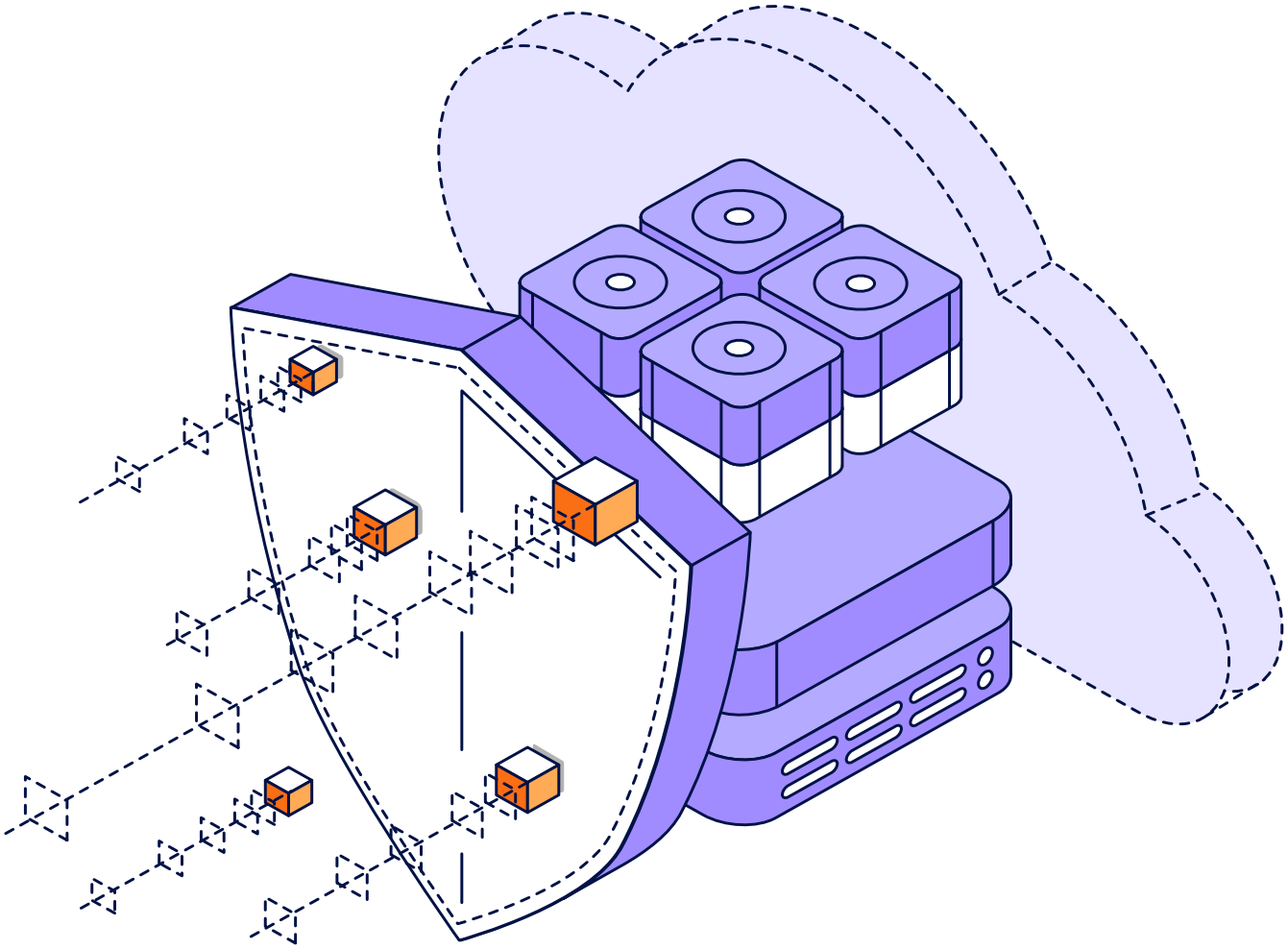
Resilienza informatica per il cloud ibrido

Lezioni apprese da oltre 7.000 professionisti IT e della sicurezza



Negli ultimi anni si è assistito al passaggio dai data center on-premises al "***cloud, quando ha senso***", alle strategie ***cloud-first***, all'***ibrido ovunque***, al punto in cui la maggior parte delle organizzazioni si trova oggi con il "***multi-cloud strategico***" come modalità normale di erogazione dell'IT moderno. Per il 2024, le domande non riguardano se utilizzare servizi basati su cloud, né quali servizi cloud utilizzare. Al contrario, le organizzazioni si chiedono quanti cloud siano necessari e come i loro team IT gestiranno tutti i cloud, garantendo al tempo stesso la prevenzione della sicurezza informatica, la protezione dei dati e altri controlli IT critici.

