5 strategie di cyber resilienza per affrontare la crescita dei dati non strutturati

Perché non puoi più affidarti alle soluzioni legacy e quali funzionalità critiche ti servono subito

rubrik

INDICE

L'ESPLOSIONE DEI DATI NON STRUTTURATI È ARRIVATA 3

CINQUE REQUISITI INDISPENSABILI PER UNA SOLUZIONE DI PROTEZIONE DEI DATI NON STRUTTURATI 5

Prestazioni su scala petabyte per la protezione dei dati non strutturati 5

Visibilità olistica su tutti i tuoi dati non strutturati 6

Sicurezza dei dati enterprise con rilevamento delle anomalie su larga scala 7

Visibilità e classificazione dei dati sensibili 8

Recovery dei dati granulare ed efficiente 9

MODERNIZZARE LA PROTEZIONE DEI DATI NON STRUTTURATI 10

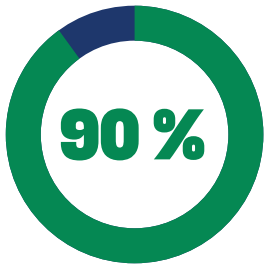
L'ESPLOSIONE DEI DATI NON STRUTTURATI È ARRIVATA

Il volume dei dati non strutturati, ossia i dati che risiedono al di fuori degli strumenti convenzionali come i database relazionali, sta crescendo in modo incontrollato. Secondo IDC, i dati non strutturati rappresentano il 90% di tutti i dati. Il problema è questo: un quarto delle organizzazioni afferma di non poter stare al passo con la crescita dei dati.[1] Questo aspetto preoccupa perché i dati non strutturati includono una grande mole di informazioni sensibili come proprietà intellettuale (PI), dati personali, risultati di ricerche e così via.

In pratica, se la tua proprietà intellettuale - tra cui dati di ricerca, design di prodotti, codice sorgente, modelli di engineering e scoperte scientifiche (tutti dati non strutturati) - subisce un attacco, rischi di perdere anni di lavoro, il tuo vantaggio competitivo e una knowledge aziendale insostituibile.

È essenziale trovare il modo di proteggere tutti questi dati non strutturati, ma non è affatto semplice. Non solo il volume dei dati non strutturati è enorme, ma è anche altamente frammentato e disperso in diversi sistemi di archiviazione e in diverse posizioni (NAS on-premise, storage di oggetti, ecc.), il che rende difficile tenerne traccia manualmente.

Per riuscire a proteggere i propri dati non strutturati, le aziende utilizzano di norma strategie di backup tradizionali. Ma questi metodi non assicurano la velocità, la visibilità e il controllo necessari per svolgere il proprio lavoro.



Secondo IDC, i dati non strutturati rappresentano il 90% di tutti i dati.

1 IDC: Il valore non sfruttato dei dati non strutturati (in inglese), https://www.box.com/resources/unstructured-data-paper

Ad esempio:

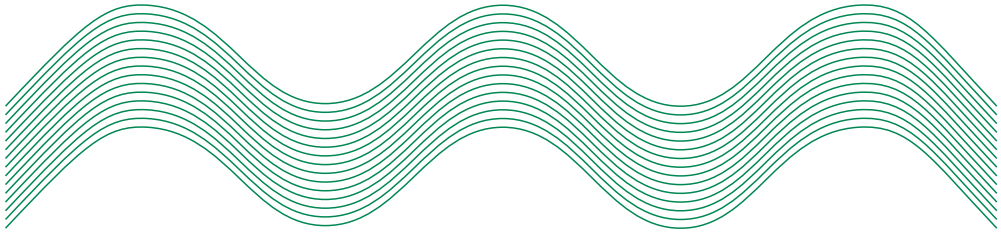
Le soluzioni di backup tradizionali non sono state progettate per il backup di grandi dataset, e il backup su scala petabyte con le soluzioni tradizionali può richiedere settimane. Ma anche se il backup dei dati viene eseguito in tempi relativamente rapidi, il processo può generare ritardi e problemi di prestazioni nell'ambiente di produzione. Nell'insieme, questi due problemi possono indurre i team a non proteggere i dati.

