Informazioni sulla protezione dal ransomware NetApp

ONTAP 9

NetApp
August 31, 2024

Sommario

Informazioni sulla protezione dal ransomware NetApp

Il portfolio di protezione di NetApp e ransomware

Il ransomware resta una delle minacce più significative che causano l'interruzione del business per le organizzazioni nel 2024. Secondo il "Sophos state of ransomware 2024", gli attacchi ransomware hanno colpito il 72% dei partecipanti intervistati. Gli attacchi ransomware si sono evoluti per diventare più sofisticati e mirati, con i soggetti delle minacce che utilizzano tecniche avanzate come l'intelligenza artificiale per massimizzare il loro impatto e i loro profitti.

Le organizzazioni devono guardare nell'intera posizione di sicurezza da perimetro, rete, identità, applicazioni e dove si trovano i dati a livello di storage e mettere al sicuro questi layer. L'adozione di un approccio incentrato sui dati alla cyber Protection nel layer di storage è fondamentale nel panorama odierno delle minacce. Anche se non esiste una singola soluzione in grado di bloccare tutti gli attacchi, l'uso di un portfolio di soluzioni, inclusi partnership e terze parti, offre una difesa a più layer.

Portfolio di prodotti NetAppFornisce vari strumenti efficaci per visibilità, rilevamento e correzione, in modo da rilevare tempestivamente il ransomware, prevenire la diffusione e ripristinare rapidamente, se necessario, per evitare costosi downtime. Le soluzioni di difesa tradizionali a layer rimangono le più diffuse, così come quelle di partner e terze parti per la visibilità e il rilevamento. Una correzione efficace rimane una parte fondamentale della risposta a qualsiasi minaccia. L'esclusivo approccio di settore che sfrutta la tecnologia Snapshot NetApp immutabile e la soluzione con interfaccia logica SnapLock è un fattore di differenziazione nel settore e una Best practice nel settore per le funzionalità di correzione dal ransomware.

> A partire da luglio 2024, il contenuto del report tecnico *TR-4572: NetApp ransomware Protection*, precedentemente pubblicato come PDF, è stato integrato con il resto della documentazione di prodotto ONTAP.

I dati sono la destinazione primaria

I criminali informatici si rivolgono sempre più direttamente ai dati, riconoscendo il loro valore. Sebbene la sicurezza perimetrale, di rete e delle applicazioni siano importanti, è possibile ignorarle. La focalizzazione sulla protezione dei dati all'origine, il layer di storage, fornisce un'ultima linea critica di difesa. L'obiettivo degli attacchi ransomware è ottenere l'accesso ai dati di produzione, crittografarli o renderli inaccessibili. Per raggiungere questo obiettivo, gli autori degli attacchi devono aver già forato le difese esistenti implementate dalle organizzazioni oggi, dal perimetro alla sicurezza delle applicazioni.

[Livelli di sicurezza dal perimetro alla sicurezza dei dati]

Purtroppo, molte organizzazioni non sfruttano le funzionalità di sicurezza a livello di dati. È qui che entra in gioco il portfolio di protezione ransomware di NetApp, con la protezione che trovi all'ultima linea di difesa.

Il costo reale del ransomware

Il pagamento del riscatto in sé non costituisce l'effetto monetario più grande per un'azienda. Anche se il pagamento non è insignificante, sale in confronto al costo dei downtime dovuti alla sofferenza di un incidente ransomware.

I pagamenti dei riscatti sono solo un elemento dei costi di recovery legati agli eventi ransomware. Escludendo qualsiasi riscatto pagato, nel 2024 le organizzazioni hanno riferito un costo medio per il recovery da un attacco ransomware di 2,73M milioni di dollari, un aumento di quasi 1M milioni di dollari rispetto ai 1,82M milioni di dollari registrati nel 2023, secondo il "2024 Sophos state of ransomware" report. Per le organizzazioni che dipendono fortemente dalla disponibilità IT, come l'e-commerce, il trading di azioni e l'assistenza sanitaria, i costi possono essere 10 volte superiori o più.