Per offrire risposte a queste domande, questo brief di ricerca seleziona tre fonti di ricerca indipendenti consultate tra agosto 2022 e marzo 2023, tra cui:

- **Tendenze nella protezione in cloud 2023**
  Con interviste a 1.700 amministratori IaaS, PaaS e SaaS sulle strategie di protezione dei dati.
- **Report sulle tendenze nella protezione dei dati 2023**
  Con interviste a 4.200 leader IT responsabili delle strategie di protezione dei dati della loro organizzazione.
- **Report sulle tendenze nel ransomware 2023**
  Con interviste a 1.200 CISO/SecPro/professionisti del backup le cui organizzazioni hanno subito un attacco informatico nel 2022.

Tutte e tre le attività di ricerca sono state condotte da enti di ricerca o analisti indipendenti provenienti da gruppi imparziali, con i dati poi acquisiti e pubblicati in varie forme da Veeam®. In questo report vengono costantemente messe in luce quattro aree chiave:

- I servizi basati sul cloud sono fondamentali per proteggere i data center e i carichi di lavoro in hosting nel cloud.
- I cloud sono altrettanto suscettibili agli attacchi ransomware, se non di più.
- Usare un cloud per proteggerne un altro è una buona idea; usare lo stesso cloud per proteggerlo non lo è.
- I team di sicurezza, DR, cloud e on-premises non sono allineati; questa è la prima cosa da correggere!

I servizi basati sul cloud sono fondamentali per proteggere i data center e i carichi di lavoro in hosting nel cloud

L'82%

delle organizzazioni ora utilizza uno storage basato sul cloud con capacità di immutabilità.

La ricerca mostra costantemente che i servizi basati su cloud sono un aspetto indispensabile per proteggere i tradizionali carichi di lavoro on-premises, così come i carichi di lavoro in hosting nel cloud. *In particolare, lo storage basato su cloud consente di avere* ***repository "in grado di sopravvivere"*** *(ad esempio l'immutabilità) così come* ***infrastruttura di disaster recovery*** *quando serve.*

Per la maggior parte delle organizzazioni, esistono verità quasi universali in materia di protezione dal ransomware:

- Per proteggere i server del data center, porta i tuoi dati fuori dall'edificio (ad esempio offsite o in un cloud).
- Per eseguire il ripristino dal ransomware, serviranno copie di backup che le minacce informatiche non possano colpire.

Secondo la Ricerca sulle tendenze nel ransomware 2023, la combinazione dei due assiomi è evidente nel 2023, come una "lezione appresa", con l'**82%** delle organizzazioni che ora utilizza storage basato su cloud dotato di immutabilità.[1]

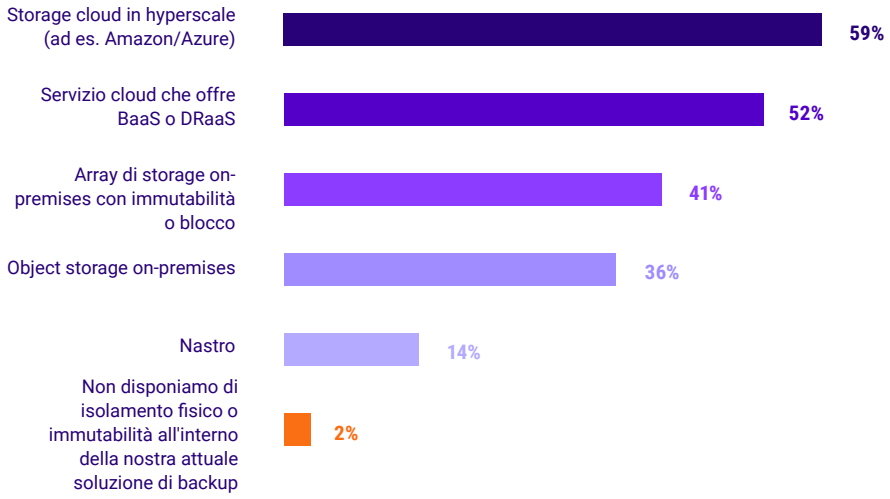


Figura 1.1

La vostra organizzazione utilizza backup offline, fisicamente isolati o immutabili con i seguenti sistemi?