Inoltre, i metodi di backup tradizionali non offrono una visibilità multipiattaforma, quindi non è possibile avere una visione unificata tra i diversi tipi di storage. Con questo approccio frammentato, gestire la protezione di un ampio panorama di dati non strutturati è difficile.

Non hai informazioni precise su dove si trovano i tuoi dati sensibili e chi vi ha accesso, quindi è più difficile individuare le aree a rischio e rispettare gli obblighi di conformità alle normative.

Mancano controlli di sicurezza adeguati per difendersi da minacce in espansione come il ransomware.

Con i metodi di backup tradizionali, inoltre, il ripristino di file e cartelle è un processo lento e manuale che può impedirti di rispettare gli SLA.



Il quadro è chiaro: con la crescita dei dati non strutturati, affidarsi ancora a soluzioni di backup tradizionali è la via giusta per il disastro. Esaminiamo cinque modi in cui una moderna soluzione di protezione dei dati non strutturati può ridurre i tuoi rischi, rendere resilienti i dati e garantire operatività all'azienda in caso di attacco.

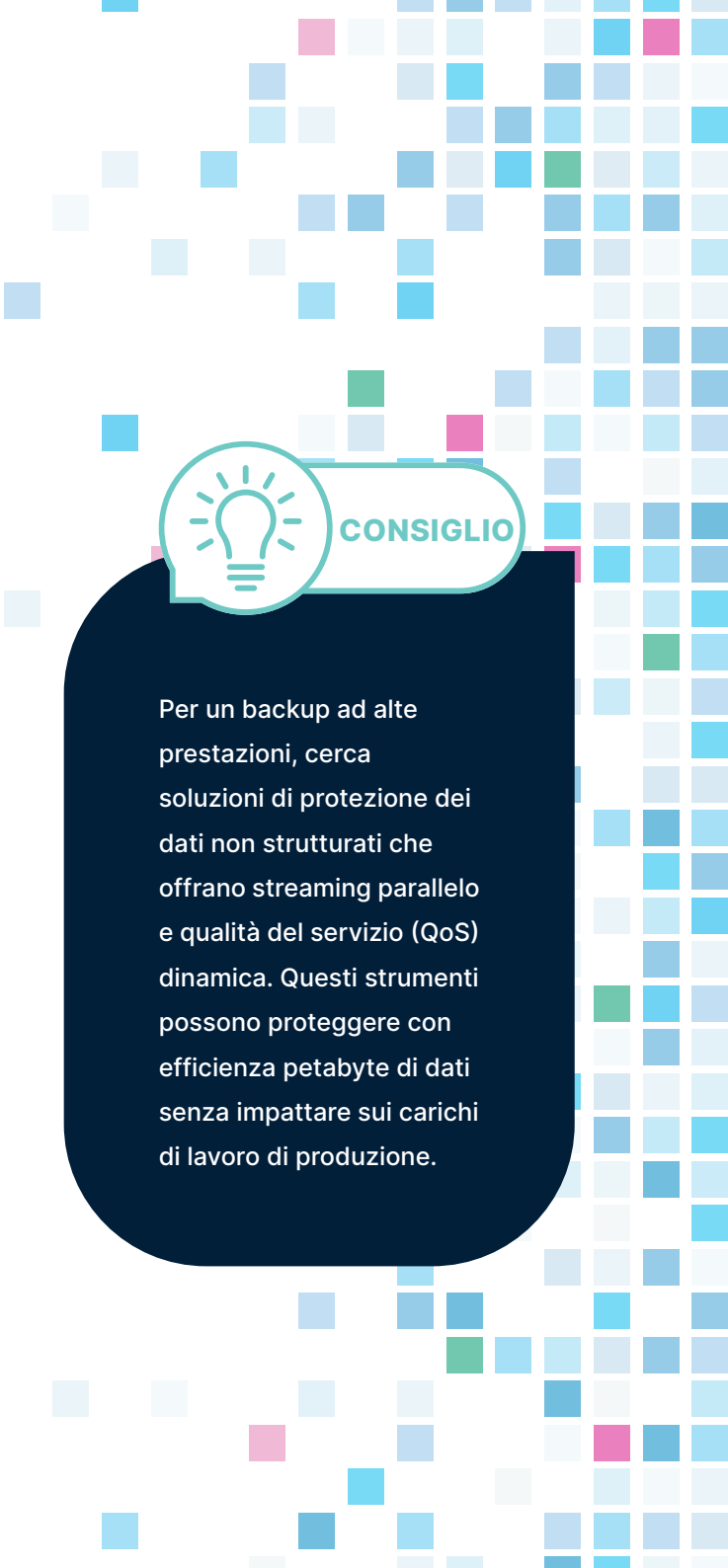
CINQUE REQUISITI
INDISPENSABILI PER UNA SOLUZIONE DI PROTEZIONE DEI DATI NON STRUTTURATI

