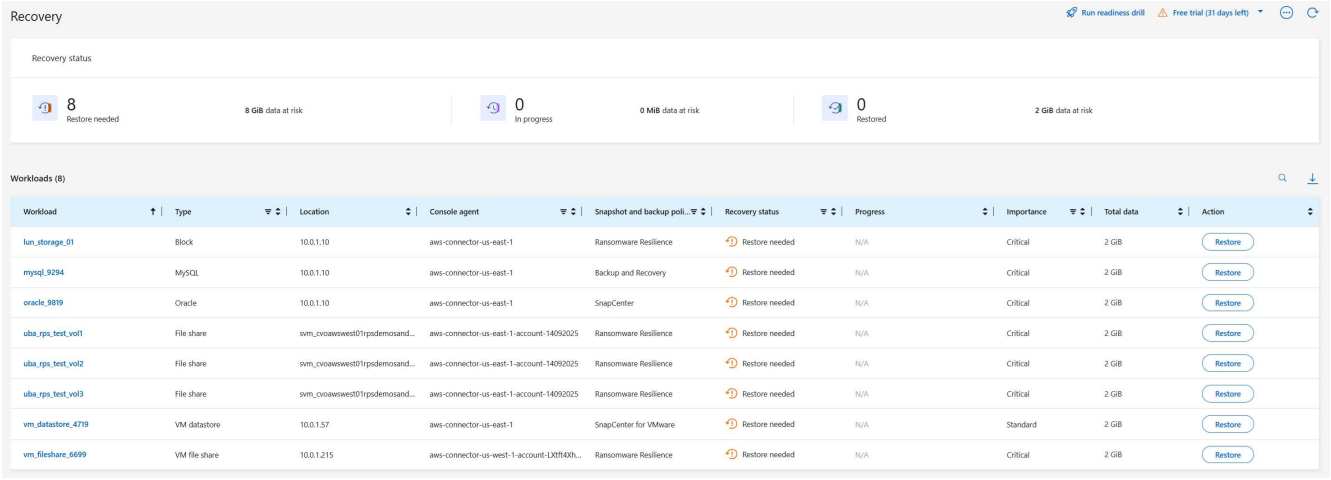
- **Ripristino necessario**: il carico di lavoro deve essere ripristinato.
- **In corso**: l'operazione di ripristino è attualmente in corso.
- **Ripristinato**: il carico di lavoro è stato ripristinato.
- **Non riuscito**: il processo di ripristino del carico di lavoro non è stato completato.

Visualizza i carichi di lavoro pronti per essere ripristinati

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

Passi

1. Eseguire una delle seguenti operazioni:
   - Dalla Dashboard, controlla i totali "Ripristino necessario" nel riquadro Avvisi e seleziona **Visualizza tutto**.
   - Dal menu, seleziona **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Recupero**.



Ripristina un carico di lavoro gestito da SnapCenter

Utilizzando Ransomware Resilience, l'amministratore dell'archiviazione può stabilire il modo migliore per ripristinare i carichi di lavoro dal punto di ripristino consigliato o da quello preferito.

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

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Passi

1. Da Ransomware Resilience, seleziona **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Recupero**.
3. Selezionare un carico di lavoro che si trovi nello stato "Ripristino necessario".
4. Per ripristinare, seleziona **Ripristina**.
5. **Ambito di ripristino**: coerente con l'applicazione (o per SnapCenter per VM, l'ambito di ripristino è "Per VM")
6. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

   Ransomware Resilience identifica come punto di ripristino migliore l'ultimo backup appena prima dell'incidente e mostra l'indicazione "Consigliato".

7. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
   a. Selezionare la posizione originale o alternativa.
   b. Selezionare il sistema.
   c. Selezionare la VM di archiviazione.
8. Se la destinazione originale non dispone di spazio sufficiente per ripristinare il carico di lavoro, viene visualizzata la riga "Archiviazione temporanea". È possibile selezionare l'archiviazione temporanea per ripristinare i dati del carico di lavoro. I dati ripristinati verranno copiati dall'archivio temporaneo alla posizione originale. Fare clic sulla **freccia giù** nella riga Archiviazione temporanea e impostare il cluster di destinazione, la VM di archiviazione e il livello locale.
9. Seleziona **Salva**.
10. Selezionare **Avanti**.
11. Rivedi le tue selezioni.
12. Selezionare **Ripristina**.
13. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati.

Ripristina un carico di lavoro non gestito da SnapCenter

Utilizzando Ransomware Resilience, l'amministratore dell'archiviazione può stabilire il modo migliore per ripristinare i carichi di lavoro dal punto di ripristino consigliato o da quello preferito.

Ruolo di console obbligatorio Per eseguire questa attività, è necessario il ruolo di amministratore dell'organizzazione, di amministratore della cartella o del progetto o di amministratore di Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

L'amministratore dell'archiviazione di sicurezza può recuperare i dati a diversi livelli:

- Recupera tutti i volumi
- Ripristina un'applicazione a livello di volume o di file e cartella.
- Ripristina una condivisione file a livello di volume, directory o file/cartella.
- Ripristina da un datastore a livello di VM.

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

Passi

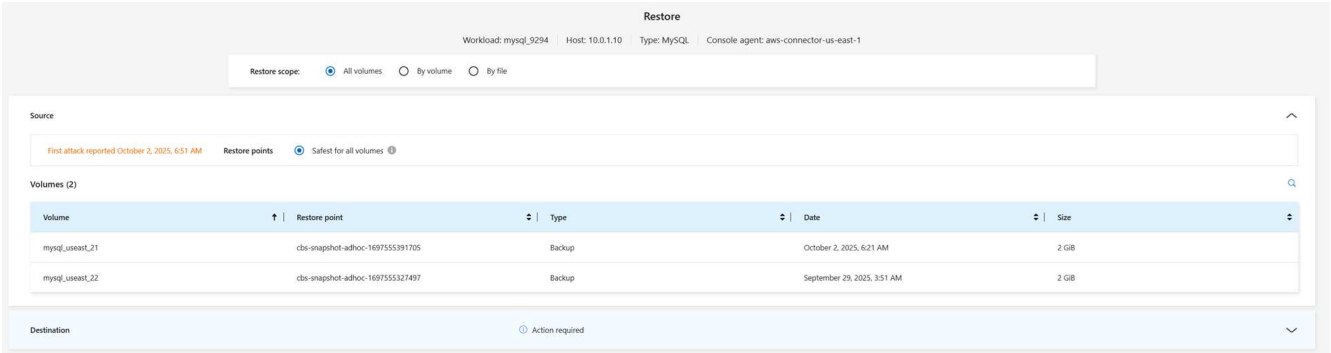
1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Recupero**.
3. Selezionare un carico di lavoro che si trovi nello stato "Ripristino necessario".
4. Per ripristinare, seleziona **Ripristina**.
5. **Ambito di ripristino**: seleziona il tipo di ripristino che desideri completare:
   - Tutti i volumi
   - Per volume
   - Per file: è possibile specificare una cartella o singoli file da ripristinare.

   Per i carichi di lavoro SAN, è possibile eseguire il ripristino solo per carico di lavoro.

   È possibile selezionare fino a 100 file o una singola cartella.
6. Procedere con una delle seguenti procedure a seconda che si sia scelto applicazione, volume o file.

Ripristina tutti i volumi

1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Selezionare un carico di lavoro che si trovi nello stato "Ripristino necessario".
3. Per ripristinare, seleziona **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, seleziona **Tutti i volumi**.