Dopo aver verificato che l'organizzazione disponga di copie di backup in grado di sopravvivere, è possibile prendere in considerazione anche altri aspetti di una tradizionale strategia di continuità aziendale o di disaster recovery (BC/DR). Se si considera che gli attacchi informatici sono sempre più considerati un'altra (anche se speciale) forma di disastro, non sorprende che molti considerino la resilienza informatica e il disaster recovery come altamente correlati. In entrambi i casi, la domanda successiva più pragmatica è **"Dove eseguirai il ripristino o il failover?"**

Come appreso dalle vittime di attacchi informatici, le strategie di ripristino delle organizzazioni includono la capacità di ripristinare i server dei data center su un'infrastruttura in hosting nel cloud durante le operazioni di rimedio dal ransomware o da un'altra crisi.[2]

Figura 1.2

Quando ripristinate i server dal ransomware, dove ripristinate i vostri dati?

I dati sopra riportati mostrano che la maggior parte delle organizzazioni ha predisposto una strategia ibrida flessibile, basata sulla portata della crisi. Infatti, il **71%** delle organizzazioni è in grado di ripristinare usando un cloud, mentre l'**81%** può ripristinare utilizzando un'infrastruttura on-premises, con una buona dose di sovrapposizione (flessibilità). Nella più ampia gamma di crisi per le quali le organizzazioni si preparano nei piani di disaster recovery, il **54%** pianifica il failover in una posizione alternativa, mentre il **46%** **prevede di usare un'infrastruttura in hosting nel cloud come sito di disaster recovery**. Detto questo, esiste più di un modo per realizzare un sito di disaster recovery basato sul cloud.[3]

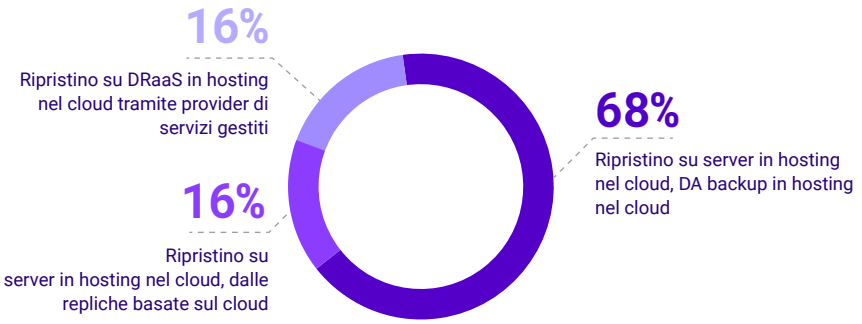


Figura 1.3

Quando utilizzate i servizi cloud per il disaster recovery, in che modo viene ripresa l'operatività?

Che il piano di disaster recovery utilizzi un provider di Disaster Recovery as-a-Service (DRaaS) o un'infrastruttura autogestita in hosting nel cloud, come Amazon Web Services o Microsoft Azure, esistono almeno due funzionalità fondamentali per il successo:

- La capacità di trasformare un backup durante il ripristino, in modo tale che un production server protetto mentre era originariamente fisico o virtuale, venga ripristinato e attivato all'interno di un host cloud.
- La capacità di orchestrare il processo di ripristino, incluso l'isolamento in quarantena per il rilevamento di malware durante il flusso di lavoro di ripristino.

Purtroppo, solo

- Il **18%** delle organizzazioni è in grado di creare script per flussi di lavoro orchestrati per il ripristino con failover.[4]
- Il **44%** utilizza un'area di test isolata o "sandbox" per eseguire la scansione del malware durante il ripristino, per avere la certezza di non infettare nuovamente l'ambiente.

Queste dovrebbero essere domande difficili da rivolgere ai dirigenti senior per sapere se la soluzione o il servizio di protezione dei dati dell'organizzazione è in grado di automatizzare il ripristino su larga scala e/o garantire un ripristino sicuro.

