



NetApp e zero trust

ONTAP Technical Reports

NetApp
January 23, 2026

Sommario

NetApp e zero trust	1
NetApp e zero trust	1
Che cos'è Zero Trust?	1
Risorse di sicurezza	2
Progetta un approccio incentrato sui dati a Zero Trust con ONTAP	2
Crea un MCAP basato sui dati Zero Trust	3
Controlli di orchestrazione e automazione della sicurezza NetApp esterni a ONTAP	7
Implementazioni di cloud ibrido e zero trust	8

NetApp e zero trust

NetApp e zero trust

Zero Trust è tradizionalmente un approccio incentrato sulla rete che prevede l'architettura di micro core e perimetro (MCAP) per proteggere dati, servizi, applicazioni o risorse con controlli noti come gateway di segmentazione. NetApp ONTAP sta adottando un approccio incentrato sui dati in Zero Trust, in cui il sistema di gestione dello storage diventa il gateway di segmentazione per proteggere e monitorare l'accesso ai dati dei clienti. In particolare, il motore FPolicy Zero Trust e l'ecosistema di partner FPolicy diventano un centro di controllo per acquisire una comprensione dettagliata dei modelli di accesso ai dati normali e aberranti e identificare le minacce interne.

 A partire da luglio 2024, il contenuto del report tecnico *TR-4829: NetApp and Zero Trust: Enabling a data-centric Zero Trust model*, precedentemente pubblicato come PDF, è disponibile all'indirizzo docs.netapp.com.

I dati sono le risorse più importanti della tua organizzazione. Secondo il 2022, le minacce interne sono la causa del 18% delle violazioni dei dati "[Rapporto Verizon Data Breach Investigations](#)". Le organizzazioni possono rafforzare la propria vigilanza implementando controlli Zero Trust leader di settore intorno ai dati con il software per la gestione dei dati NetApp ONTAP.

Che cos'è Zero Trust?

Il modello Zero Trust è stato sviluppato per la prima volta da John Kindervag in Forrester Research. Prevede la sicurezza della rete dall'interno verso l'esterno e non dall'esterno. L'approccio Inside-out Zero Trust identifica un microcore e un perimetro (MCAP). La certificazione MCAP è una definizione interna di dati, servizi, applicazioni e risorse da proteggere con un set completo di controlli. Il concetto di perimetro esterno sicuro è obsoleto. Le entità attendibili e autorizzate ad eseguire correttamente l'autenticazione attraverso il perimetro possono rendere l'organizzazione vulnerabile agli attacchi. Gli addetti interni, per definizione, sono già all'interno del perimetro sicuro. Dipendenti, appaltatori e partner sono inclusi e devono essere abilitati a operare con controlli appropriati per l'esecuzione dei loro ruoli all'interno dell'infrastruttura dell'organizzazione.

Zero Trust è stata menzionata come una tecnologia che offre promesse al DoD nel settembre 2019 "[FY19-23 DoD strategia di modernizzazione digitale](#)". Definisce Zero Trust come "Una strategia di sicurezza informatica che incorpora la sicurezza in tutta l'architettura allo scopo di fermare le violazioni dei dati. Questo modello di protezione incentrato sui dati elimina l'idea di reti, dispositivi, figure o processi attendibili o non attendibili e passa a livelli di confidenza basati su più attributi che consentono l'autenticazione e l'autorizzazione dei criteri in base al concetto di accesso con privilegi minimi. L'implementazione di zero trust richiede un ripensamento del modo in cui utilizziamo l'infrastruttura esistente per implementare la sicurezza in base alla progettazione in modo più semplice ed efficiente, consentendo allo stesso tempo operazioni senza ostacoli."