Anche i costi dell'assicurazione informatica continuano ad aumentare, considerata la verosimile probabilità che si verifichi un attacco ransomware sulle aziende assicurate.

Protezione dal ransomware ai layer di dati

NetApp comprende che il tuo livello di sicurezza è ampio e profondo in tutta l'organizzazione, dal perimetro alla posizione in cui risiedono i dati nel layer di storage. Lo stack di sicurezza è complesso e dovrebbe fornire sicurezza a ogni livello dello stack tecnologico.

La protezione in real-time a livello di dati è ancora più importante e ha requisiti specifici. Per essere efficaci, le soluzioni di questo livello devono offrire questi attributi critici:

- **Sicurezza per progettazione** per ridurre al minimo la possibilità di un attacco riuscito
- **Rilevamento e risposta in tempo reale** per ridurre al minimo l'impatto di un attacco riuscito
- **Protezione WORM a mappatura D'aria** per isolare i backup dei dati critici
- **Un singolo piano di controllo** per una difesa ransomware completa

NetApp è in grado di offrire tutto questo e molto altro.

[Portfolio di protezione dal ransomware di NetApp che include gli attributi critici descritti]

Il portfolio di protezione dal ransomware di NetApp

NetApp "protezione dal ransomware integrata"offre una difesa real-time, solida e sfaccettata per i tuoi dati critici. Al centro, gli algoritmi di rilevamento avanzati basati sull'ai monitorano costantemente i modelli di dati, identificando rapidamente le potenziali minacce ransomware con una precisione del 99%. La rapida reazione agli attacchi consente al nostro storage di creare rapidamente un snapshot dei dati e di proteggere le copie, garantendo un rapido recovery.

Per rafforzare ulteriormente i dati, "replica informatica"la capacità di NetApp isola i dati con un'air gap logica. Salvaguardando i dati critici, garantiamo una rapida business continuity.

NetApp "Protezione ransomware BlueXP"riduce gli oneri operativi con un singolo pannello di controllo per coordinare ed eseguire in modo intelligente una difesa ransomware incentrata sul carico di lavoro end-to-end. In questo modo puoi identificare e proteggere i dati critici dei carichi di lavoro a rischio con un singolo clic, rilevare e rispondere in modo preciso e automatico per limitare l'impatto di un potenziale attacco e ripristinare i carichi di lavoro in pochi minuti, e non giorni, proteggendo i dati importanti del carico di lavoro e riducendo al minimo le costose interruzioni.

In quanto soluzione ONTAP integrata e nativa per la protezione degli accessi non autorizzati ai dati, "Verifica multi-admin (MAV)" dispone di un solido set di funzionalità che garantiscono l'esecuzione di operazioni quali l'eliminazione di volumi, la creazione di ulteriori utenti amministrativi o l'eliminazione di copie Snapshot solo dopo le approvazioni di almeno un secondo amministratore designato. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati. È possibile configurare tutti i responsabili dell'approvazione dell'amministratore designati che si desidera prima di eliminare una copia snapshot.

NetApp ONTAP soddisfa i requisiti per l' "Autenticazione a più fattori (MFA)"autenticazione CLI basata su web in System Manager e SSH.

La protezione dal ransomware di NetApp offre tranquillità in un panorama di minacce in continua evoluzione. Il suo approccio completo non solo si difende dalle attuali varianti di ransomware, ma si adatta anche alle minacce emergenti, garantendo sicurezza a lungo termine per la tua infrastruttura dati.

Ulteriori informazioni sulle altre opzioni di protezione

- "Protezione dal ransomware Active IQ"
- "Sicurezza dei workload di storage Cloud Insights (CISWS)"
- "FPolicy"
- "Copie Snapshot SnapLock e a prova di manomissione"

Garanzia di recovery dal ransomware

NetApp offre una garanzia di ripristino dei dati Snapshot in caso di attacco ransomware. La nostra garanzia: Se non possiamo aiutarvi a ripristinare i vostri dati snapshot, noi lo faremo. La garanzia è disponibile sui nuovi acquisti dei sistemi AFF A-Series, AFF C-Series, ASA e FAS.