1 Prestazioni su scala petabyte per la protezione dei dati non strutturati

I sistemi di backup legacy entrano in crisi quando i dati non strutturati arrivano su scala petabyte. Il motivo è semplice: questi strumenti obsoleti non sono stati concepiti per gestire gli elevati requisiti di volume e velocità di elaborazione necessari per proteggere miliardi di file.

Di fronte a una mole di dati così elevata, i sistemi di backup tradizionali iniziano a cedere. Le prestazioni iniziano a rallentare, sia all'interno dello stesso sistema di backup che nei sistemi sottoposti a backup. Gli obiettivi del punto di ripristino (RPO) iniziano a slittare insieme alla finestra di backup, mettendo a rischio informazioni critiche. Ma ricorrere ad altre soluzioni hardware per risolvere il problema è una scelta costosa e poco produttiva. Il protocollo di gestione dei dati di rete (NDMP) e altri approcci tradizionali non hanno la consapevolezza delle applicazioni e la scalabilità necessarie per gestire con efficienza volumi di dati così estesi. Quindi, anche con hardware aggiuntivo, si finirà comunque per riscontrare gli stessi problemi.

Ma allora qual è la soluzione? È necessaria una metodologia moderna che consenta di proteggere con efficienza miliardi di file tramite scansioni, indicizzazioni e spostamenti di dati altamente parallelizzati. Massimizzando la produttività e regolando dinamicamente le risorse per un utilizzo ottimale della rete, si possono ridurre le finestre di backup e proteggere totalmente i dati senza spendere una fortuna.

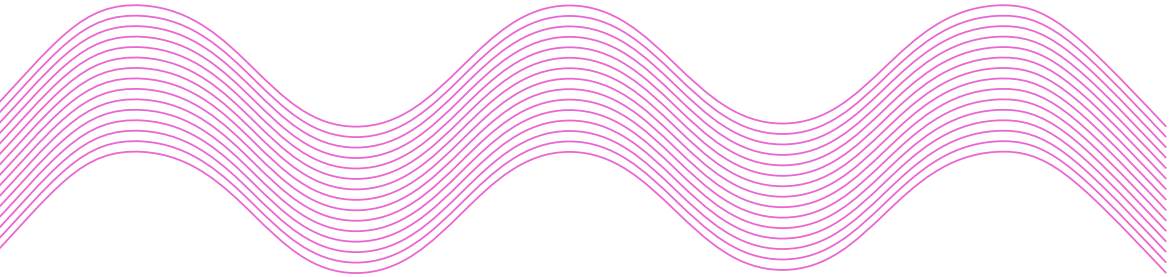


2 Visibilità olistica su tutti i tuoi dati non strutturati

Come abbiamo visto i dati non strutturati sono sparsi su più piattaforme e ubicazioni NAS, pertanto è difficile sapere esattamente dove si trovano, chi vi ha accesso e se la loro protezione è adeguata.

Le soluzioni di backup tradizionali non facilitano la visualizzazione e la protezione di tutti questi dati. Queste soluzioni spesso si basano su architetture isolate che richiedono policy, pianificazioni e supervisione proprie, rendendo quasi impossibile mantenere una strategia di protezione dei dati coerente e basata sugli SLA. In questo modo è estremamente difficile avere una visione complessiva dell'impronta globale dei dati non strutturati. Senza informazioni centralizzate sulla crescita dei dati, sui pattern di utilizzo e sulle tendenze, non è possibile gestire efficacemente il ciclo di vita dei dati o prendere decisioni strutturate su cosa conservare e cosa archiviare. E se esegui il backup dei dati sul cloud, conservare grandi quantità di dati nel livello sbagliato può modificare in modo significativo i tuoi costi cloud.