Nell'agosto del 2020, il NIST ha pubblicato "[Speciale Pub 800-207 architettura Zero Trust](#)" (ZTA). ZTA si concentra sulla protezione delle risorse, non dei segmenti di rete, perché la posizione della rete non è più considerata come il componente principale della posizione di sicurezza della risorsa. Le risorse sono dati e calcolo. Le strategie ZTA sono destinate agli architetti di reti aziendali. ZTA introduce una nuova terminologia dai concetti originali di Forrester. I meccanismi di protezione denominati PDP (Policy Decision Point) e PEP (Policy Enforcement Point) sono analoghi a un gateway di segmentazione Forrester. ZTA introduce quattro modelli di distribuzione:

- Implementazione basata su gateway o agente dispositivo
- Implementazione basata su Enclave (in qualche modo analoga alla certificazione Forrester MCAP)
- Implementazione basata su portale di risorse
- Sandboxing dell'applicazione del dispositivo

Ai fini di questa documentazione, utilizziamo concetti e terminologia di Forrester Research piuttosto che NIST ZTA.

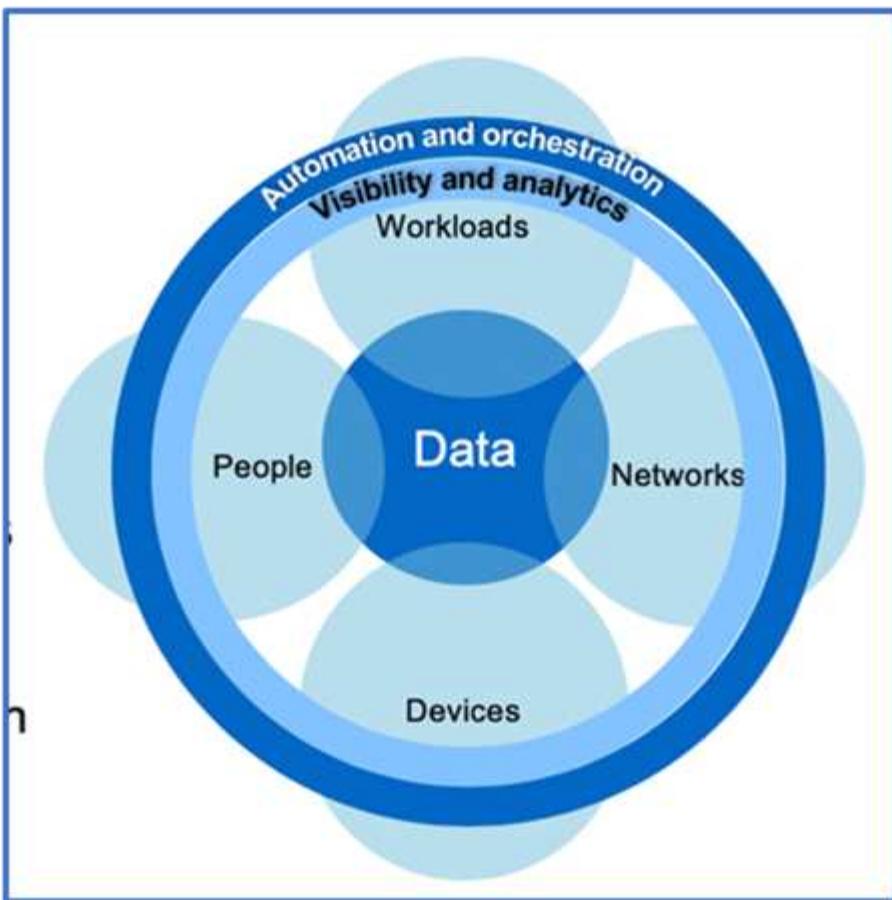
Risorse di sicurezza

Per informazioni sulla segnalazione di vulnerabilità e incidenti, risposte di sicurezza NetApp e riservatezza dei clienti, vedere "[Portale NetApp sulla sicurezza](#)".