Scopri di più

- "Descrizione del servizio di garanzia di recupero"
- "Blog sulla garanzia di recovery dal ransomware".

Informazioni correlate

- Pagina delle risorse del sito di supporto NetApp http://mysupport.netapp.com/ontap/resources
- Sicurezza dei prodotti NetApp https://security.netapp.com/resources/

Copie Snapshot SnapLock e a prova di manomissione per la protezione dal ransomware

Un'arma vitale nell'arsenale Snap di NetApp è SnapLock, che si è dimostrato altamente efficace nel proteggere dalle minacce ransomware. Prevenendo la cancellazione non autorizzata dei dati, SnapLock fornisce un ulteriore livello di sicurezza, garantendo che i dati critici rimangano intatti e accessibili anche in caso di attacchi dannosi.

Conformità SnapLock

SnapLock Compliance (SLC) fornisce una protezione indelebile dei tuoi dati. SLC impedisce l'eliminazione dei dati anche quando un amministratore tenta di reinizializzare l'array. A differenza di altri prodotti della concorrenza, SnapLock Compliance non è vulnerabile agli attacchi di social engineering attraverso i team di supporto di questi prodotti. I dati protetti da SnapLock Compliance Volumes sono ripristinabili fino a quando tali dati non hanno raggiunto la data di scadenza.

Per abilitare SnapLock, "ONTAP uno"è necessaria una licenza.

Scopri di più

- "Documentazione SnapLock"

Copie Snapshot a prova di manomissione

Le copie Snapshot a prova di manomissione (TPS) offrono un modo rapido e pratico per proteggere i dati da atti dannosi. A differenza di SnapLock Compliance, il TPS viene in genere utilizzato sui sistemi primari in cui l'utente può proteggere i dati per un determinato periodo di tempo e lasciato localmente per ripristini rapidi o in cui i dati non devono essere replicati dal sistema primario. TPS utilizza tecnologie SnapLock per impedire l'eliminazione della copia snapshot primaria anche da parte di un amministratore ONTAP utilizzando lo stesso periodo di scadenza della conservazione SnapLock. La cancellazione della copia Snapshot viene impedita anche se il volume non è abilitato per SnapLock, sebbene gli snapshot non abbiano la stessa natura indelebile dei volumi SnapLock Compliance.

Per rendere le copie snapshot a prova di manomissione, "ONTAP uno"è necessaria una licenza.

Scopri di più

- "Blocca una copia snapshot per proteggerti dagli attacchi ransomware".

Blocco dei file FPolicy

FPolicy blocca la memorizzazione dei file indesiderati nell'appliance di storage Enterprise. FPolicy ti offre inoltre un modo per bloccare le estensioni di file ransomware note. Un utente dispone ancora delle autorizzazioni di accesso completo alla cartella principale, ma FPolicy non consente a un utente di memorizzare i file contrassegnati dall'amministratore come bloccati. Non importa se quei file sono file MP3 o estensioni note di file ransomware.

Blocco dei file dannosi con la modalità nativa di FPolicy

La modalità nativa di NetApp FPolicy (un'evoluzione del nome, file Policy) è un framework di blocco delle estensioni di file che consente di impedire che estensioni di file indesiderate entrino nell'ambiente. Fa parte di ONTAP da oltre dieci anni ed è incredibilmente utile per aiutarti a proteggerti dai ransomware. Questo motore Zero Trust è utile perché offre ulteriori misure di sicurezza oltre i permessi dell'elenco di controllo degli accessi (ACL).

In Gestione di sistema di ONTAP e BlueXP , è disponibile un elenco di oltre 3000 estensioni di file come riferimento.