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

   Ransomware Resilience identifica come punto di ripristino migliore l'ultimo backup appena prima dell'incidente e mostra l'indicazione "Il più sicuro per tutti i volumi". Ciò significa che tutti i volumi verranno ripristinati in una copia precedente al primo attacco al primo volume rilevato.
6. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
   a. Selezionare il sistema.
   b. Selezionare la VM di archiviazione.

c. Selezionare l’aggregato.

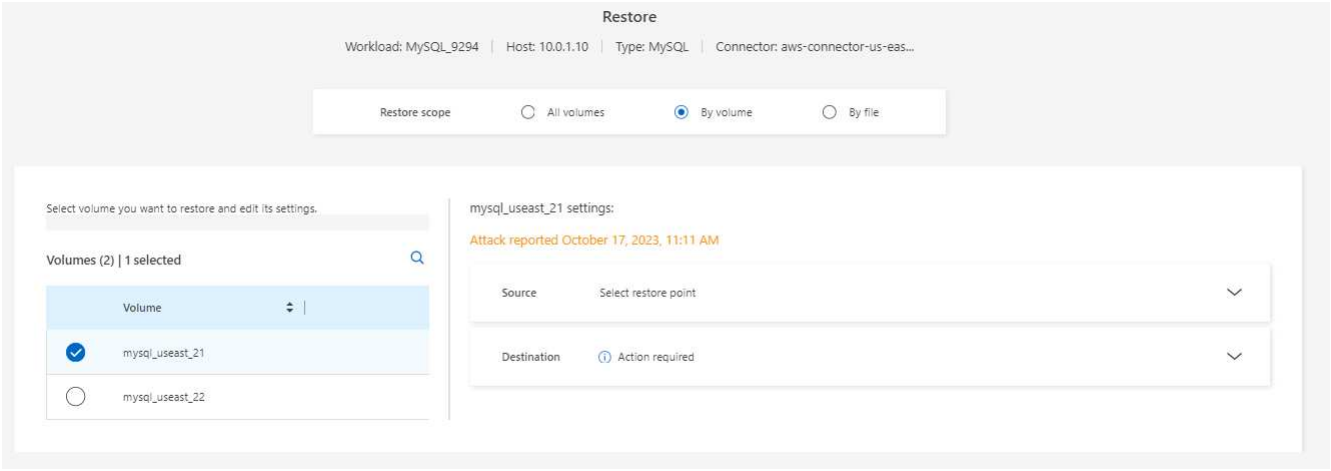
d. Modifica il prefisso del volume che verrà aggiunto a tutti i nuovi volumi.

> Il nuovo nome del volume appare come prefisso + nome del volume originale + nome del backup + data del backup.

7. Seleziona **Salva**.
8. Selezionare **Avanti**.
9. Rivedi le tue selezioni.
10. Selezionare **Ripristina**.
11. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell’operazione scorre tra gli stati.

Ripristinare un carico di lavoro applicativo a livello di volume

1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Selezionare un carico di lavoro applicativo che si trovi nello stato "Ripristino necessario".
3. Per ripristinare, seleziona **Ripristina**.
4. Nella pagina Ripristina, nell’ambito Ripristina, seleziona **Per volume**.



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

> Ransomware Resilience identifica come punto di ripristino migliore l’ultimo backup appena prima dell’incidente e mostra l’indicazione "Consigliato".

7. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
   a. Selezionare il sistema.
   b. Selezionare la VM di archiviazione.
   c. Selezionare l’aggregato.
   d. Controllare il nuovo nome del volume.

Il nuovo nome del volume appare come nome del volume originale + nome del backup + data del backup.

8. Seleziona **Salva**.
9. Selezionare **Avanti**.
10. Rivedi le tue selezioni.
11. Selezionare **Ripristina**.
12. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati.

Ripristinare il carico di lavoro di un'applicazione a livello di file

Prima di ripristinare il carico di lavoro di un'applicazione a livello di file, è possibile visualizzare un elenco dei file interessati. È possibile accedere alla pagina Avvisi per scaricare un elenco dei file interessati. Quindi utilizzare la pagina Recupero per caricare l'elenco e scegliere quali file ripristinare.

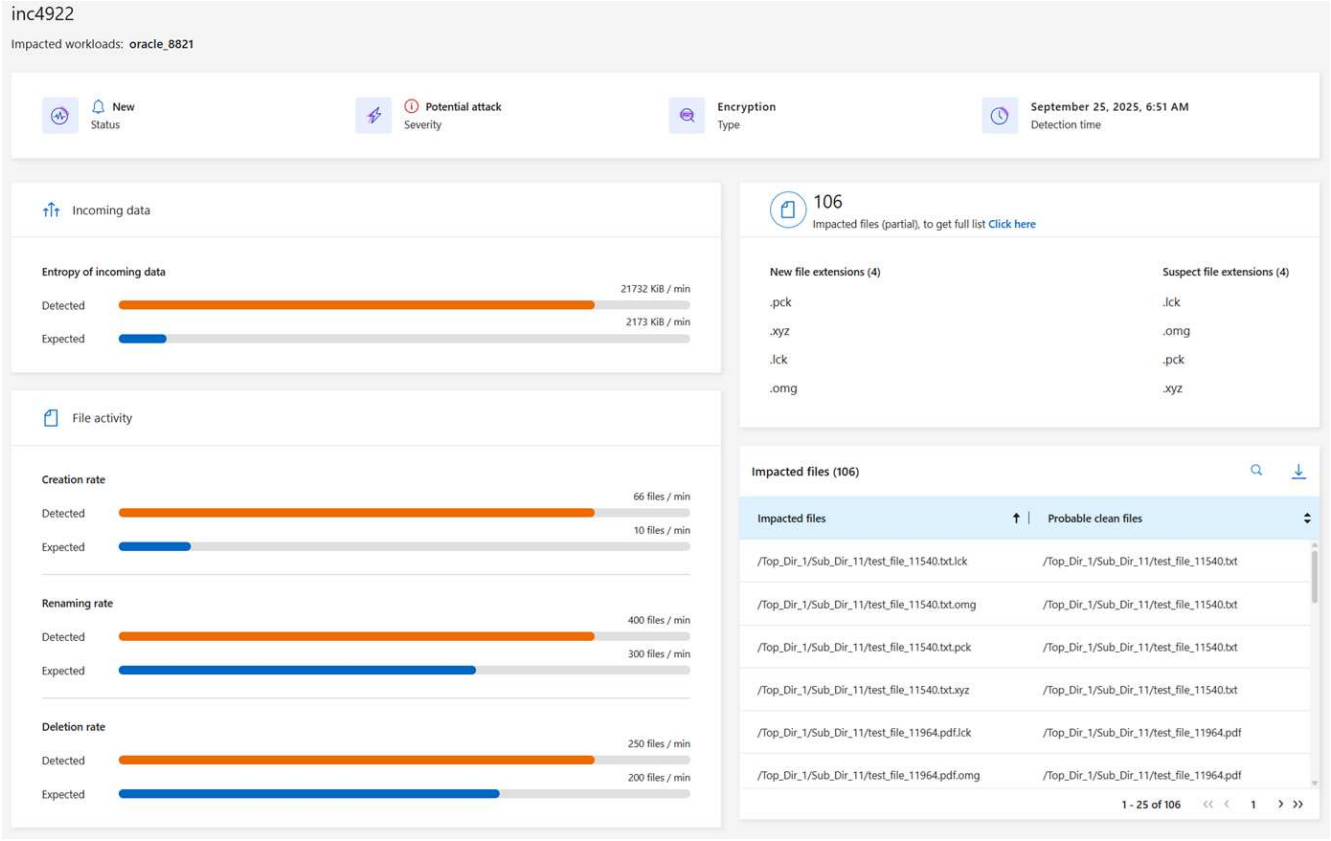
È possibile ripristinare il carico di lavoro di un'applicazione a livello di file sullo stesso sistema o su un sistema diverso.