I cloud sono altrettanto suscettibili agli attacchi ransomware, forse di più

Presumibilmente perché i servizi basati su cloud sono perfettamente accessibili all'interno delle architetture IT ibride, la ricerca rivela costantemente che **i carichi di lavoro basati sul cloud hanno la stessa probabilità di essere colpiti durante un attacco informatico**. *Infatti, se si considera che molte organizzazioni devono utilizzare diverse tecnologie di sicurezza per impedire l'accesso ai servizi cloud rispetto alle risorse dei loro data center, diventano possibili ulteriori opportunità di attacco, come l'interruzione della connettività tra gli utenti e le loro piattaforme cloud.*

Oltre a riconoscere che "il cloud non sta arrivando, è già qui", bisogna anche riconoscere che l'IT non sta dismettendo le piattaforme on-premises allo stesso ritmo con cui vengono avviati nuovi carichi di lavoro all'interno dei servizi basati sul cloud. Le organizzazioni continuano ad adottare l'infrastruttura in hosting nel cloud come parte integrante di una strategia sempre più ibrida per la delivery dell'IT.

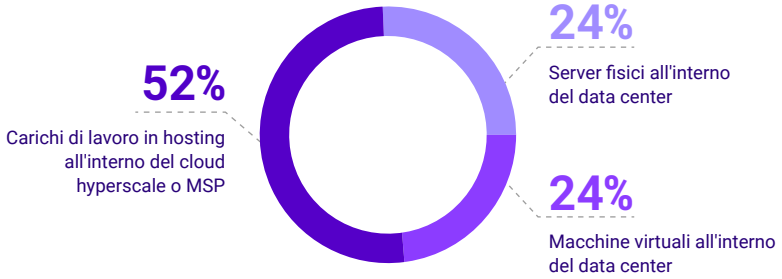


Figura 2.1

Implementazione "ibrida" delle piattaforme prevista per i carichi di lavoro dei production server nel 2024.[6]

Va notato che, a differenza dell'evoluzione delle piattaforme all'interno di un IT incentrato sui data center, non esiste solamente un'"unica architettura cloud" da implementare, utilizzare e proteggere, indipendentemente dal fornitore del cloud. Si devono invece considerare una miriade di architetture cloud, ciascuna realizzata da una varietà di provider, i cui framework di gestione sottostanti variano notevolmente.

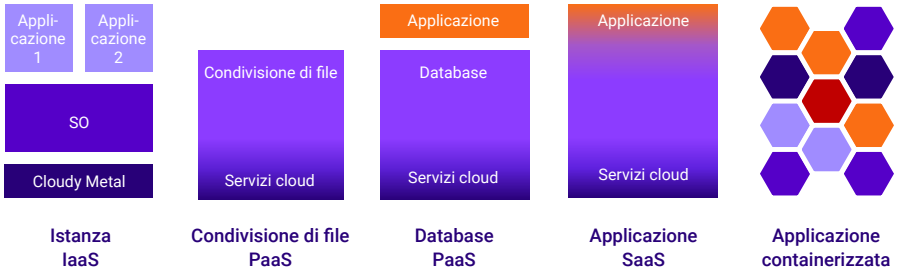


Figura 2.2

Miriadi di architetture cloud.

Purtroppo, sebbene i servizi basati su cloud siano spesso percepiti come resilienti, si verificano comunque interruzioni, a causa dei problemi interni del provider di servizi cloud, di configurazioni errate dell'amministratore tra i servizi cloud e della connettività tra gli utenti e i servizi cloud stessi. Detto questo, in entrambi i rapporti di ricerca del 2021 e del 2022, le interruzioni del servizio dovute ad attacchi informatici sono aumentate di anno in anno, rimanendo anche la causa delle interruzioni di maggiore impatto sia nel 2021 che nel 2022 (senza alcun segno di rallentamento nel 2023).[6]

- Il **48%** delle organizzazioni ha subito interruzioni IT a causa di **"risorse del cloud pubblico non disponibili".**
- Il **52%** delle organizzazioni ha subito interruzioni IT a causa di **"indisponibilità dell'infrastruttura o della rete".**
- Il **53%** delle organizzazioni ha subito interruzioni IT a causa di un **"evento di sicurezza informatica".**

Nella maggior parte degli attacchi informatici, se l'ingresso iniziale può essere sistematicamente opportunistico (ad esempio, inviare e-mail di phishing sperando che un utente faccia clic), quegli stessi aggressori prendono poi di mira i sistemi in base a vulnerabilità note o potenziale incapacità di proteggere adeguatamente le piattaforme IT più diffuse. La ricerca basata sul Report sulle tendenze nel ransomware per il 2023 mostra che **i criminali informatici hanno preso di mira i carichi di lavoro in hosting sul cloud nel 38% degli attacchi.**[7]

Durante le interviste a 1.200 vittime di attacchi informatici, è emerso che è stata crittografata/interessata una quantità di dati in hosting nel cloud quasi uguale a quella dei dati del data center.