Progetta un approccio incentrato sui dati a Zero Trust con ONTAP

Una rete Zero Trust viene definita da un approccio incentrato sui dati, in cui i controlli di sicurezza devono trovarsi il più vicino possibile ai dati. Le funzionalità di ONTAP, insieme all'ecosistema partner di NetApp FPolicy, possono fornire i controlli necessari per il modello Zero Trust incentrato sui dati.

ONTAP è un software NetApp per la gestione dei dati con sicurezza robusta e il motore Zero Trust di FPolicy è una funzione ONTAP leader di settore che offre un'interfaccia di notifica di eventi granulare e basata su file. I partner NetApp FPolicy possono utilizzare questa interfaccia per ottenere maggiore visibilità sull'accesso ai dati all'interno di ONTAP.



Crea un MCAP basato sui dati Zero Trust

Per progettare una certificazione MCAP Zero Trust incentrata sui dati, attenersi alla seguente procedura:

1. Identificare l'ubicazione di tutti i dati dell'organizzazione.
2. Classificazione dei dati.
3. Smaltire in modo sicuro i dati non più necessari.
4. Comprendere quali ruoli devono avere accesso alle classificazioni dei dati.
5. Applicare il principio del privilegio minimo per applicare i controlli di accesso.
6. Utilizza la Multifactor Authentication per l'accesso amministrativo e l'accesso ai dati.
7. Utilizza la crittografia per i dati a riposo e in uso.
8. Monitorare e registrare tutti gli accessi.
9. Avvisa di accessi o comportamenti sospetti.

Identificare l'ubicazione di tutti i dati dell'organizzazione

La funzionalità FPolicy di ONTAP, insieme all'ecosistema di partner NetApp Alliance, ti consente di identificare dove sono presenti i dati della tua organizzazione e chi ne ha accesso. Ciò avviene con l'analisi dei comportamenti degli utenti, che identifica se gli schemi di accesso ai dati sono validi. Ulteriori dettagli sull'analisi del comportamento degli utenti sono discussi in Monitor e registrano tutti gli accessi. Se non si capisce dove si trovano i dati e chi vi ha accesso, l'analisi comportamentale degli utenti può fornire una base per creare classificazione e policy a partire da osservazioni empiriche.

Classificazione dei dati

Nella terminologia del modello Zero Trust, la classificazione dei dati implica l'identificazione dei dati tossici. I dati tossici sono dati sensibili che non sono destinati a essere divulgati all'esterno di un'organizzazione. La divulgazione di dati tossici potrebbe violare la conformità normativa e danneggiare la reputazione di un'organizzazione. In termini di conformità normativa, i dati tossici includono i dati del titolare della carta per "[Payment Card Industry Data Security Standard \(PCI-DSS\)](#)" , dati personali per l'UE "[Regolamento generale sulla protezione dei dati \(GDPR\)](#)" , o dati sanitari per il "[Health Insurance Portability and Accountability Act \(HIPAA\)](#)" . Puoi usare NetApp "[NetApp Data Classification](#)" (precedentemente noto come Cloud Data Sense), un toolkit basato sull'intelligenza artificiale per analizzare, scansionare e categorizzare automaticamente i tuoi dati.

Smaltire in modo sicuro i dati non più necessari

Dopo aver classificato i dati della tua organizzazione, potresti scoprire che alcuni di essi non sono più necessari o rilevanti per la funzione della tua organizzazione. La conservazione di dati non necessari è una responsabilità e tali dati devono essere cancellati. Per un meccanismo avanzato che consente di cancellare crittograficamente i dati, vedere la descrizione dell'eliminazione sicura nella crittografia dei dati inattivi.

Comprendere quali ruoli devono avere accesso alle classificazioni dei dati e applicare il principio del minimo privilegio per applicare i controlli di accesso

La mappatura dell'accesso ai dati sensibili e l'applicazione del principio del privilegio minimo consentono agli utenti dell'organizzazione di accedere solo ai dati necessari per svolgere il proprio lavoro. Questo processo comporta il controllo dell'accesso basato sui ruoli ("[RBAC](#)"), che si applica all'accesso ai dati e all'accesso amministrativo.