Passaggi per ottenere l'elenco dei file interessati

Utilizzare la pagina Avvisi per recuperare l'elenco dei file interessati.

Se un volume presenta più avvisi, sarà necessario scaricare l'elenco CSV dei file interessati per ciascun avviso.

1. Dal menu Ransomware Resilience, seleziona **Avvisi**.
2. Nella pagina Avvisi, ordina i risultati in base al carico di lavoro per visualizzare gli avvisi per il carico di lavoro dell'applicazione che desideri ripristinare.
3. Dall'elenco degli avvisi per quel carico di lavoro, seleziona un avviso.
4. Per quell'avviso, seleziona un singolo incidente.



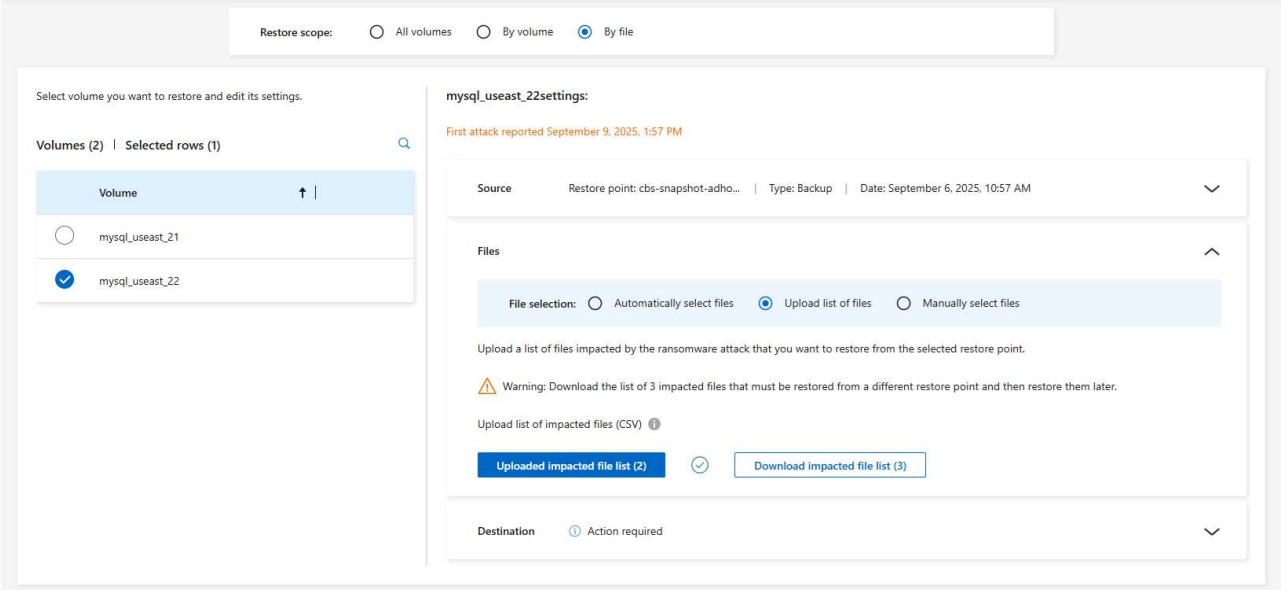
5. Per visualizzare l'elenco completo dei file, seleziona **Clicca qui** nella parte superiore del riquadro File interessati.
6. Per tale incidente, seleziona l'icona di download e scarica l'elenco dei file interessati in formato CSV.

Passaggi per ripristinare quei file

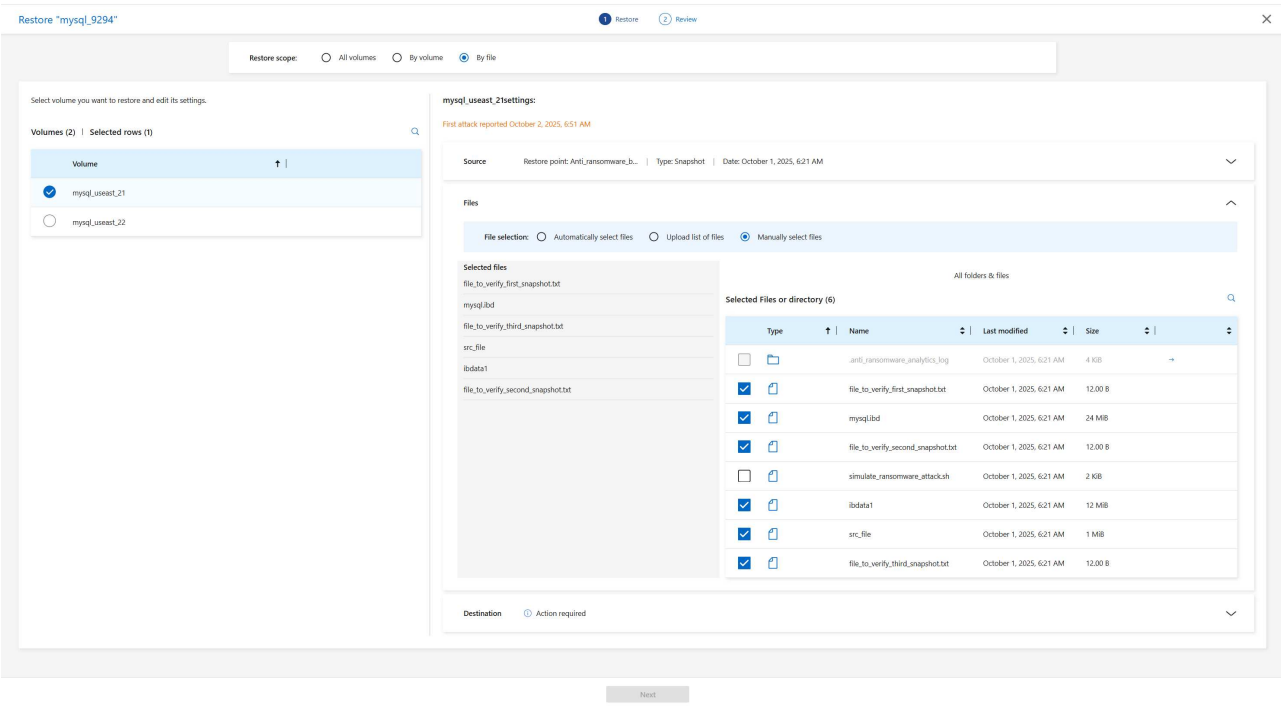
1. Dal menu Ransomware Resilience, seleziona **Ripristino**.
2. Selezionare un carico di lavoro applicativo che si trovi nello stato "Ripristino necessario".
3. Per ripristinare, seleziona **Ripristina**.
4. Nella pagina Ripristina, nell'ambito Ripristina, seleziona **Per file**.
5. Nell'elenco dei volumi, seleziona il volume che contiene i file che desideri ripristinare.
6. **Punto di ripristino**: seleziona la freccia rivolta verso il basso accanto a **Punto di ripristino** per visualizzare i dettagli. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> Nella colonna Motivo nel riquadro Punti di ripristino viene visualizzato il motivo dello snapshot o del backup, ovvero "Pianificato" o "Risposta automatica a un incidente ransomware".

7. **File**:
   - **Seleziona automaticamente i file**: lascia che Ransomware Resilience selezioni i file da ripristinare.
   - **Carica elenco file**: carica un file CSV contenente l'elenco dei file interessati che hai ricevuto dalla pagina Avvisi o che possiedi. È possibile ripristinare fino a 10.000 file alla volta.



- **Seleziona manualmente i file**: seleziona fino a 10.000 file o una singola cartella da ripristinare.