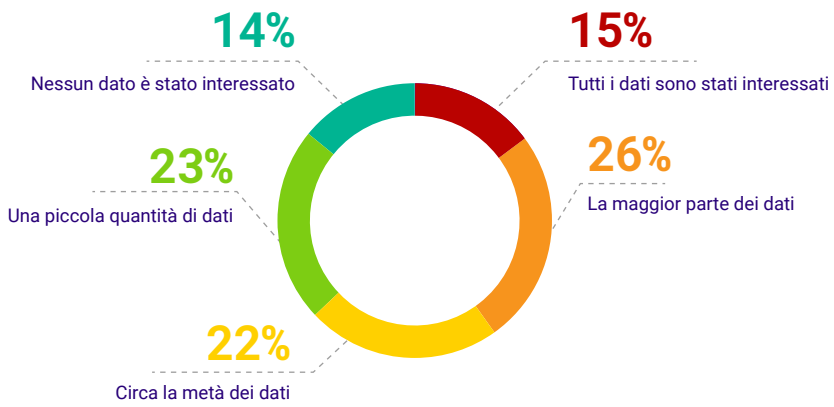


Figura 2.3

% di dati in hosting su piattaforme cloud colpiti dall'ultimo attacco ransomware.[9]

È importante notare che, dalle somiglianze nei tassi di infezione tra dati di data center, dati di filiali/remoti e dati in hosting su cloud si deducono due verità fondamentali:

- Poiché l'IT ibrido viene fornito senza soluzione di continuità, una volta che una minaccia informatica si attiva nell'ambiente della vittima, i dati in hosting nel cloud sono vulnerabili agli attacchi tanto quanto le applicazioni e i file all'interno del data center fisico.
- A causa di questa continuità e della stessa vulnerabilità, file, database e applicazioni in hosting nel cloud devono essere protetti con lo stesso rigore e le stesse metodologie dei carichi di lavoro on-premises.

Entro il 2024, per la prima volta, si prevede che verranno eseguiti più carichi di lavoro al di fuori dei data center fisici autogestiti rispetto ai data center aziendali del passato.

Usare un cloud per proteggerne un altro è una buona idea; usare lo stesso cloud per proteggerlo non lo è

2 : 1

la maggior parte della protezione dei dati viene eseguita dal team di backup IT "tradizionale" rispetto agli amministratori del cloud.

In seguito a un sondaggio su "chi" effettuava il backup dei dati dei propri cloud e su "come" i dati vengono protetti nel 2023, tutti e tre i progetti di ricerca hanno confermato che ***il team di backup "principale" (o il suo provider di servizi) che protegge il resto dei dati on-premises di un'organizzazione ha spesso anche il compito di proteggere i dati in hosting nel cloud.*** *Detto questo, c'è ancora molta confusione sul "come", un classico quando le organizzazioni presumono che la loro unica opzione sia quella di utilizzare l'utilità "integrata" di una piattaforma, invece di una soluzione per il backup aziendale eterogeneo.*

Prima di considerare "come" le organizzazioni proteggono il carico di lavoro in hosting nel cloud, è importante considerare i vari "chi": con una maggioranza relativamente consistente di 2:1 della protezione dei dati effettuata dal "tradizionale" team di backup IT rispetto agli amministratori del cloud.