Con ONTAP, è possibile utilizzare una Storage Virtual Machine (SVM) per segmentare l'accesso ai dati organizzativi da parte dei tenant all'interno di un cluster ONTAP. RBAC può essere applicato all'accesso ai dati e all'accesso amministrativo alla SVM. RBAC può anche essere applicato a livello amministrativo del cluster.

Oltre ai role-based access control, è possibile utilizzare ONTAP "[verifica con amministratori multipli](#)" (MAV) per richiedere a uno o più amministratori di approvare comandi come `volume delete` o `volume snapshot delete`. Una volta attivato MAV, la modifica o la disattivazione di MAV richiede l'approvazione dell'amministratore MAV.

Un altro modo per proteggere gli snapshot è con ONTAP "[blocco delle istantanee](#)". Il blocco degli snapshot è una funzionalità SnapLock in cui gli snapshot vengono resi indelebili manualmente o automaticamente, con un periodo di conservazione nel criterio dello snapshot del volume. Il blocco delle istantanee viene anche definito blocco delle istantanee a prova di manomissione. Lo scopo del blocco delle snapshot è impedire agli amministratori non autorizzati o non attendibili di eliminare snapshot sui sistemi ONTAP primari e secondari. È possibile ottenere un rapido recovery degli snapshot bloccati sui sistemi primari per ripristinare volumi corrotti dal ransomware.

Utilizza la Multifactor Authentication per l'accesso amministrativo e l'accesso ai dati

Oltre al RBAC amministrativo del cluster, "[Autenticazione multifattore \(MFA\)](#)" può essere implementato per l'accesso amministrativo web di ONTAP e l'accesso Secure Shell (SSH) a riga di comando. MFA per l'accesso amministrativo è un requisito per le organizzazioni del settore pubblico statunitense o per quelle che devono seguire il PCI-DSS. MFA rende impossibile per un utente malintenzionato compromettere un account utilizzando solo un nome utente e una password. L'autenticazione MFA richiede due o più fattori indipendenti. Un esempio di autenticazione a due fattori è qualcosa che un utente possiede, come una chiave privata, e qualcosa che un utente conosce, come una password. L'accesso web amministrativo al ONTAP System Manager o ActiveIQ Unified Manager è abilitato dal Security Assertion Markup Language (SAML) 2,0. L'accesso a riga di comando SSH utilizza un'autenticazione a due fattori concatenata con una chiave pubblica

e una password.

È possibile controllare l'accesso di utenti e macchine tramite API con le funzionalità di gestione delle identità e degli accessi di ONTAP:

- Utente:
 - **Autenticazione e autorizzazione.** Attraverso le funzionalità dei protocolli NAS per SMB e NFS.
 - **Audit.** Syslog di accesso ed eventi. Logging dettagliato dell'audit del protocollo CIFS per testare le policy di autenticazione e autorizzazione. Controllo FPolicy granulare e fine dell'accesso NAS dettagliato a livello di file.
- Dispositivo:
 - **Autenticazione.** Autenticazione basata su certificati per l'accesso API.
 - **Autorizzazione.** Controllo degli accessi (RBAC) predefinito o personalizzato in base al ruolo.
 - **Audit.** Syslog di tutte le azioni eseguite.