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

8. **Destinazione**: seleziona la freccia rivolta verso il basso accanto a Destinazione per visualizzare i dettagli.
   a. Scegli dove ripristinare i dati: la posizione di origine originale o una posizione alternativa che puoi specificare.

Sebbene i file o la directory originali verranno sovrascritti dai dati ripristinati, i nomi originali dei file e delle cartelle rimarranno gli stessi, a meno che non vengano specificati nuovi nomi.

b. Selezionare il sistema.

c. Selezionare la VM di archiviazione.

d. Facoltativamente, inserisci il percorso.

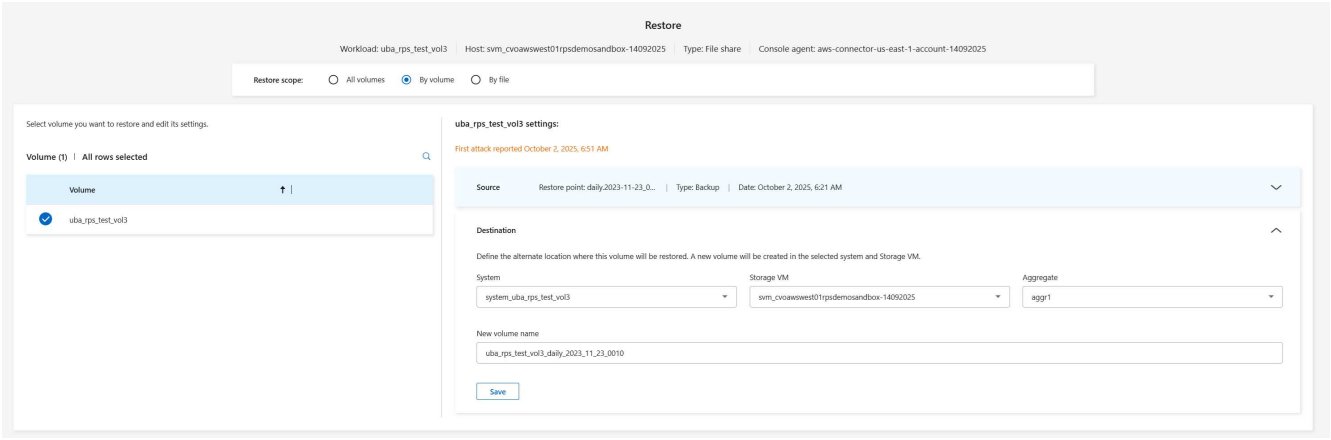
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

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

9. Selezionare **Avanti**.
10. Rivedi le tue selezioni.
11. Selezionare **Ripristina**.
12. Dal menu in alto, seleziona **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati.

Ripristinare una condivisione file o un archivio dati

1. Dopo aver selezionato una condivisione file o un datastore da ripristinare, nella pagina Ripristina, nell'ambito Ripristina, seleziona **Per volume**.



2. Nell'elenco dei volumi, seleziona il volume che desideri ripristinare.
3. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli.

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

> Ransomware Resilience identifica come punto di ripristino migliore l'ultimo backup appena prima dell'incidente e mostra l'indicazione "Consigliato".

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

a. Scegli dove ripristinare i dati: la posizione di origine originale o una posizione alternativa che puoi specificare.

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

b. Selezionare il sistema.

c. Selezionare la VM di archiviazione.

d. Facoltativamente, inserisci il percorso.

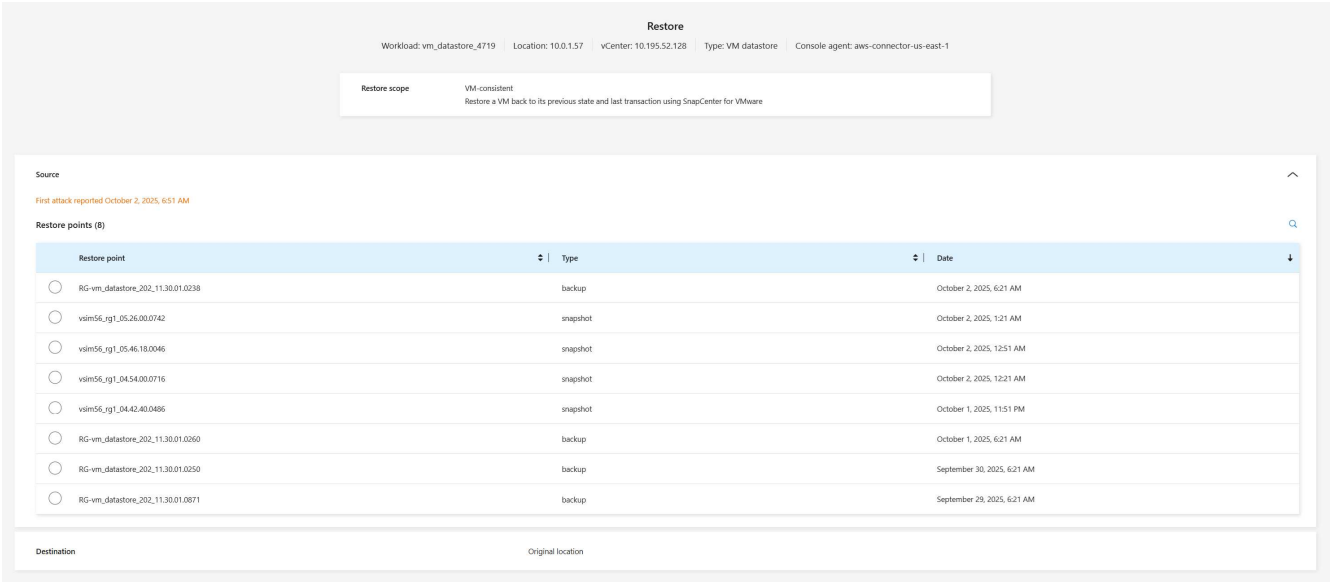
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

5. Seleziona **Salva**.
6. Rivedi le tue selezioni.
7. Selezionare **Ripristina**.
8. Dal menu, selezionare **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione passa attraverso i vari stati.

Ripristinare una condivisione file VM a livello di VM

Nella pagina Ripristino, dopo aver selezionato una VM da ripristinare, continuare con questi passaggi.

1. **Origine**: seleziona la freccia rivolta verso il basso accanto a Origine per visualizzare i dettagli.



2. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.
3. **Destinazione**: Verso la posizione originale.
4. Selezionare **Avanti**.
5. Rivedi le tue selezioni.
6. Selezionare **Ripristina**.
7. Dal menu, selezionare **Ripristino** per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione passa attraverso i vari stati.

Scarica i report in NetApp Ransomware Resilience

È possibile esportare i dati di protezione e scaricare i file CSV o JSON che mostrano i

dettagli delle esercitazioni di preparazione agli attacchi, della protezione, degli avvisi e del ripristino.

Prima di scaricare i file, aggiorna la dashboard per acquisire i dati più recenti nei tuoi report.

Ruolo Console obbligatorio Per eseguire questa attività, è necessario il ruolo Amministratore organizzazione, Amministratore cartella o progetto, Amministratore Ransomware Resilience o Visualizzatore Ransomware Resilience. "Scopri di più sui ruoli di Ransomware Resilience per NetApp Console" .