> Alcune estensioni potrebbero essere legittime nell'ambiente e il loro blocco può causare problemi imprevisti. Prima di configurare FPolicy nativo, creare un elenco personalizzato appropriato per l'ambiente in uso.

La modalità nativa FPolicy è inclusa in tutte le licenze ONTAP.

Scopri di più

- "Blog: Combattere il ransomware: Parte tre — ONTAP FPolicy, un altro potente tool nativo (anche noto come gratuito)"

Abilitare l'analisi del comportamento di utenti ed entità (UEBA) con la modalità esterna FPolicy

La modalità esterna FPolicy è un framework di controllo e notifica delle attività dei file che fornisce visibilità delle attività degli utenti e dei file. Queste notifiche possono essere utilizzate da una soluzione esterna per

eseguire analytics basati su ai per rilevare comportamenti dannosi.

La modalità esterna FPolicy può anche essere configurata in modo da attendere l'approvazione dal server FPolicy prima di consentire l'esecuzione di attività specifiche. In un cluster è possibile configurare più policy di questo tipo, per una maggiore flessibilità.

> I server FPolicy devono rispondere alle richieste FPolicy se configurati per fornire l'approvazione; altrimenti, le performance del sistema storage potrebbero avere un impatto negativo.

La modalità esterna FPolicy è inclusa in "Tutte le licenze ONTAP".

Scopri di più

- "Blog: Combattere il ransomware: Parte quarta — UBA e ONTAP con modalità esterna FPolicy."

Sicurezza dei workload di storage Cloud Insights (CISWS)

Storage workload Security (SWS) è una funzionalità di NetApp Cloud Insights che migliora notevolmente il livello di sicurezza, la ripristinabilità e la responsabilità di un ambiente ONTAP. SWS adotta un approccio incentrato sull'utente, monitorando tutte le attività dei file da ogni utente autenticato nell'ambiente. Utilizza analytics avanzate per stabilire modelli di accesso normali e stagionali per ogni utente. Questi modelli vengono utilizzati per identificare rapidamente i comportamenti sospetti senza la necessità di firme ransomware.

Quando SWS rileva un potenziale attacco ransomware, alla cancellazione dei dati o all'esfiltrazione, può intraprendere azioni automatiche come:

- Creare un'istantanea del volume interessato.
- Bloccare l'account utente e l'indirizzo IP sospettati di attività dannose.
- Inviare un avviso agli amministratori.

Poiché può intraprendere azioni automatizzate per fermare rapidamente una minaccia interna e tenere traccia di ogni attività dei file, SWS rende il recovery da un evento ransomware molto più semplice e veloce. Con gli strumenti avanzati di audit e analisi forense integrati, gli utenti possono vedere immediatamente quali volumi e file sono stati influenzati da un attacco, da quale account utente proviene l'attacco e da quale azione dannosa è stata eseguita. Gli snapshot automatici riducono i danni e accelerano il ripristino dei file.

[Risultati degli attacchi alla sicurezza del workload dello storage Cloud Insights]

Gli avvisi della protezione autonoma da ransomware (ARP) di ONTAP sono visibili anche in SWS, che fornisce una singola interfaccia per i clienti che utilizzano sia ARP che SWS per proteggersi dagli attacchi ransomware.

Scopri di più

- "NetApp Cloud Insights"

Rilevazione e risposta NetApp ONTAP integrate on-box basata su ai

Mentre le minacce ransomware diventano sempre più sofisticate, i tuoi meccanismi di difesa dovrebbero farlo. La protezione autonoma da ransomware (ARP) di NetApp si basa sull'ai con rilevamento intelligente delle anomalie integrato in ONTAP. Attiva questa funzione per aggiungere un altro livello di difesa alla tua resilienza informatica.

ARP e ARP/ai sono configurabili tramite l'interfaccia di gestione integrata di ONTAP, System Manager, e abilitati in base al volume.