Utilizza la crittografia per i dati a riposo e in uso

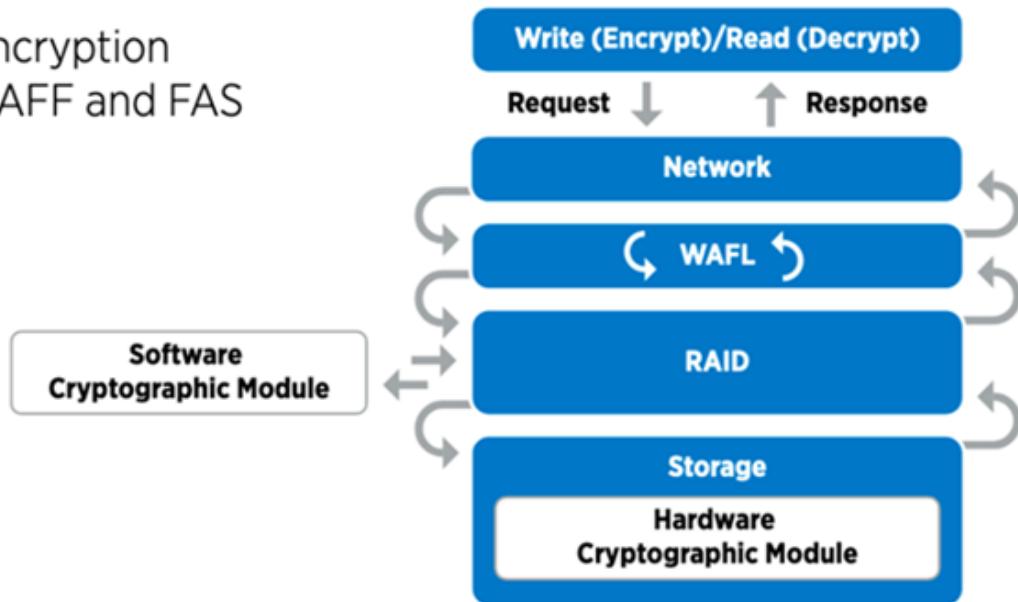
Crittografia dei dati inattivi

Ogni giorno esistono nuovi requisiti per ridurre i rischi del sistema storage e il gap dell'infrastruttura quando un'organizzazione riutilizza i dischi, restituisce i dischi difettosi o effettua gli upgrade a dischi più grandi vendendoli o tramite permuta. Come amministratori e operatori dei dati, i tecnici dello storage sono tenuti a gestire e mantenere i dati in modo sicuro per tutto il loro ciclo di vita. "[Crittografia dello storage NetApp \(NSE\)](#)" e "[crittografia dei volumi NetApp \(NVE\)](#)" aiuta a crittografare costantemente tutti i dati a riposo, che siano tossici e non influiscano sulle operazioni quotidiane. "[NSE](#)" È una soluzione hardware ONTAP "[dati a riposo](#)" che utilizza dischi con crittografia automatica convalidati FIPS 140-2 livello 2. "[NVE e NAE](#)" Sono una soluzione software ONTAP "[dati a riposo](#)" che utilizza "[Modulo crittografico NetApp validato FIPS 140-2 livello 1](#)". Con NVE e NAE, è possibile utilizzare i dischi rigidi o i dischi a stato solido per la crittografia dei dati a riposo. Inoltre, i dischi NSE possono essere utilizzati per fornire una soluzione per la crittografia nativa e su più layer che garantisca ridondanza della crittografia e sicurezza aggiuntiva. Se un livello viene violato, il secondo livello protegge comunque i dati. Queste funzionalità rendono ONTAP ben posizionato per "[crittografia quantum-ready](#)".

NVE fornisce anche una funzionalità chiamata "[spurgo sicuro](#)" che rimuove crittograficamente i dati tossici da perdite di dati quando i file sensibili vengono scritti in un volume non classificato.

È possibile utilizzare il "[Onboard Key Manager \(OKM\)](#)", che è il gestore delle chiavi integrato in ONTAP, o "[approvato](#)" terze parti "[responsabili esterni delle chiavi](#)" con NSE e NVE per memorizzare in modo sicuro il materiale di codifica.

Two-layer encryption solution for AFF and FAS



Come illustrato nella figura precedente, è possibile combinare la crittografia basata su hardware e software. Questa funzionalità ha portato a "[Convalida di ONTAP nelle soluzioni commerciali della NSA per il programma classificato](#)" che consente la memorizzazione di dati top secret.

