

# NETAPP RANSOMWARE RESILIENCE



Rilevare gli attacchi ransomware in tempo reale, prevenire la perdita di dati, ripristinare rapidamente e ridurre al minimo l'impatto sull'attività

## Pronti per affrontare un attacco ransomware?

Un aspetto fondamentale per prepararsi a un attacco ransomware è proteggere i dati del carico di lavoro a livello di archiviazione, ovvero l'ultima linea di difesa. Poiché gli attacchi stanno diventando sempre più sofisticati, automatizzati e costosi, prevenire un attacco ransomware è irrealistico. Bisogna essere pronti quando arrivano gli aggressori.

I backup da soli non bastano. È necessario essere in grado di valutare i rischi per i dati critici del carico di lavoro, nonché di rilevare le minacce e rispondere in tempo reale. È inoltre necessario predisporre piani di ripristino che possano essere eseguiti in modo rapido e semplice. Tuttavia, ottenere una resilienza efficace contro un attacco ransomware è un onere operativo, con molte attività manuali soggette a errori e troppo poco personale con le competenze necessarie.

Se non si dispone di un programma in atto, gli attacchi ai carichi di lavoro passeranno inosservati e le risposte saranno ritardate. Il ripristino del carico di lavoro sarà complesso e richiederà in media 7 giorni<sup>1</sup>—e i dati potrebbero non essere nemmeno completamente recuperati. Ciò ovviamente è troppo poco e troppo tardi.

## Ottenere la protezione completa sull'ultima linea di difesa

Il servizio NetApp® Ransomware Resilience consente di eseguire il programma in modo rapido e semplice, dalla prevenzione al rilevamento, alla risposta e al ripristino.

Ransomware Resilience fornisce un'unica interfaccia per orchestrare in modo intelligente la difesa contro i ransomware incentrata sul carico di lavoro. Con pochi clic è possibile identificare e proteggere i dati critici del carico di lavoro a rischio. Il servizio rileva e risponde in modo accurato e automatico ai potenziali attacchi, limitandone l'impatto. Ed è possibile ripristinare i carichi di lavoro, liberi da malware, in pochi minuti, salvaguardando i dati preziosi e riducendo al minimo i danni e i costi di interruzione dell'attività.

Ransomware Resilience unisce le potenti funzionalità del software NetApp ONTAP® con NetApp Data Services, aggiungendo raccomandazioni e indicazioni intelligenti con flussi di lavoro automatizzati per:

- **Identificare.** È possibile identificare automaticamente i carichi di lavoro (VM, condivisioni di file, database più diffusi) e i relativi dati nello storage NetApp, associare i dati al carico di lavoro e determinare la sensibilità, l'importanza e il rischio dei dati.
- **Proteggere.** È possibile ottenere consigli sulle policy di protezione dei carichi di lavoro e applicarli con un clic.
- **Rilevare.** È possibile rilevare in tempo reale attività sospette su file e comportamenti degli utenti che potrebbero segnalare potenziali tentativi di esfiltrazione dei dati, nonché tentativi di crittografia dei file e di eliminazione di massa.
- **Rispondere.** È possibile proteggere i carichi di lavoro creando automaticamente copie NetApp Snapshot™ e bloccando gli utenti quando si sospetta un potenziale attacco. Il servizio si integra anche con le soluzioni SIEM (Security Information and Event Management) leader del settore.
- **Ripristinare.** È possibile ripristinare rapidamente i carichi di lavoro e i dati associati tramite un processo di ripristino semplice e orchestrato. Utilizzando l'ambiente di ripristino isolato, si otterrà un ripristino dei dati pulito e privo di malware.
- **Governare.** È possibile implementare la strategia e le policy di protezione da ransomware e monitorare i risultati.

### Prepararsi per un attacco: risparmiare tempo e migliorare l'efficacia

Ransomware Resilience identifica automaticamente i tipi di dati presenti nello storage NetApp, li associa a carichi di lavoro specifici, valuta la sensibilità e la criticità dei dati e analizza il rischio. Questo processo riduce la necessità di affidarsi a complicate analisi manuali, strumenti di terze parti aggiuntivi e competenze specialistiche.

## BENEFICI PRINCIPALI

Ottenere una protezione completa e orchestrata all'ultima linea di difesa:

- Ottenere una visibilità completa sulla postura di protezione del carico di lavoro.
- Rilevare tempestivamente un attacco e prevenire la perdita di dati.
- Ripristinare rapidamente interi carichi di lavoro senza malware per ridurre al minimo interruzioni, costi, mancati ricavi e danni aziendali.
- Ottenere dati per analisi forensi e consigli per migliorare la sicurezza.