Protezione ransomware autonoma (ARP)

Protezione autonoma dal ransomware (ARP), un'altra soluzione nativa integrata nel ONTAP dal 9.10.1, analizza l'attività dei file di workload del volume di storage NAS e l'entropia dei dati per rilevare automaticamente il potenziale ransomware. ARP offre agli amministratori un rilevamento in tempo reale, informazioni approfondite e un punto di ripristino dei dati per un potenziale rilevamento ransomware on-box senza precedenti.

Per ONTAP 9.15,1 e le versioni precedenti che supportano ARP, ARP inizia in modalità di apprendimento per apprendere le attività tipiche dei dati del carico di lavoro. Questa operazione può richiedere sette giorni per la maggior parte degli ambienti. Una volta completata la modalità di apprendimento, ARP passerà automaticamente alla modalità attiva e inizierà a cercare attività anomale sui carichi di lavoro che potrebbero essere potenzialmente ransomware.

Se viene rilevata un'attività anomala, viene immediatamente creata una copia automatica dello snapshot, che fornisce un punto di ripristino il più vicino possibile al momento dell'attacco con un numero minimo di dati infetti. Allo stesso tempo, viene generato un avviso automatico (configurabile) che consente agli amministratori di visualizzare le attività anomale dei file in modo che possano determinare se l'attività è effettivamente dannosa e intraprendere le azioni appropriate.

Se l'attività è un carico di lavoro previsto, gli amministratori possono facilmente contrassegnarla come un falso positivo. ARP apprende questo cambiamento come attività normale del carico di lavoro e non lo contrassegna più come un potenziale attacco in futuro.

Per attivare ARP, "ONTAP uno"è necessaria una licenza.

Scopri di più

- "Protezione ransomware autonoma"

Protezione autonoma da ransomware/ai (ARP/ai)

Introdotto come anteprima tecnica in ONTAP 9.15,1, ARP/ai porta il rilevamento in tempo reale on-box dei sistemi storage NAS a un livello superiore. La nuova tecnologia di rilevamento basata sull'ai è preparata su oltre un milione di file e vari attacchi ransomware noti. Oltre ai segnali utilizzati in ARP, ARP/ai rileva anche la cifratura dell'intestazione. La potenza ai e i segnali aggiuntivi consentono ad ARP/ai di fornire una precisione di rilevamento superiore al 99%. Questo è stato convalidato da se Labs, un laboratorio di test indipendente che ha assegnato ad ARP/ai la più alta classificazione AAA.

Poiché l'addestramento dei modelli avviene continuamente nel cloud, ARP/ai non richiede una modalità di apprendimento. È attivo nel momento in cui viene acceso. Il training continuo significa anche che l'ARP/ai è sempre validata a fronte di nuovi tipi di attacchi ransomware man mano che si presentano. ARP/ai include

anche funzionalità di aggiornamento automatico che forniscono nuovi parametri a tutti i clienti per mantenere aggiornato il rilevamento del ransomware. Tutte le altre funzionalità di rilevazione, Insight e punto di recupero dati di ARP sono mantenute per ARP/ai.

Per abilitare ARP/ai, "ONTAP uno"è necessaria una licenza.

Scopri di più

- "Blog: La soluzione di rilevamento ransomware in tempo reale basata su ai di NetApp ottiene una classificazione AAA"

Protezione DA VITE SENZA FINE con gapping pneumatico con cyber vaulting

L'approccio di NetApp a un cyber-vault è un'architettura di riferimento appositamente creata per un cyber-vault logicamente a mappatura d'aria. Questo approccio sfrutta le tecnologie di protezione avanzata e conformità, come SnapLock, per consentire snapshot immutabili e indelebili.

Il vaulting dei computer informatici con SnapLock Compliance e un'air gap logico

Un trend in crescita è quello di distruggere le copie di backup e, in alcuni casi, persino crittografarle. Questo è il motivo per cui molti nel settore della sicurezza informatica consigliano di utilizzare i backup air gap come parte di una strategia globale di resilienza informatica.