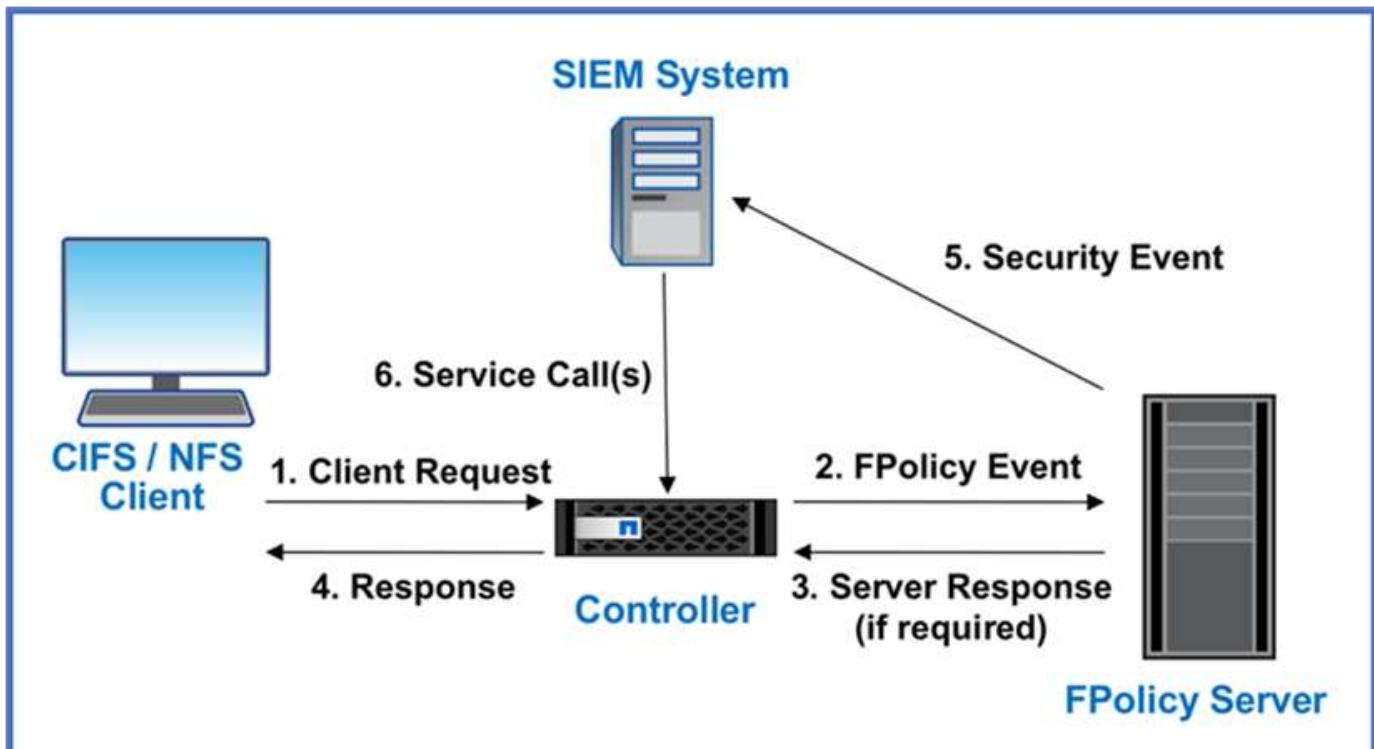
Crittografia dei dati in-flight

La crittografia dei dati in-flight di ONTAP protegge l'accesso ai dati degli utenti e l'accesso da un piano di controllo. L'accesso ai dati degli utenti può essere crittografato con la crittografia SMB 3,0 per l'accesso alla condivisione CIFS di Microsoft o con krb5P per NFS Kerberos 5. L'accesso ai dati dell'utente può anche essere crittografato con "[IPSec](#)" per CIFS, NFS e iSCSI. L'accesso al piano di controllo è crittografato con Transport Layer Security (TLS). ONTAP fornisce la "[FIPS](#)" modalità di conformità per l'accesso al piano di controllo, che attiva algoritmi approvati FIPS e disattiva algoritmi non approvati FIPS. La replica dei dati viene crittografata con "[crittografia di peering dei cluster](#)". In questo modo viene fornita la crittografia per le tecnologie ONTAP SnapVault e SnapMirror.