Quali dati puoi scaricare? È possibile scaricare i file da una qualsiasi delle opzioni del menu principale:

- **Riepilogo**: include elenchi di carichi di lavoro supportati e non supportati, azioni consigliate per migliorare la tua postura di resilienza informatica e informazioni acquisite nella dashboard Ransomware Resilience.
- **Protezione**: include lo stato e i dettagli di tutti i carichi di lavoro, incluso il numero totale di quelli protetti e a rischio.
- **Avvisi**: include lo stato e i dettagli di tutti gli avvisi, tra cui il numero totale di avvisi e snapshot automatici.
- **Ripristino**: include lo stato e i dettagli di tutti i carichi di lavoro che devono essere ripristinati, incluso il numero totale di carichi di lavoro contrassegnati come "Ripristino necessario", "In corso", "Ripristino non riuscito" e "Ripristino riuscito".
- **Report**: puoi esportare i dati da qualsiasi pagina e scaricare i file.

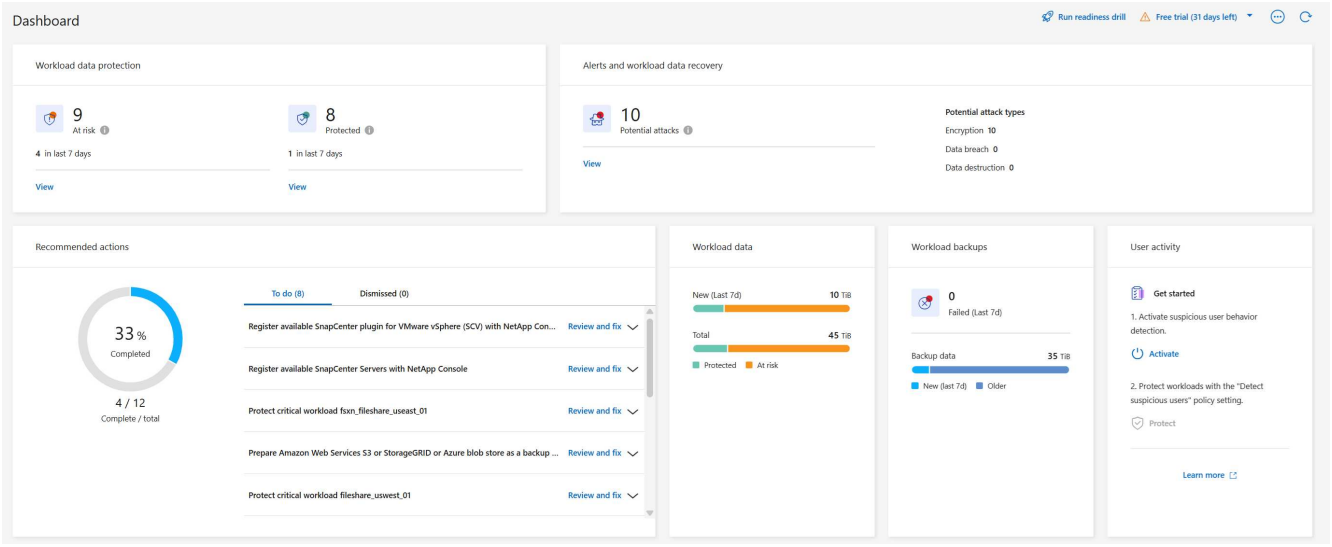
È possibile scaricare i report delle esercitazioni di preparazione solo dalla pagina **Report**.

Se scarichi file CSV o JSON dalla pagina Protezione, Avvisi o Ripristino, i dati mostrano solo i dati presenti in quella pagina.

I file CSV o JSON includono dati per tutti i carichi di lavoro su tutti i sistemi Console.

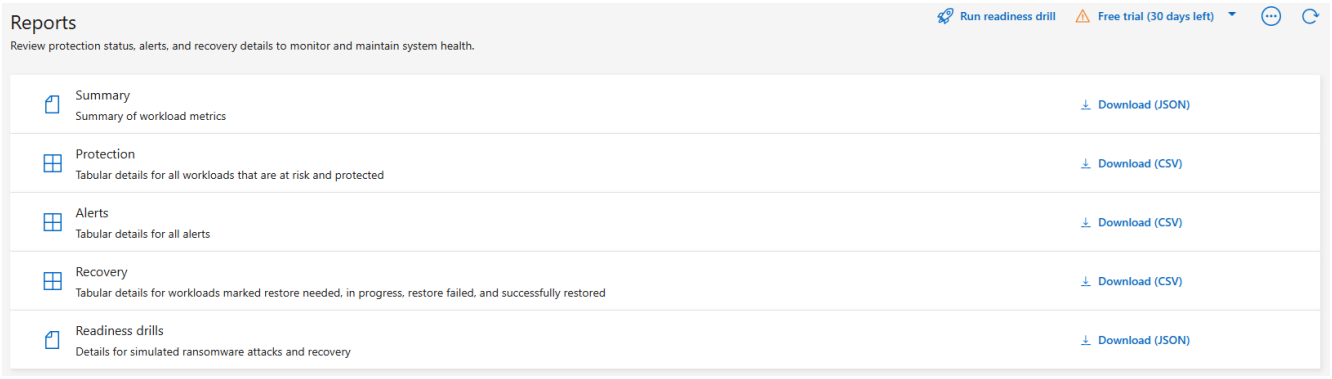
Passi

1. Dal menu di navigazione a sinistra della Console, seleziona **Protezione** > **Ransomware Resilience**.



2. Dalla Dashboard o da un'altra pagina, seleziona *Aggiorna* opzione in alto a destra per aggiornare i dati che appariranno nei report.

3. Eseguire una delle seguenti operazioni:
   - Dalla pagina, seleziona *Download*  opzione.
   - Dal menu NetApp Ransomware Resilience , seleziona **Report**.
4. Se hai selezionato l'opzione **Report**, seleziona uno dei nomi di file preconfigurati e seleziona **Scarica**.



Conoscenza e supporto

Registrati per ricevere supporto

Per ricevere supporto tecnico specifico per NetApp Console e le sue soluzioni di storage e servizi dati è necessaria la registrazione al supporto. La registrazione del supporto è inoltre richiesta per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP .

La registrazione per il supporto non abilita il supporto NetApp per un servizio file del provider cloud. Per assistenza tecnica relativa a un servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla sezione "Ottenere assistenza" nella documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Panoramica della registrazione del supporto

Per attivare il diritto al sostegno sono previste due modalità di registrazione:

- Registrando il numero di serie del tuo account NetApp Console (il numero di serie di 20 cifre 960xxxxxxxx che si trova nella pagina Risorse di supporto nella Console).

  Questo funge da ID di abbonamento unico per qualsiasi servizio all'interno della Console. Ogni account Console deve essere registrato.

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

  Questi numeri di serie sono comunemente denominati *numeri di serie PAYGO* e vengono generati dalla NetApp Console al momento della distribuzione Cloud Volumes ONTAP .

La registrazione di entrambi i tipi di numeri di serie consente funzionalità quali l'apertura di ticket di supporto e la generazione automatica di casi. La registrazione viene completata aggiungendo gli account NetApp Support Site (NSS) alla Console come descritto di seguito.

Registra NetApp Console per il supporto NetApp

Per registrarsi per ricevere supporto e attivare il diritto al supporto, un utente del tuo account NetApp Console deve associare un account NetApp Support Site al proprio accesso alla Console. La modalità di registrazione per l'assistenza NetApp varia a seconda che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

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

Passi

1. Selezionare **Amministrazione** > **Credenziali**.

2. Selezionare **Credenziali utente**.
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp (NSS).
4. Per confermare che il processo di registrazione è andato a buon fine, seleziona l'icona Aiuto e poi **Supporto**.

   La pagina **Risorse** dovrebbe mostrare che il tuo account Console è registrato per il supporto.