Il problema è che i tradizionali gap aerei (nastro e supporti offline) possono aumentare significativamente i tempi di ripristino, aumentando così i tempi di inattività e i costi complessivi associati. Anche un approccio più moderno a una soluzione per il gap aereo può rivelarsi problematico. Ad esempio, se il vault di backup viene temporaneamente aperto per ricevere nuove copie di backup e quindi disconnette e chiude la connessione di rete ai dati primari per essere nuovamente "sottoposto a air gap", un utente malintenzionato potrebbe sfruttare l'apertura temporanea. Nel momento in cui la connessione è in linea, un utente malintenzionato potrebbe colpire per compromettere o distruggere i dati. Questo tipo di configurazione, inoltre, in genere aggiunge complessità indesiderata. Un air gap logico è un eccellente sostituto di un air gap tradizionale o moderno, perché ha gli stessi principi di protezione della sicurezza mantenendo il backup online. Con NetApp, è possibile risolvere la complessità del trasferimento di aria su nastro o disco con il gapping logico, che può essere ottenuto con copie snapshot immutabili e NetApp SnapLock Compliance.

[Un gioco logico con il Cyber Vault di NetApp]

NetApp ha rilasciato la funzione SnapLock più di 10 anni fa per soddisfare i requisiti di conformità dei dati, come la legge HIPAA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley e altre regole normative in materia di dati. È inoltre possibile archiviare copie snapshot primarie in volumi SnapLock in modo che le copie possano essere assegnate al WORM, impedendo la cancellazione. Esistono due versioni di licenza SnapLock: SnapLock Compliance e SnapLock Enterprise. Per la protezione dal ransomware, NetApp consiglia SnapLock Compliance, perché puoi impostare un periodo di conservazione specifico durante il quale le copie Snapshot sono bloccate e non possono essere eliminate, anche da parte degli amministratori ONTAP o del supporto NetApp.

Scopri di più

- "Blog: Protezione ransomware a più livelli con la soluzione Cyber Vault di NetApp"

Copie snapshot a prova di manomissione

Sfruttando SnapLock Compliance come air gap logico, è possibile proteggere al meglio per impedire agli hacker di eliminare le copie di backup, ma richiede anche di spostare le copie Snapshot utilizzando SnapVault in un volume secondario abilitato per SnapLock. Di conseguenza, molti clienti implementano questa configurazione su storage secondario in tutta la rete. Causando tempi di ripristino più lunghi rispetto al ripristino di una copia Snapshot del volume primario sullo storage primario.

A partire da ONTAP 9.12,1, le copie snapshot a prova di manomissione offrono una protezione di livello quasi SnapLock Compliance per le copie Snapshot su storage primario e nei volumi primari. Non è necessario archiviare la copia snapshot utilizzando SnapVault in un volume SnapLocked secondario. Le copie snapshot a prova di manomissione utilizzano la tecnologia SnapLock per impedire l'eliminazione della copia Snapshot primaria, anche da parte di un amministratore ONTAP completo che utilizza lo stesso periodo di scadenza della conservazione SnapLock. Ciò consente tempi di ripristino più rapidi e la possibilità di eseguire il backup di un volume FlexClone da una copia snapshot protetta e a prova di manomissione, cosa che non è possibile fare con una copia Snapshot tradizionale vault di SnapLock Compliance.

La differenza principale tra le copie snapshot SnapLock Compliance e antimanomissione consiste nel fatto che SnapLock Compliance non consente l'inizializzazione e il cancellazione dell'array ONTAP se i volumi SnapLock Compliance esistono con copie Snapshot in vault che non hanno ancora raggiunto la data di scadenza. Per rendere le copie Snapshot a prova di manomissione, è necessaria una licenza SnapLock Compliance.

Scopri di più

- "Blocca una copia snapshot per proteggerti dagli attacchi ransomware"

Protezione dal ransomware Active IQ

NetApp Active IQ è un consulente digitale che semplifica la cura e l'ottimizzazione proattive dello storage NetApp con informazioni utilizzabili per una gestione ottimale dei dati. Alimentato da dati telemetrici provenienti dalla nostra base installata, estremamente diversificata, utilizza tecniche di ai e ML avanzate per individuare opportunità per ridurre i rischi e migliorare le performance e l'efficienza del tuo ambiente di storage.