È ora di governare i tuoi dati non strutturati con un approccio unificato che ti offra una supervisione generale da un'unica interfaccia. L'uso di dashboard centralizzate, ad esempio, può fornirti informazioni utili per la gestione proattiva dei dati, garantendo al contempo l'applicazione coerente delle policy.



CONSIGLIO

Insisti su soluzioni che forniscano un piano di controllo unificato per gestire la protezione dei dati non strutturati su tutti i sistemi e le ubicazioni NAS. Una visibilità generale e centralizzata è essenziale per sviluppare un ciclo di vita dei dati aziendali ottimizzato e conforme.

3 Sicurezza dei dati enterprise con rilevamento delle anomalie su larga scala

I criminali informatici stanno intensificando i loro attacchi e i tuoi dati sono un target. Il 93% delle organizzazioni ha segnalato di aver subito tentativi di compromissione dei propri backup nel corso di un attacco informatico e nel 73% dei casi questi tentativi sono almeno in parte riusciti.[2]

Parte del problema risiede nel fatto che le soluzioni legacy lasciano spesso i dati di backup online, quindi accessibili, e non riescono a fornire solidi air gap logici. Gli **air gap** isolano e nascondono i tuoi backup, rendendoli invisibili alle minacce. Senza air gap, i backup rimangono vulnerabili, compromettendo la tua capacità di ripristino in caso di attacco.

Questo è anche il motivo per cui i **backup immutabili**, cioè i backup che non si possono modificare, eliminare o cambiare, sono così importanti. Ma gli strumenti tradizionali spesso non offrono questa caratteristica. Se i tuoi backup non sono immutabili, un attacco potrebbe sovrascriverli e non lasciare alcun punto di ripristino pulito.

Come se non bastasse, gli strumenti legacy spesso offrono pochi **controlli di accesso basati sui ruoli** e permessi troppo estesi. Questa lacuna nella sicurezza lascia una porta aperta a insider malevoli e hacker che rubano le credenziali. Senza controlli degli accessi granulari e basati sui ruoli che richiedano l'accesso con privilegi minimi, gli utenti (o gli autori delle minacce che utilizzano credenziali rubate) possono accedere a più dati di quelli gli occorrono, aumentando il rischio di compromissione dei dati.

È necessario modernizzare la protezione dei dati non strutturati con soluzioni che prevedano controlli di sicurezza integrati. La tua checklist dovrebbe includere: air gap, immutabilità del backup, controlli di accesso basati sui ruoli e **rilevamento delle anomalie**.

Il rilevamento delle anomalie aiuta a determinare la portata di un attacco perché identifica eliminazioni, modifiche e crittografie, assicurandoti un'indagine ottimale sul ransomware. Con queste informazioni, puoi intervenire in modo mirato e recuperare solo i dati di cui hai bisogno senza dover avviare un processo di recupero completo (e lungo), ripristinando velocemente l'operatività e mantenendo i dati intatti.

CONSIGLIO

Dai priorità a soluzioni di protezione dei dati non strutturati con robusti air gap logici, backup immutabili, controlli di accesso granulari basati sui ruoli e rilevamento delle anomalie. Queste difese a più livelli cooperano per proteggere i dati di backup da accessi e modifiche non autorizzati e possono aiutarti a ripristinare l'operatività in caso di attacco.

2 The State of Data Security: The Hard Truths, https://www.rubrik.com/zero-labs/2023-spring

4 Visibilità e classificazione dei dati sensibili

Per dati sensibili si intendono tutte le informazioni che, se compromesse, potrebbero danneggiare persone o organizzazioni. Ciò può includere informazioni di identificazione personale (PII), dati finanziari, proprietà intellettuale, cartelle cliniche o ogni altra informazione riservata che richieda protezione per ragioni di privacy, sicurezza e conformità.

La gestione e la protezione dei dati sensibili sono una priorità assoluta per mantenere la conformità legale e la fiducia dei clienti. Tuttavia, con la crescita dei dati non strutturati a livello di petabyte, individuare e identificare i dati sensibili o regolamentati diventa un'impresa.