Monitorare e registrare tutti gli accessi

Una volta messe in atto le policy RBAC, devi implementare monitoring, audit e avvisi attivi. Il motore Zero Trust FPolicy di NetApp ONTAP, insieme a "[Ecosistema di partner NetApp FPolicy](#)", fornisce i controlli necessari per il modello Zero Trust incentrato sui dati. NetApp ONTAP è un software per la gestione dei dati ricco di sicurezza e "[FPolicy](#)" una funzionalità ONTAP leader di settore che offre un'interfaccia di notifica degli eventi granulare basata su file. I partner NetApp FPolicy possono utilizzare questa interfaccia per ottenere maggiore visibilità sull'accesso ai dati all'interno di ONTAP. La funzionalità FPolicy di ONTAP, insieme all'ecosistema di partner NetApp Alliance di FPolicy, ti consente di identificare dove sono presenti i dati della tua organizzazione e chi ne ha accesso. Ciò avviene con l'analisi dei comportamenti degli utenti, che identifica se gli schemi di accesso ai dati sono validi. L'analisi del comportamento degli utenti può essere utilizzata per avvisare in caso di accesso ai dati sospetto o aberrante che non rientra nel normale modello e, se necessario, per intraprendere azioni volte a negare l'accesso.

I partner FPolicy stanno andando oltre gli analytics comportamentali degli utenti verso il machine learning (ML) e l'intelligenza artificiale (ai), per una maggiore fedeltà agli eventi e meno falsi positivi, se presenti. Tutti gli eventi devono essere registrati su un server syslog o su un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) in grado di utilizzare ML e ai.



NetApp "Sicurezza del carico di lavoro di archiviazione DII" sfrutta l'interfaccia FPolicy e l'analisi comportamentale degli utenti sui sistemi di archiviazione ONTAP sia cloud che on-premise per fornire avvisi in tempo reale sui comportamenti dannosi degli utenti. Storage Workload Security protegge i dati aziendali dall'uso improprio da parte di utenti malintenzionati o compromessi tramite apprendimento automatico avanzato e rilevamento delle anomalie. Storage Workload Security è in grado di identificare attacchi ransomware o altri comportamenti illeciti, richiamare snapshot e mettere in quarantena gli utenti malintenzionati. Storage Workload Security è dotato anche di una capacità forense per visualizzare in dettaglio le attività degli utenti e delle entità. Storage Workload Security è una parte di NetApp Data Infrastructure Insights.

Oltre alla sicurezza del workload di storage, ONTAP dispone di una funzionalità di rilevamento del ransomware integrata nota come "[Protezione ransomware autonoma](#)" (ARP). ARP usa l'apprendimento automatico per determinare se un'attività anomala dei file indica che è in corso un attacco ransomware e richiama una snapshot e avvisa gli amministratori. Storage workload Security si integra con ONTAP per ricevere eventi ARP e fornisce un livello aggiuntivo di analisi e risposte automatiche.

Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "[Riferimento comando ONTAP](#)".

Controlli di orchestrazione e automazione della sicurezza NetApp esterni a ONTAP

L'automazione consente di eseguire un processo o una procedura con un'assistenza minima da parte dell'operatore. L'automazione consente alle organizzazioni di scalare le implementazioni di tipo Zero Trust ben oltre le procedure manuali, in modo da difendersi da attività miscibili e automatizzate.

