Note di rilascio

BlueXP ransomware protection

NetApp
December 20, 2024

Sommario

Note di rilascio 1
Novità di BlueXP per la protezione dal ransomware 1

Note di rilascio

Novità di BlueXP per la protezione dal ransomware

Scopri le novità di BlueXP ransomware Protection.

16 dicembre 2024

Rileva il comportamento anomalo degli utenti utilizzando Data Infrastructure Insights Storage workload Security

Con questa release, puoi utilizzare Data Infrastructure Insights Storage workload Security per rilevare il comportamento anomalo degli utenti nei workload di storage. Questa funzionalità ti aiuta a identificare potenziali minacce alla sicurezza e a bloccare utenti potenzialmente malintenzionati per proteggere i tuoi dati.

Per ulteriori informazioni, fare riferimento alla "Rispondi a un avviso ransomware rilevato".

Prima di utilizzare Data Infrastructure Insights Storage workload Security per rilevare il comportamento anomalo degli utenti, devi configurare l'opzione utilizzando l'opzione protezione dal ransomware BlueXP **Impostazioni**.

Fare riferimento alla "Configurare le impostazioni di protezione dal ransomware BlueXP".

Seleziona i workload da rilevare e proteggere

Con questa versione, è possibile effettuare le seguenti operazioni:

- All'interno di ogni connettore, seleziona gli ambienti di lavoro in cui desideri rilevare i carichi di lavoro. Questa funzionalità può essere utile se si desidera proteggere carichi di lavoro specifici del proprio ambiente e non di altri.
- Durante il rilevamento dei carichi di lavoro, è possibile abilitare il rilevamento automatico dei carichi di lavoro per ogni connettore. Questa funzionalità consente di selezionare i carichi di lavoro da proteggere.
- Scopri i workload appena creati per gli ambienti di lavoro selezionati in precedenza.

Fare riferimento alla "Rileva i carichi di lavoro".

7 novembre 2024

Abilitare la classificazione dei dati e la scansione delle informazioni di identificazione personale (PII)

Con questa release, puoi abilitare la classificazione BlueXP , un componente fondamentale della famiglia BlueXP , per analizzare e classificare i dati nei carichi di lavoro di condivisione file. La classificazione dei dati ti aiuta a capire se i tuoi dati includono informazioni personali o private, con conseguenti rischi per la sicurezza. Questo processo influisce anche sull'importanza dei carichi di lavoro e ti aiuta ad assicurare che tu stia proteggendo i carichi di lavoro con il giusto livello di protezione.

L'analisi dei dati PII nella protezione ransomware BlueXP è generalmente disponibile per i clienti che hanno implementato la classificazione BlueXP . La classificazione BlueXP è disponibile come parte della piattaforma BlueXP senza costi aggiuntivi e può essere implementata on-premise o nel cloud del cliente.

Fare riferimento alla "Configurare le impostazioni di protezione dal ransomware BlueXP".

Per avviare la scansione, nella pagina protezione, fare clic su **identifica esposizione** nella colonna esposizione privacy.

"Eseguire la scansione dei dati sensibili identificabili personalmente con la classificazione BlueXP ".

Integrazione SIEM con Microsoft Sentinel

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

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

Prova gratuita ora 30 giorni

Con questa release, le nuove implementazioni della protezione ransomware BlueXP ora hanno 30 giorni per una prova gratuita. In precedenza, la protezione ransomware di BlueXP ha fornito 90 giorni come prova gratuita. Se sei già in prova gratuita di 90 giorni, l'offerta continua per i 90 giorni.

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

Prima di ripristinare un workload dell'applicazione a livello di file, è possibile visualizzare un elenco di file che potrebbero essere stati coinvolti da un attacco e identificare quelli che si desidera ripristinare. In precedenza, se i connettori BlueXP di un'organizzazione (in precedenza un account) utilizzavano Podman, questa funzionalità era disattivata. Ora è abilitato per Podman. Puoi permettere alla protezione anti-ransomware di BlueXP di scegliere i file da ripristinare, caricare un file CSV che elenca tutti i file interessati da un avviso o identificare manualmente i file da ripristinare.

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

30 settembre 2024

Raggruppamento personalizzato dei carichi di lavoro di condivisione file

Con questa release, puoi raggruppare le condivisioni di file in gruppi per semplificare la protezione dell'ambiente dati. Il servizio può proteggere tutti i volumi in un gruppo allo stesso tempo. In precedenza, era necessario proteggere ciascun volume separatamente.

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

2 settembre 2024

Valutazione dei rischi di protezione di Digital Advisor

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

Fare riferimento alla "Documentazione di Digital Advisor".