Non solo può "NetApp Active IQ" aiutare "eliminare le vulnerabilità di sicurezza", ma fornisce anche informazioni e linee guida specifiche per la protezione dai ransomware. Una wellness card dedicata mostra le azioni necessarie e i rischi affrontati, in modo da essere sicuri che i sistemi soddisfino le raccomandazioni sulle Best practice.

[Monitoraggio del benessere sul dashboard NetApp Active IQ]

I rischi e le azioni tracciati nella pagina benessere della difesa dal ransomware includono quanto segue (e molto altro ancora):

- Il numero di copie Snapshot dei volumi è basso, riducendo il potenziale di protezione ransomware.
- FPolicy non è abilitato per tutte le Storage Virtual Machine (SVM) configurate per i protocolli NAS.

Per vedere la protezione dal ransomware Active IQ in azione, consulta "NetApp Active IQ".

Resilienza completa grazie alla protezione dal ransomware BlueXP

È importante che il rilevamento di ransomware si verifichi il prima possibile, in modo da poter prevenire la diffusione e prevenire costosi downtime. Tuttavia, un'efficace strategia di rilevamento del ransomware dovrebbe includere più di un singolo livello di protezione. La protezione ransomware di NetApp adotta un approccio completo che include funzionalità on-box e real-time che si estendono ai servizi dati utilizzando BlueXP e una soluzione isolata e a più livelli per il cyber vaulting.

Protezione ransomware BlueXP

BlueXP è un pannello di controllo singolo per orchestrare in maniera intelligente una difesa ransomware completa e incentrata sul workload. La protezione ransomware di BlueXP riunisce le potenti funzionalità di resilienza informatica di ONTAP, come le snapshot ARP, FPolicy e a prova di manomissione, e i servizi dati BlueXP , come backup e recovery di BlueXP . Aggiunge inoltre consigli e linee guida con flussi di lavoro automatizzati per fornire una difesa end-to-end tramite un'unica interfaccia utente. Opera a livello del carico di lavoro per garantire che le applicazioni che eseguono l'azienda siano protette e possano essere recuperate il più rapidamente possibile in caso di attacco.

[La protezione dal ransomware di BlueXP è un'intelligenza basata su ai e l'assistenza necessarie per ridurre al minimo la perdita di dati dei workload e tornare rapidamente. Questa immagine mostra l'interfaccia utente di BlueXP .]

Vantaggi per il cliente:

- La predisposizione al ransomware assistita riduce l'overhead operativo e migliora l'efficacia
- Il rilevamento delle anomalie basato su ai/ML offre una maggiore precisione e una risposta più rapida per contenere i rischi
- Il ripristino guidato, coerente con l'applicazione, ti consente di ripristinare i workload più facilmente e in pochi minuti

"Protezione ransomware BlueXP" Rende queste funzioni NIST più facili da ottenere:

- Automaticamente **rilevamento** e assegnazione di priorità ai dati nello storage NetApp **con particolare attenzione ai workload basati sulle applicazioni**.
- **Protezione con un solo clic** del backup dei dati del carico di lavoro principale, configurazione immutabile e sicura, blocco di file dannosi e dominio di sicurezza diverso.
- **Rileva con precisione** il ransomware nel modo **rapido** possibile utilizzando **il rilevamento delle anomalie basato su ai di prossima generazione.**
- Risposta e flussi di lavoro automatizzati e integrazione con le principali soluzioni **SIEM e XDR.**
- Ripristina rapidamente i dati utilizzando un "recovery orchestrato" semplificato per accelerare l'uptime dell'applicazione.
- Implementa la tua protezione dal ransomware **strategia** e **policy**, e **monitora i risultati**.

Informazioni sul copyright

Informazioni sul marchio commerciale