Ransomware Resilience propone quindi policy di protezione intelligenti utilizzando le funzionalità ONTAP, tra cui NetApp Autonomous Ransomware Protection con rilevamento delle anomalie AI (ARP/AI), blocco delle estensioni dannose FPolicy e copie Snapshot a prova di manomissione. Ransomware Resilience adatta inoltre le raccomandazioni di protezione alla sensibilità e alla criticità delle risorse dati.

Con un solo clic, è possibile applicare le policy di protezione ai tuoi dati del carico di lavoro perfettamente e coerentemente. Ransomware Resilience funziona in background per configurare le funzionalità di ONTAP e NetApp Data Services e per orchestrare i flussi di lavoro di protezione su ogni volume di dati, riducendo la necessità di attività manuali ripetitive.

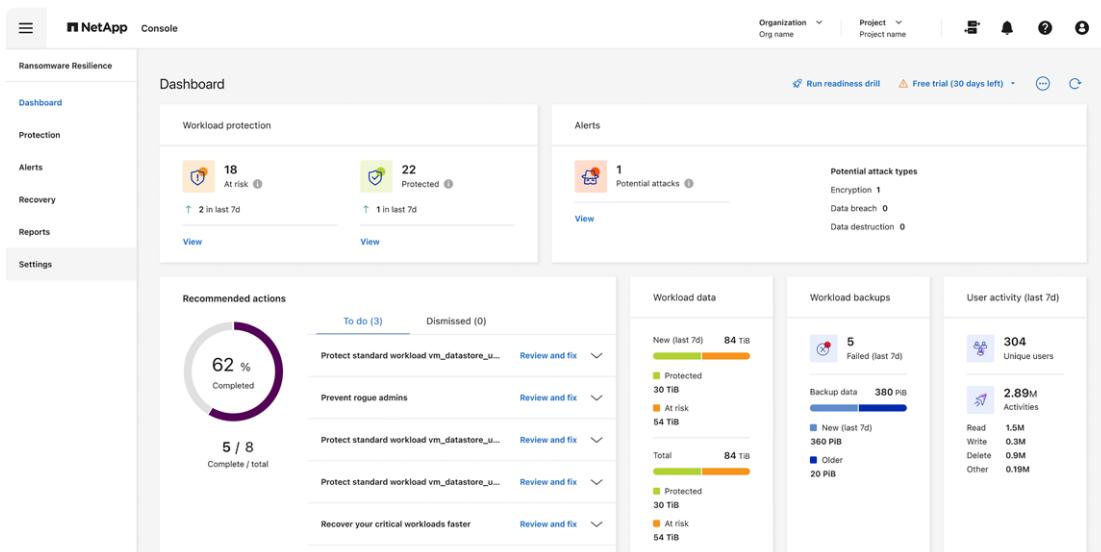
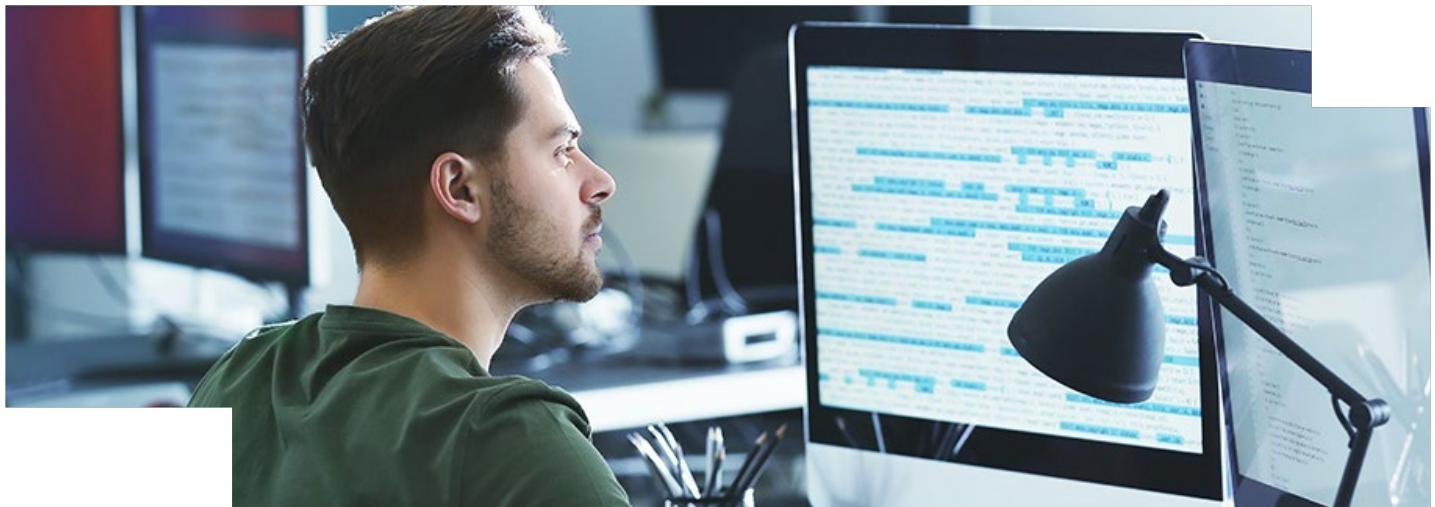