Gli strumenti di backup tradizionali non offrono funzionalità native per individuare e classificare i dati. Senza informazioni precise sui tipi di dati sensibili in proprio possesso o su dove risiedono, la postura di sicurezza e conformità è soggetta a rischiosi punti ciechi.

Non poter identificare i dati sensibili, come PII, PHI e PCI, nascosti nei propri set di dati non strutturati rende vulnerabili all'esposizione involontaria e alla non conformità alle normative sulla privacy, come GDPR, HIPAA e CCPA. Non è possibile applicare protezioni adeguate se non si sa dove risiedono i dati critici.

La mancanza di consapevolezza dei dati comporta inoltre un uso inefficiente delle risorse di backup e costi più elevati. Senza una conoscenza dettagliata sul valore e la sensibilità dei dati, si è costretti a trattarli tutti allo stesso modo. Eseguire il backup e la replica di informazioni non critiche in modo superfluo comporta in definitiva un aumento dei costi di archiviazione.

Per ridurre l'esposizione dei dati sensibili e semplificare la conformità, occorrono soluzioni moderne in grado di unire la protezione dei dati a una profonda intelligence dei contenuti. Con il discovery, la classificazione e la segnalazione automatiche dei dati sensibili puoi concentrarti sulla protezione dei dati più critici, suddividendoli in base al livello di rischio e gestendo meglio i costi.

Richiedi soluzioni di protezione dei dati con funzionalità integrate di discovery e classificazione dei dati sensibili. Individuando i dati regolamentati e valutando i rischi per la privacy e la sicurezza, queste informazioni aiutano a migliorare la governance dei dati e a dimostrare la conformità. Consentono inoltre di sapere meglio ciò che si possiede, per proteggere meglio le informazioni critiche ed eseguire il backup solo di ciò che serve.

5 Recovery dei dati granulare ed efficiente

Per oltre il 90% delle aziende di medie e grandi dimensioni, il costo medio di una singola ora di downtime supera oggi $ 300.000, secondo l'indagine di Information Technology Intelligence Consulting *Rapporto sul costo orario dei downtime del 2024*.[3] In caso di incidente informatico ogni secondo è prezioso, ed è necessario ripristinare il sistema in modo rapido e preciso per ridurre al minimo le perdite. Ma potrebbe essere difficile riuscirci se si utilizzano ancora soluzioni di backup tradizionali.

Avvalersi di strumenti di backup legacy per recuperare i propri dati è come cercare un ago in un pagliaio. Senza funzionalità di ricerca granulare, gli amministratori IT sono costretti a setacciare una miriade di dati sparsi nell'intero ambiente per cercare di individuare cosa è stato colpito da un attacco o da un disastro.

Se non è possibile individuare i dati interessati, l'unica scelta è recuperare interi sistemi. Questa opzione intasa le reti, sovraccarica i dispositivi di archiviazione e alla fine rallenta il recovery. E come puoi avere la certezza che i dati di cui stai facendo il backup siano effettivamente puliti?

Ecco un altro aspetto in cui le soluzioni legacy sono spesso carenti: non consentono di verificare l'integrità del backup, quindi corri il rischio di ripristinare dati danneggiati o infetti senza rendertene conto. In un attimo ti ritrovi al punto di partenza, ma avendo sprecato tempo e risorse preziose. A ciò si aggiunge che le soluzioni legacy non hanno processi di ripristino automatizzati, il che rallenta ulteriormente le attività.

Per ridurre la perdita di dati e i tempi di recovery, servono strumenti moderni che consentano un ripristino rapido e mirato su larga scala. Le opzioni di ricerca approfondita e di ripristino granulare permettono di recuperare rapidamente i dati di cui hai bisogno. La verifica dei backup e i flussi di lavoro di recovery automatizzati accelerano l'intero processo.

CONSIGLIO

Scegli strumenti che offrano un recovery rapido e mirato su larga scala, in modo da individuare e recuperare rapidamente dati specifici senza eseguire ripristini completi del sistema. Inoltre, cerca le funzioni di verifica e automazione dei backup che semplificano il processo di recovery, riducono gli errori umani e migliorano l'efficienza del ripristino.