   Tieni presente che gli altri utenti della Console non vedranno lo stesso stato di registrazione del supporto se non hanno associato un account NetApp Support Site al loro login. Tuttavia, ciò non significa che il tuo account non sia registrato per l'assistenza. Se un utente dell'organizzazione ha seguito questi passaggi, il tuo account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp esistente con licenze e numeri di serie esistenti ma *nessun* account NSS, devi creare un account NSS e associarlo al tuo accesso alla Console.

Passi

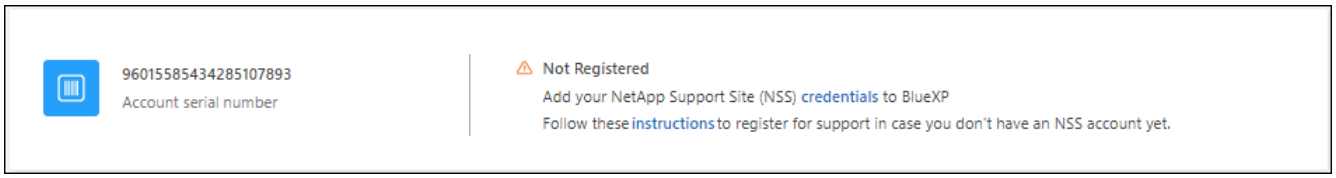
1. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account della console (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione dell'account.
2. Associa il tuo nuovo account NSS al tuo accesso alla Console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Novità assoluta per NetApp

Se sei un nuovo utente NetApp e non hai un account NSS, segui i passaggi indicati di seguito.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.
2. Individua il numero di serie del tuo ID account nella pagina di registrazione del supporto.



3. Vai a "Sito di registrazione del supporto NetApp" e seleziona **Non sono un cliente NetApp registrato**.
4. Compila i campi obbligatori (quelli contrassegnati da asterischi rossi).
5. Nel campo **Linea di prodotti**, seleziona **Cloud Manager** e poi seleziona il tuo fornitore di fatturazione applicabile.
6. Copia il numero di serie del tuo account dal passaggio 2 sopra, completa il controllo di sicurezza e conferma di aver letto l'Informativa globale sulla privacy dei dati di NetApp.

   Per finalizzare questa transazione sicura, verrà inviata immediatamente un'e-mail alla casella di posta indicata. Se l'e-mail di convalida non arriva entro pochi minuti, assicurati di controllare la cartella spam.

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

   La conferma invia la richiesta a NetApp e ti consiglia di creare un account sul sito di supporto NetApp .

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

Dopo aver finito

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

Una volta ottenuto l'account del sito di supporto NetApp , associalo al tuo accesso alla console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

L'associazione delle credenziali del sito di supporto NetApp al tuo account della console è necessaria per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP a consumo per il supporto

  Per attivare il supporto per il tuo sistema e accedere alle risorse di supporto tecnico NetApp è necessario fornire il tuo account NSS.

- Distribuzione di Cloud Volumes ONTAP quando si utilizza la propria licenza (BYOL)

  È necessario fornire il proprio account NSS affinché la Console possa caricare la chiave di licenza e abilitare l'abbonamento per il periodo acquistato. Ciò include aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP all'ultima versione

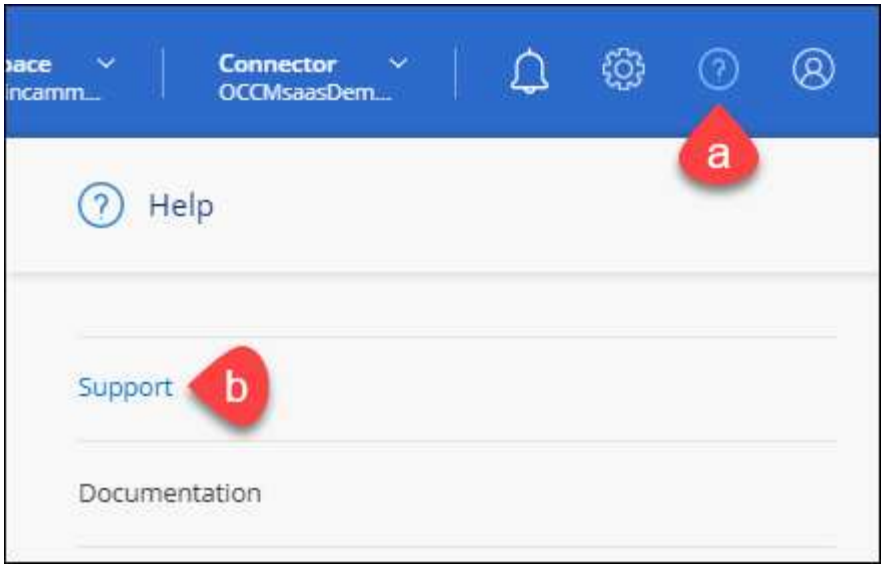
L'associazione delle credenziali NSS al tuo account NetApp Console è diversa dall'associazione dell'account NSS all'accesso utente della Console.

Queste credenziali NSS sono associate al tuo ID account Console specifico. Gli utenti che appartengono all'organizzazione Console possono accedere a queste credenziali da **Supporto > Gestione NSS**.

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

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, seleziona **Continua** per essere reindirizzato alla pagina di accesso di Microsoft.

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

4. Nella pagina di accesso, inserisci l'indirizzo email e la password registrati sul sito di supporto NetApp per eseguire il processo di autenticazione.

   Queste azioni consentono alla Console di utilizzare il tuo account NSS per attività quali download di licenze, verifica di aggiornamenti software e future registrazioni di supporto.

   Notare quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account ospite o temporaneo). È possibile avere più account NSS a livello di cliente.
   - Può esserci un solo account NSS se tale account è un account a livello di partner. Se provi ad aggiungere account NSS a livello di cliente ed esiste già un account a livello di partner, riceverai il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account poiché sono già presenti utenti NSS di tipo diverso."

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

   - Dopo aver effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che corrisponde al tuo indirizzo email. Nella pagina **Gestione NSS**, puoi visualizzare la tua email da ••• menu.

   - Se hai bisogno di aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Aggiorna credenziali** in ••• menu.

     Utilizzando questa opzione ti verrà richiesto di effettuare nuovamente l'accesso. Si noti che il token per questi account scade dopo 90 giorni. Verrà pubblicata una notifica per avvisarti di ciò.

Ottieni aiuto

NetApp fornisce supporto per NetApp Console e i suoi servizi cloud in vari modi. Sono disponibili ampie opzioni di auto-supporto gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include supporto tecnico remoto tramite ticket web.

Ottieni supporto per un servizio file di un provider cloud

Per il supporto tecnico relativo al servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Per ricevere supporto tecnico specifico per NetApp e le sue soluzioni di storage e servizi dati, utilizzare le opzioni di supporto descritte di seguito.

Utilizzare opzioni di auto-supporto

Queste opzioni sono disponibili gratuitamente, 24 ore al giorno, 7 giorni alla settimana:

- Documentazione

  La documentazione NetApp Console che stai visualizzando.

- "Base di conoscenza"

  Cerca nella knowledge base NetApp per trovare articoli utili per la risoluzione dei problemi.

- "Comunità"

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

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo aver attivato il supporto.

Prima di iniziare

- Per utilizzare la funzionalità **Crea un caso**, devi prima associare le credenziali del sito di supporto NetApp all'accesso alla console. "Scopri come gestire le credenziali associate al tuo accesso alla Console" .
- Se stai aprendo un caso per un sistema ONTAP che ha un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Nella pagina **Risorse**, seleziona una delle opzioni disponibili in Supporto tecnico:

a. Seleziona **Chiamaci** se desideri parlare con qualcuno al telefono. Verrai indirizzato a una pagina su netapp.com in cui sono elencati i numeri di telefono che puoi chiamare.