Ansible è un tool di provisioning software open-source, gestione della configurazione e implementazione dell'applicazione. Funziona su molti sistemi Unix-like, e può configurare sia sistemi Unix-like che Microsoft

Windows. Include il proprio linguaggio dichiarativo per descrivere la configurazione del sistema. Ansible è stato scritto da Michael DeHaan e acquisito da Red Hat nel 2015. Ansible si connette temporaneamente e senza agenti tramite SSH o Windows Remote Management (consentendo l'esecuzione remota di PowerShell) per eseguire i task. NetApp ha sviluppato molto di più di "[150 moduli Ansible per il software ONTAP](#)", consentendo un'ulteriore integrazione con il framework di automazione Ansible. I moduli Ansible per NetApp forniscono una serie di istruzioni su come definire lo stato desiderato e trasferirlo all'ambiente NetApp di destinazione. I moduli sono realizzati per supportare task come l'impostazione del licensing, la creazione di aggregati e di Storage Virtual Machine, la creazione di volumi e il ripristino di snapshot per citarne alcuni. Un ruolo Ansible è stato ["Pubblicato su GitHub"](#) specifico per la NetApp DoD Unified Capabilities (UC) Deployment Guide.

Utilizzando la libreria di moduli disponibili, gli utenti possono facilmente sviluppare i playbook Ansible e personalizzarli in base alle proprie applicazioni e esigenze aziendali per automatizzare i task ordinari. Una volta scritto un playbook, puoi eseguirlo per eseguire il task specificato, risparmiando tempo e migliorando la produttività. NetApp ha creato e condiviso playbook di esempio che possono essere utilizzati direttamente o personalizzati per le tue esigenze.

Data Infrastructure Insights è uno strumento di monitoraggio dell'infrastruttura che ti offre visibilità sull'intera infrastruttura. Con Data Infrastructure Insights puoi monitorare, risolvere i problemi e ottimizzare tutte le tue risorse, comprese le istanze del cloud pubblico e i data center privati. Data Infrastructure Insights può ridurre il tempo medio di risoluzione del 90% e impedire che l'80% dei problemi del cloud interessino gli utenti finali. Può inoltre ridurre in media del 33% i costi dell'infrastruttura cloud e ridurre l'esposizione alle minacce interne proteggendo i dati con informazioni fruibili. La funzionalità Storage Workload Security di Data Infrastructure Insights consente l'analisi comportamentale degli utenti con intelligenza artificiale e apprendimento automatico per avvisare quando si verificano comportamenti anomali degli utenti dovuti a una minaccia interna. Per ONTAP, Storage Workload Security utilizza il motore Zero Trust FPolicy.

Implementazioni di cloud ibrido e zero trust

NetApp è l'autorità in materia di dati per il cloud ibrido. NetApp offre diverse opzioni per estendere i sistemi di gestione dei dati on-premise al cloud ibrido con Amazon Web Services (AWS), Microsoft Azure, Google Cloud e altri importanti provider cloud. Le soluzioni cloud ibrido NetApp supportano gli stessi controlli di sicurezza Zero Trust disponibili con i sistemi ONTAP on-premise e lo storage software-defined ONTAP Select .

È possibile espandere facilmente la capacità nei cloud pubblici senza i tipici vincoli CAPEX utilizzando servizi file cloud-native di livello enterprise per AWS (FSxN), Google Cloud (GCNV) e Azure NetApp Files per Microsoft Azure. Ideali per carichi di lavoro ad alta intensità di dati, come analisi e DevOps, questi servizi di dati cloud combinano l'archiviazione elastica e on-demand come servizio di NetApp con la gestione dei dati ONTAP in un'offerta completamente gestita.

ONTAP consente lo spostamento dei dati tra i sistemi ONTAP locali e l'ambiente di archiviazione AWS, Google Cloud o Azure con il software di replicazione dei dati NetApp SnapMirror .

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.