3 ITIC 2024 Hourly Cost of Downtime Report Part 1, https://itic-corp.com/itic-2024-hourly-cost-of-downtime-report/

MODERNIZZARE LA PROTEZIONE DEI DATI NON STRUTTURATI

Le soluzioni di backup legacy hanno svolto bene la loro funzione storica ma oggi lo scenario dei dati e delle minacce si è evoluto. I dati non strutturati ora richiedono la stessa rigorosa protezione e gestione di tutti gli altri dati critici.

Per risolvere queste sfide, è essenziale trovare una soluzione progettata per gestire dati non strutturati su scala petabyte. Rubrik NAS Cloud Direct offre funzionalità chiave per una protezione all'avanguardia dei tuoi asset critici.

Ecco in che modo Rubrik NAS Cloud Direct fornisce una protezione dei dati non strutturati senza lacune:

Backup rapido e prestazioni su larga scala

Rubrik NAS Cloud Direct offre backup e recovery di petabyte di dati e di miliardi di file in modo più rapido ed efficiente rispetto a NDMP, andando molto oltre i sistemi di backup tradizionali. La scansione, l'indicizzazione e il movimento dei dati in parallelo massimizzano il throughput, mentre la qualità del servizio intelligente evita impatti sui carichi di lavoro di produzione.

> Configurazione facile del backup, backup molto veloce e procedure di recovery semplicissime.

Sr. IT Infra Admin
Società di servizi per il divertimento e ricreativi

Gestione e visibilità unificate

NAS Cloud Direct offre un piano di controllo centralizzato per la gestione unificata dei dati non strutturati. Le dashboard globali forniscono informazioni e report utili per ottimizzare la protezione, l'archiviazione e la conformità. Puoi semplificare le tue operazioni con policy coerenti per l'intera area operativa.

> Rubrik NAS Cloud Direct ha migliorato la nostra efficienza generale in termini di velocità e delivery.

Lead Product Designer
Società finanziaria

Sicurezza avanzata dei dati con rilevamento delle anomalie

Rubrik NAS Cloud Direct migliora la sicurezza dei dati grazie ad air gap logici, backup immutabili e controlli di accesso basati sui ruoli. Inoltre, con Rubrik Anomaly Detection, ricevi una notifica se qualcosa va storto e puoi così valutare il potenziale impatto di un attacco. Con Rubrik puoi vedere come è avvenuto l'attacco, identificare le attività nocive, rispondere e ripristinare rapidamente i dati.

> Ora possiamo monitorare e analizzare i backup NAS e ricevere avvisi se si verifica qualcosa di anomalo, per intervenire immediatamente.

Kevin Mortimer
Responsabile delle operazioni, Università di Reading

Monitoraggio e conformità dei dati sensibili

NAS Cloud Direct combina protezione dei dati e intelligence dei contenuti per rilevare, classificare e segnalare i dati sensibili. Automatizza il discovery di PII, PHI, PCI e di altri dati regolamentati per valutare i rischi di conformità e trovare e proteggere facilmente le risorse di dati più critiche.

> NAS Cloud Direct monitora il sistema e mi avvisa se succede qualcosa. Mi fa dormire meglio la notte.

Travis Spurley
Ingegnere di sistemi senior, Quantum Spatial

Recovery rapido e granulare su larga scala

Rubrik NAS Cloud Direct consente la ricerca istantanea e il recovery granulare per ridurre al minimo la perdita di dati e i downtime. Durante un attacco, NAS Cloud Direct esegue ricerche rapide su miliardi di file e orchestra il recovery per farti ripristinare l'operatività il prima possibile.

> È straordinario poter effettuare ricerche su milioni, se non miliardi di file. La soluzione Rubrik ha sicuramente migliorato la nostra capacità di fare il nostro lavoro.

Carl Lucas
VP di Information Technology, Quantum Spatial

Non lasciare che il tuo fornitore di backup legacy metta a rischio i tuoi dati non strutturati. Rubrik ti consente di proteggere e gestire con efficienza enormi set di dati non strutturati, assicurandoti la resilienza contro minacce in continua evoluzione.

rubrik

È ora di adottare soluzioni moderne.

Scopri di più su Rubrik e NAS Cloud Direct.