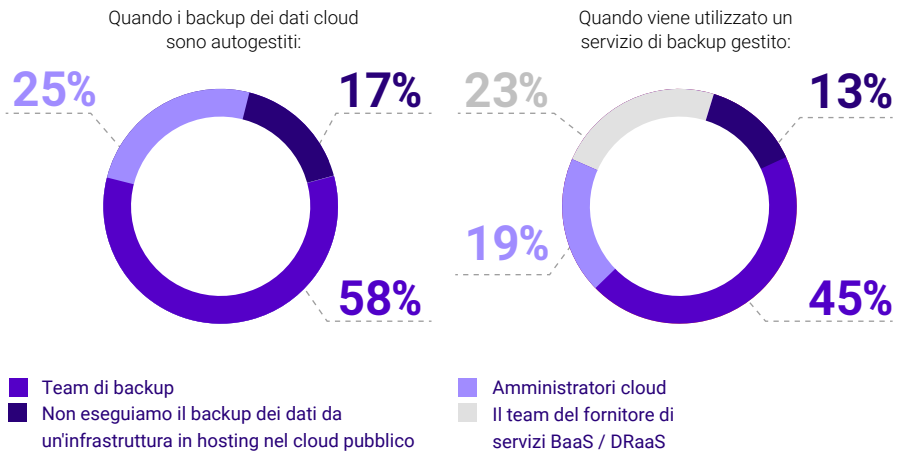


Figura 3.1

Chi gestisce i backup/la protezione dei dati dei server in hosting nel cloud nella vostra organizzazione?[10]

Sorprendentemente, un intervistato su otto **(il 13%)** ritiene che la propria organizzazione non esegua il backup della propria infrastruttura in hosting nel cloud. Quindi, la domanda successiva per molte organizzazioni che stanno adottando strategie ibride è il riconoscimento che i backup in cloud potrebbero trovarsi all'interno dello stesso cloud, in una regione diversa, in un cloud diverso o addirittura on-premises.
Questa diventa una considerazione importante quando si sceglie una soluzione di backup per carichi di lavoro in hosting nel cloud:

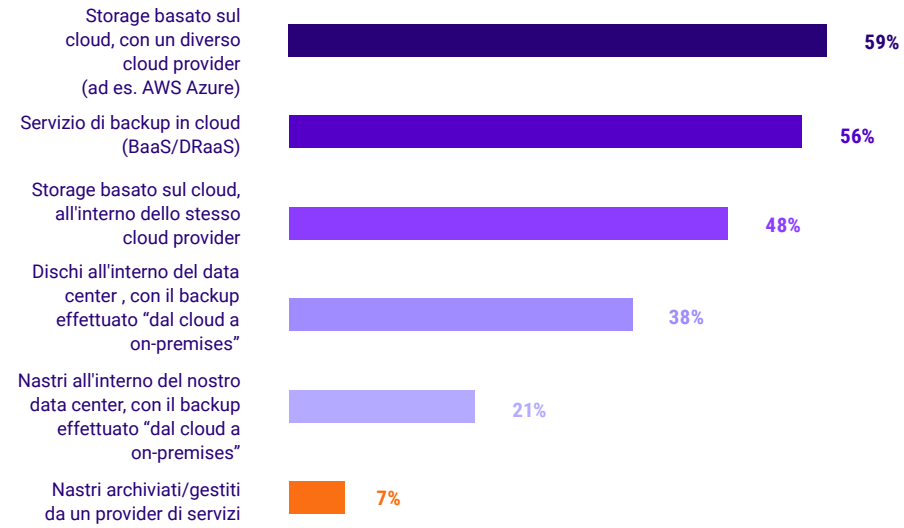


Figura 3.2

Dove archiviate i dati di cloud backup che la vostra organizzazione conserva per un anno o più?[11]

- Il **37%** dei leader IT considera la "possibilità di spostare carichi di lavoro da un cloud a un altro” come un aspetto determinante di una soluzione di protezione dei dati "moderna" o "innovativa".[12]
- L'**88%** delle organizzazioni ha riportato i carichi di lavoro on-premises da un cloud o li ha spostati su un altro cloud.[13]

Naturalmente, l’altra opzione quando si sceglie una soluzione di backup per carichi di lavoro in hosting nel cloud è semplicemente affidarsi all’utilità “integrata” o alla funzione di esportazione fornita da molte aziende cloud per ciascun particolare carico di lavoro. Spesso, il fattore limitante è semplicemente la consapevolezza che sono disponibili strumenti di terze parti che proteggono