Figura 1: Il servizio NetApp Ransomware Resilience fornisce una difesa contro i ransomware completa e orchestrata incentrata sul carico di lavoro, dal rilevamento al ripristino, tramite un unico piano di controllo.



### Rilevare e rispondere alle minacce in tempo reale

Ransomware Resilience monitora costantemente la presenza di anomalie nei file sospetti e nel comportamento degli utenti. È in grado di rilevare violazioni dei dati identificando precocemente i comportamenti degli utenti che potrebbero segnalare potenziali tentativi di esfiltrazione dei dati, nonché tentativi di crittografia dei file e di eliminazione di massa. Quando si sospetta un attacco, Ransomware Resilience crea una copia Snapshot per impedire la perdita di dati e consente di bloccare l'utente che sta eseguendo l'attacco per fermarlo e prevenire ulteriori attacchi.

Questo servizio utilizza un rilevamento ransomware innovativo e avanzato basato sull'intelligenza artificiale sullo storage primario. Questo approccio consente di individuare rapidamente i potenziali attacchi e di mitigarli immediatamente.

Ransomware Resilience fornisce report sugli incidenti a supporto delle indagini forensi e si integra con le soluzioni SIEM leader del settore.

### Recuperare facilmente i carichi di lavoro, in pochi minuti

Ransomware Resilience orchestra il flusso di lavoro per il ripristino coerente con l'applicazione di tutti i dati del carico di lavoro associati e offre visibilità sul processo e sullo stato in tempo reale. Le copie snapshot possono essere ripristinate a livello di carico di lavoro o in modo più granulare a livello di volume o di file.

Come parte del processo di ripristino, Ransomware Resilience fornisce un ambiente di ripristino isolato che isola i carichi di lavoro infetti, rimuove il malware, consiglia un punto di ripristino e guida l'utente attraverso un processo di ripristino intuitivo. Questo approccio garantisce un ripristino pulito e privo di malware e impedisce la reinfezione dei dati.

### Minimizzare le interruzioni al business

Ransomware Resilience elimina l'onere e l'ansia di dover proteggere i carichi di lavoro dai tempi di inattività e dalla perdita di dati correlati al ransomware. Fornisce un servizio completo che migliora la prontezza, risponde agli attacchi e guida l'utente attraverso il recupero. Solo con NetApp è possibile avere la tranquillità di sapere che, in caso di attacco, l'utente sarà avvisato immediatamente, i preziosi dati del carico di lavoro saranno protetti e il ripristino sarà rapido e semplice, riducendo al minimo l'interruzione dell'attività.

### Ottenere NetApp Ransomware Resilience oggi stesso

<sup>1</sup> ESG, [Prontezza contro il ransomware nel 2023: la strada verso la rapidità e la mitigazione](#), Novembre 2023.

Il presente documento è una traduzione generata con la traduzione automatica. In caso di contraddizioni o incongruenze con la versione inglese, farà fede il contenuto della versione inglese.

#### A proposito di NetApp

NetApp è l'azienda di infrastrutture dati intelligenti che unisce storage dati unificato, dati integrati, servizi operativi e di carico di lavoro per trasformare un mondo di cambiamenti radicali in opportunità per ogni cliente. NetApp crea infrastrutture indipendenti da silos e, sfruttando l'Intelligenza Artificiale, abilita la miglior gestione dei dati del settore. Il nostro storage, l'unico servizio enterprise integrato nativamente nelle principali soluzioni cloud del mondo, offre una flessibilità perfetta. Inoltre, i nostri servizi dati consentono di ottenere un vantaggio competitivo grazie a una governance, una resilienza informatica e un'agilità delle applicazioni di livello superiore. I nostri servizi operativi e di gestione dei carichi di lavoro garantiscono un'ottimizzazione continua delle prestazioni e dell'efficienza per infrastrutture e carichi di lavoro attraverso l'osservabilità e l'intelligenza artificiale. A prescindere dal tipo di dati, dal workload o dall'ambiente, con NetApp puoi trasformare la tua infrastruttura dati per aumentare le opportunità di business. Scopri di più su [www.netapp.com](http://www.netapp.com) oppure seguici su [X](#), [LinkedIn](#), [Facebook](#), E [Instagram](#).



Contattaci