Esegui il backup su Google Cloud Platform

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

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

Supporto per Google Cloud Platform

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

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

Controllo degli accessi in base al ruolo

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

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

5 agosto 2024

Rilevamento delle minacce con Splunk Cloud

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

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

1 luglio 2024

BYOL

Con questa versione, è possibile utilizzare una licenza BYOL, ovvero un file di licenza NetApp (NLF) che si ottiene dal proprio rappresentante di vendita NetApp

"Ulteriori informazioni sull'impostazione delle licenze".

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

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

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

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

Scaricare un elenco dei file interessati

Prima di ripristinare un workload dell'applicazione a livello di file, è possibile accedere alla pagina Avvisi per scaricare un elenco di file interessati in un file CSV, quindi utilizzare la pagina di ripristino per caricare il file CSV.

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

Eliminare il piano di protezione

Con questa release, ora puoi eliminare una strategia di protezione dal ransomware.

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

10 giugno 2024

Blocco delle copie Snapshot sullo storage primario

Abilitare questo blocco per bloccare le copie Snapshot sullo storage primario in modo che non possano essere modificate o eliminate per un determinato periodo di tempo anche in caso di attacco ransomware che smetta di raggiungere la destinazione storage di backup.

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

Supporto di Cloud Volumes ONTAP per Microsoft Azure

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

"Avvio rapido di Cloud Volumes ONTAP in Azure"

"Scopri di più sulla protezione ransomware di BlueXP".

Microsoft Azure aggiunto come destinazione di backup

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

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

14 maggio 2024

Aggiornamenti delle licenze

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

"Ulteriori informazioni sull'impostazione delle licenze".

Protocollo CIFS

Il servizio ora supporta ONTAP e Cloud Volumes ONTAP on-premise negli ambienti di lavoro AWS con

protocolli NFS e CIFS. La release precedente supportava solo il protocollo NFS.

Dettagli sui carichi di lavoro

Questa versione fornisce ora ulteriori dettagli sulle informazioni sul carico di lavoro dalle pagine protezione e altre per una migliore valutazione della protezione del carico di lavoro. Dai dettagli del carico di lavoro, è possibile esaminare il criterio attualmente assegnato e le destinazioni di backup configurate.

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

Protezione e recovery coerenti con l'applicazione e con le macchine virtuali

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

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

Strategie di protezione dal ransomware

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

- Policy di Snapshot
- Policy di backup
- Policy di rilevamento

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

Rilevamento delle minacce

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

"Ulteriori informazioni sulla configurazione delle opzioni di impostazione".

Ignora gli avvisi falsi positivi

Dalla scheda Avvisi, è ora possibile eliminare i falsi positivi o decidere di recuperare immediatamente i dati.

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

Stato di rilevamento

Nuovi stati di rilevamento vengono visualizzati nella pagina di protezione, che mostra lo stato del rilevamento di ransomware applicato al workload.

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

Scaricare i file CSV

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

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

Collegamento alla documentazione

Il collegamento per la visualizzazione della documentazione è ora incluso nell'interfaccia utente. È possibile accedere a questa documentazione dall'opzione verticale **azioni** del dashboard  . Seleziona **Novità** per visualizzare i dettagli nelle Note sulla versione o **documentazione** per visualizzare la home page della documentazione relativa alla protezione dal ransomware di BlueXP.

Backup e ripristino BlueXP

Il servizio di backup e recovery di BlueXP non deve più essere già abilitato nell'ambiente di lavoro. Vedere "prerequisiti". Il servizio di protezione dal ransomware di BlueXP aiuta a configurare una destinazione di backup tramite l'opzione Settings. Vedere "Configurare le impostazioni".

Impostazioni

Ora puoi configurare destinazioni di backup nelle impostazioni di protezione dal ransomware BlueXP .

"Ulteriori informazioni sulla configurazione delle opzioni di impostazione".

5 marzo 2024

Gestione delle policy di protezione

Oltre a utilizzare criteri predefiniti, è ora possibile creare criteri. "Ulteriori informazioni sulla gestione dei criteri".

Immutabilità sullo storage secondario (DataLock)

È ora possibile rendere immutabile il backup nello storage secondario utilizzando la tecnologia DataLock di NetApp nell'archivio di oggetti. "Ulteriori informazioni sulla creazione di criteri di protezione".

Backup automatico su NetApp StorageGRID

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

Funzioni aggiuntive per esaminare potenziali attacchi

Ora puoi visualizzare ulteriori dettagli forensi per analizzare il potenziale attacco rilevato. "Scopri di più sulla risposta a un avviso ransomware rilevato".

Processo di ripristino

Il processo di ripristino è stato migliorato. Ora è possibile ripristinare volume per volume o tutti i volumi per un carico di lavoro. "Scopri di più sul ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti)".

"Scopri di più sulla protezione ransomware di BlueXP".

6 ottobre 2023

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

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

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

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

"Scopri di più sulla protezione ransomware di BlueXP".