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

   - **Servizio**: seleziona il servizio a cui è associato il problema. Ad esempio, * NetApp Console* quando si tratta di un problema specifico di supporto tecnico con flussi di lavoro o funzionalità all'interno della Console.
   - **Sistema**: se applicabile all'archiviazione, selezionare * Cloud Volumes ONTAP* o **On-Prem** e quindi l'ambiente di lavoro associato.

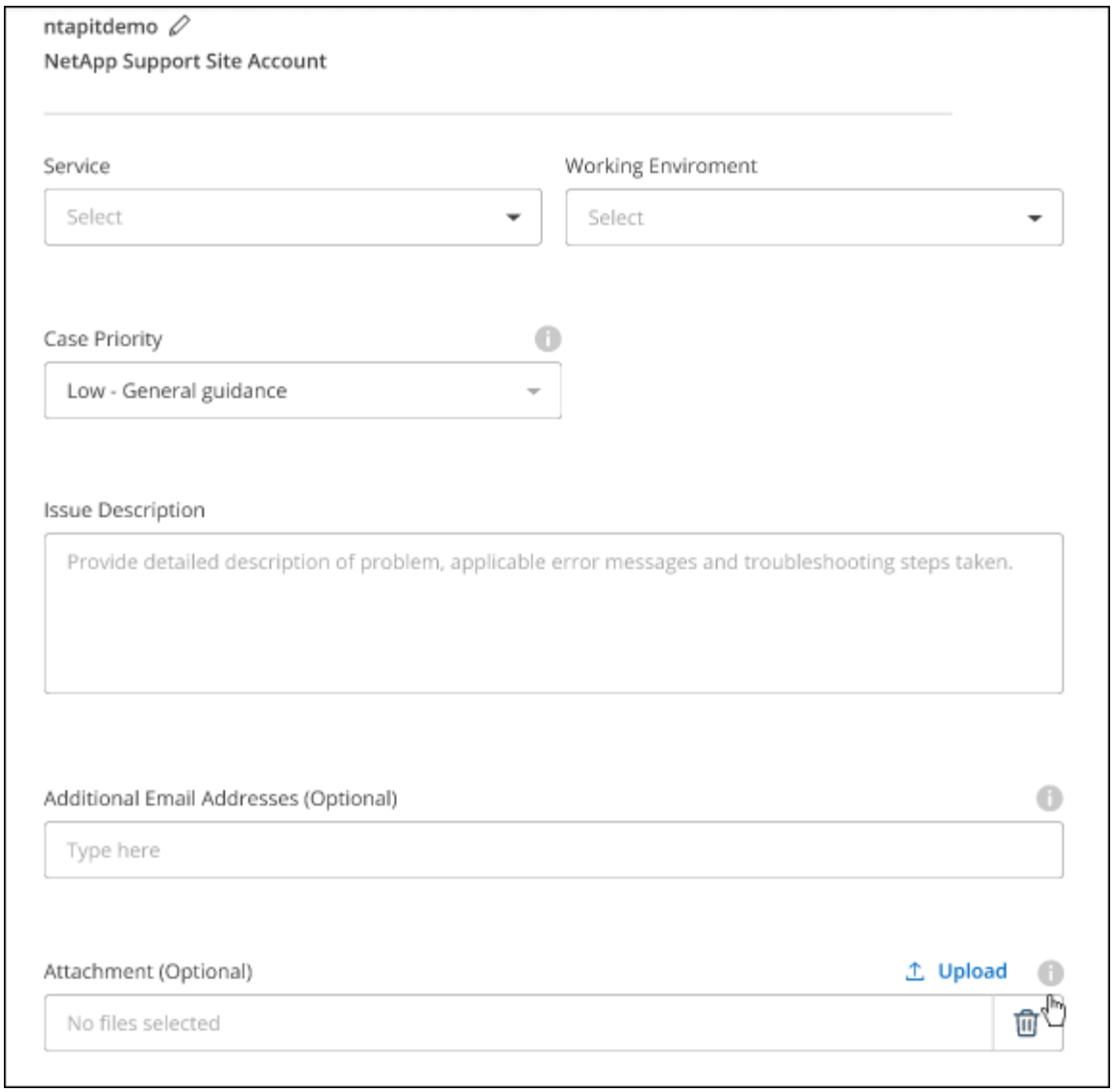
     L'elenco dei sistemi rientra nell'ambito dell'organizzazione della Console e dell'agente della Console selezionato nel banner in alto.

   - **Priorità del caso**: scegli la priorità del caso, che può essere Bassa, Media, Alta o Critica.

     Per saperne di più su queste priorità, passa il mouse sull'icona informativa accanto al nome del campo.

   - **Descrizione del problema**: fornisci una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o passaggi per la risoluzione dei problemi eseguiti.
   - **Indirizzi email aggiuntivi**: inserisci altri indirizzi email se desideri informare qualcun altro di questo problema.
   - **Allegato (facoltativo)**: carica fino a cinque allegati, uno alla volta.

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



Dopo aver finito

Apparirà una finestra pop-up con il numero del tuo caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

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

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

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

Questo errore potrebbe indicare che l'account NSS e la società registrata a cui è associato non corrispondono alla stessa società registrata per il numero di serie dell'account NetApp Console (ad esempio 960xxxx) o il numero di serie dell'ambiente di lavoro. Puoi richiedere assistenza utilizzando una delle seguenti opzioni:

- Invia un caso non tecnico a https://mysupport.netapp.com/site/help

Gestisci i tuoi casi di supporto

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

Notare quanto segue:

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

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

  Per maggiori dettagli, vedere i passaggi riportati di seguito.
- A livello di singolo caso, offriamo la possibilità di aggiornare le note del caso o di chiudere un caso che non sia già nello stato Chiuso o In attesa di chiusura.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Seleziona **Gestione casi** e, se richiesto, aggiungi il tuo account NSS alla Console.

   La pagina **Gestione casi** mostra i casi aperti relativi all'account NSS associato al tuo account utente della Console. Si tratta dello stesso account NSS che appare in cima alla pagina **Gestione NSS**.
3. Facoltativamente, modifica le informazioni visualizzate nella tabella:
   - In **Casi dell'organizzazione**, seleziona **Visualizza** per visualizzare tutti i casi associati alla tua azienda.
   - Modifica l'intervallo di date scegliendo un intervallo di date esatto o un intervallo di tempo diverso.
   - Filtra il contenuto delle colonne.
   - Modifica le colonne che appaiono nella tabella selezionando e quindi scegli le colonne che desideri visualizzare.
4. Gestisci un caso esistente selezionando e selezionando una delle opzioni disponibili:
   - **Visualizza caso**: visualizza i dettagli completi su un caso specifico.
   - **Aggiorna note sul caso**: fornisci ulteriori dettagli sul tuo problema o seleziona **Carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Chiudi caso**: fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.

Domande frequenti su NetApp Ransomware Resilience

Questa sezione FAQ può aiutarti se stai cercando una risposta rapida a una domanda su NetApp Ransomware Resilience.

Distribuzione

Hai bisogno di una licenza per utilizzare Ransomware Resilience?

È possibile utilizzare i seguenti tipi di licenza:

- Registrati per una prova gratuita di 30 giorni.
- Acquista un abbonamento pay-as-you-go (PAYGO) a NetApp Intelligent Services e Ransomware Resilience con Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace e Microsoft Azure Marketplace.
- Bring your own license (BYOL), ovvero un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante di vendita NetApp . Puoi utilizzare il numero di serie della licenza per attivare BYOL nella sezione Licenses and subscriptions della Console.

Come si abilita la Ransomware Resilience?

