Note di rilascio

NetApp Ransomware Resilience

NetApp
February 12, 2026

Sommario

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.