È possibile accedere a Ransomware Resilience dalla NetApp Console. Assicurati di aver "ruoli di accesso" E "prerequisiti". Se hai configurato correttamente un agente Console, puoi quindi "scoprire i carichi di lavoro".

Per maggiori informazioni, vedere"Access Ransomware Resilience" E"Guida rapida alla resilienza del ransomware" .

Ransomware Resilience è disponibile nelle modalità standard, limitata e privata?

Al momento, Ransomware Resilience è disponibile solo in modalità standard.

Per una spiegazione su queste modalità in tutti i servizi dati NetApp , fare riferimento a "Modalità di distribuzione NetApp Console" .

Accesso

Qual è l'URL di Ransomware Resilience?

In un browser, inserisci "https://console.netapp.com/ransomware-resilience" per accedere alla Console.

Come vengono gestiti i permessi di accesso?

"Scopri di più sui ruoli di accesso alla console per tutti i servizi". Ransomware Resilience ha anche "ruoli di accesso dedicati".

Quale risoluzione del dispositivo è migliore?

La risoluzione del dispositivo consigliata per Ransomware Resilience è 1920x1080 o superiore.

Quale browser dovrei usare?

È possibile accedere alla NetApp Console con qualsiasi browser Web moderno.

Interoperabilità

Ransomware Resilience è a conoscenza delle impostazioni di protezione in ONTAP?

Sì, Ransomware Resilience rileva le pianificazioni degli snapshot impostate in ONTAP.

In che modo Ransomware Resilience interagisce con NetApp Backup and Recovery e SnapCenter?

Ransomware Resilience interagisce con Backup and Recovery per individuare e impostare policy di snapshot e backup per i carichi di lavoro di condivisione file.

Ransomware Resilience funziona con SnapCenter o SnapCenter per VMware per individuare e impostare policy di snapshot e backup per carichi di lavoro di applicazioni e VM.

Ransomware Resilience funziona anche con Backup and Recovery e SnapCenter (incluso SnapCenter per VMware) per eseguire un ripristino coerente con i file e i carichi di lavoro.

Per quanto riguarda le licenze e la fatturazione, Ransomware Resilience può integrarsi con Backup and Recovery anche se non si dispone di una licenza separata per Backup and Recovery. Se disponi sia di Backup and Recovery che di Ransomware Resilience, tutti i dati comuni protetti da entrambi i prodotti verranno fatturati solo da Ransomware Resilience.

Carichi di lavoro

Cos'è un carico di lavoro nel contesto della resilienza al ransomware?

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, si consideri un database Oracle distribuito su ora3.host.com con `vol1` contenente dati e `vol2` contenente registri. I due volumi costituiscono il carico di lavoro per quell'istanza di Oracle Database.

In che modo Ransomware Resilience assegna la priorità ai dati del carico di lavoro?

La priorità del carico di lavoro (critica, standard, importante) è determinata dalle frequenze degli snapshot già applicate a ciascun volume associato al carico di lavoro e dai backup pianificati.

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

Quali carichi di lavoro supporta Ransomware Resilience?

Ransomware Resilience è in grado di identificare i seguenti carichi di lavoro: Oracle, condivisioni di file, storage a blocchi, VM e datastore di VM.

Se utilizzi SnapCenter o SnapCenter per VMware, tutti i carichi di lavoro supportati da questi prodotti sono identificati anche in Ransomware Resilience. Ransomware Resilience può proteggere e ripristinare SnapCenter e i carichi di lavoro SnapCenter in modo coerente con il carico di lavoro.

Come si associano i dati a un carico di lavoro?

Ransomware Resilience rileva i volumi e le estensioni dei file e li associa al carico di lavoro appropriato.

Se disponi SnapCenter o SnapCenter per VMware e hai configurato carichi di lavoro in Backup e ripristino, Ransomware Resilience rileva i carichi di lavoro gestiti da SnapCenter e SnapCenter per VMware e i volumi associati.

Che cosa è un carico di lavoro protetto?

In Ransomware Resilience, un carico di lavoro mostra uno stato di **protetto** quando ha una policy di

rilevamento primaria abilitata, ovvero "Protezione autonoma dal ransomware (ARP)" è abilitato su tutti i volumi correlati al carico di lavoro.

Che cosa si intende per carico di lavoro "a rischio"?

Se un carico di lavoro non ha un criterio di rilevamento primario abilitato, viene etichettato come "a rischio" anche se ha un criterio di backup e snapshot abilitato. Per la protezione dal ransomware, dovresti abilitare un "politica di rilevamento".

Ho aggiunto un nuovo volume, ma non è ancora uscito. Cosa dovrei fare?

Se hai aggiunto un nuovo volume al tuo ambiente, avvia nuovamente l'individuazione del carico di lavoro. Dopo che il volume è stato scoperto, "applicare policy di protezione per proteggere il nuovo volume".

Politiche di protezione

Le policy ransomware Ransomware Resilience coesistono con altri tipi di policy relative ai carichi di lavoro?

Al momento, Backup e ripristino (Cloud Backup) supporta un criterio di backup per volume. Se si configura la protezione del backup con Backup e ripristino, questa condivide i criteri di backup con Ransomware Resilience.

Le copie snapshot non hanno limiti e possono essere aggiunte separatamente da ciascun servizio.

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

UN "strategia di protezione dal ransomware" richiede:

- una politica di rilevamento del ransomware e
- una politica di snapshot

Nella strategia Ransomware Resilience non è richiesta una policy di backup.

Ransomware Resilience è a conoscenza delle impostazioni di protezione in ONTAP?

Sì, Ransomware Resilience rileva le pianificazioni degli snapshot impostate in ONTAP. Rileva inoltre se ARP e FPolicy sono abilitati su tutti i volumi in un carico di lavoro rilevato. Le informazioni visualizzate nella Ransomware Resilience Dashboard sono aggregate da altre soluzioni e prodotti NetApp .

Ransomware Resilience è a conoscenza delle policy già definite in Backup and Recovery e SnapCenter?

Sì, se hai carichi di lavoro gestiti in Backup and Recovery o SnapCenter, le policy gestite da tali prodotti vengono importate in Ransomware Resilience.

È possibile modificare le policy trasferite da NetApp Backup and Recovery e/o SnapCenter?

No, non è possibile modificare i criteri gestiti da Backup and Recovery o SnapCenter da Ransomware Resilience. È possibile gestire eventuali modifiche a tali criteri in Backup e ripristino o SnapCenter.

Se esistono policy di ONTAP (come ARP, FPolicy e snapshot), queste vengono modificate in Ransomware Resilience?

No. Ransomware Resilience non modifica alcuna policy di rilevamento esistente (impostazioni ARP, FPolicy) da ONTAP.

Cosa succede se aggiungi nuove policy in Backup and Recovery o SnapCenter dopo aver effettuato la registrazione a Ransomware Resilience?

Ransomware Resilience riconosce le policy appena create e le modifiche alle policy in Backup and Recovery o SnapCenter.

È possibile modificare le politiche di ONTAP?

Sì, è possibile modificare le policy da ONTAP in Ransomware Resilience. È anche possibile creare nuove policy in Ransomware Resilience e applicarle ai carichi di lavoro. Questa azione sostituisce le policy ONTAP esistenti con le policy create in Ransomware Resilience.

È possibile disattivare le policy in ONTAP?

È possibile disabilitare ARP nei criteri di rilevamento tramite l'interfaccia utente di System Manager, le API o la CLI in ONTAP.

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

Note legali

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

Copyright

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

Marchi

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

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

Brevetti

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

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

Politica sulla riservatezza

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

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

- "Avviso per la NetApp Console"

Informazioni sul copyright

Informazioni sul marchio commerciale