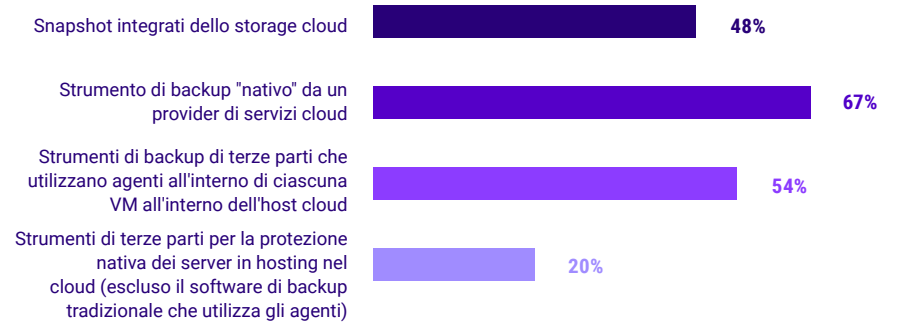


Figura 3.3

Di quali meccanismi di protezione dei dati in hosting nel cloud siete a conoscenza (indipendentemente dal fatto che li stiate usando attualmente)?

in modo completo i carichi di lavoro cloud.[14]

Se consideri gli snapshot, chiediti se ti affideresti esclusivamente agli snapshot dei tuoi file server on-premises. Gli snapshot sono potenti strumenti di ripristino per punti di ripristino quasi in tempo reale che possono essere istantanei. Tuttavia, **gli snapshot non sono mai stati un sostituto dei backup,** per questi motivi:

- Stesso silo di esposizione (correlazione di un NAS standalone a uno stack di storage IaaS, incluse le credenziali comuni).
- Costoso da mantenere nel tempo; ecco perché la maggior parte delle organizzazioni conserva pochi giorni di snapshot ma settimane, mesi e anni di backup.

Se stai considerando utilità "native" incentrate sul carico di lavoro o integrate, chiediti se le tue piattaforme on-premises sono protette in questo modo:

- Facendo affidamento solo su ZDLRA (o RMAN) per proteggere i database **Oracle**.
- Facendo affidamento solo sull'utilità di backup NT (o allo strumento di sistema) per il backup dei **server Windows**.
- Facendo affidamento solo su VDPA per il backup degli host **VMware**.
- Facendo affidamento solo su ASB per il backup di **Microsoft 365**.

Ora chiediti quanti strumenti vuole gestire il tuo team IT per il backup e di quanto budget disponi per lo storage (poiché ciascuno di questi strumenti scrive in repository e formati diversi). La creazione di snapshot e altre utilità a piattaforma singola (ad esempio "integrate") sono ancora più problematiche se si considera che la maggior parte è progettata con una gamma limitata di retention per abilitare rollback veloci in seguito a un errore recente, come una sovrascrittura di dati o un'importazione sbagliata. Se si considera come l'organizzazione ripristinerà dal ransomware che potrebbe essere rimasto inattivo per settimane, questi approcci tattici sembrano insufficienti (o proibitivi in termini di costi). Questi giudizi sono quantificati in due dati aggiuntivi:

- Il **35%** dei leader IT considera la **"protezione standardizzata di ambienti on-premises e IaaS/SaaS"** come aspetto determinante di una soluzione di protezione dei dati "moderna" o "innovativa".[15]
- Il **42%** delle organizzazioni ritiene che la **"capacità di proteggere i carichi di lavoro in hosting nel cloud"** sia un attributo indispensabile per le soluzioni di protezione dei dati aziendali.[16] Questa è stata la risposta più comune e più importante per il 2023.

Il 35%

dei leader IT considera la "protezione standardizzata di ambienti on-premises e IaaS/SaaS" come aspetto determinante di una soluzione di protezione dei dati "moderna" o "innovativa".

I team addetti a sicurezza, DR, cloud e on-premises non sono allineati; correggi questo aspetto prima di tutto!

Durante i tre progetti di ricerca è stata intervistata una varietà di ruoli, tra cui leader IT responsabili della protezione dei dati, CISO e dirigenti analoghi, professionisti della sicurezza, amministratori IaaS/PaaS/SaaS e operatori di backup. Tutte e tre le ricerche hanno rivelato che nessun singolo team possedeva una funzione principale, c'era sempre una sovrapposizione di influenza e responsabilità. Eppure, ***raramente i dati hanno dimostrato che gli intervistati ritenevano di essere ben allineati tra loro sui requisiti della strategia o sull'implementazione/utilizzo delle tecnologie.***

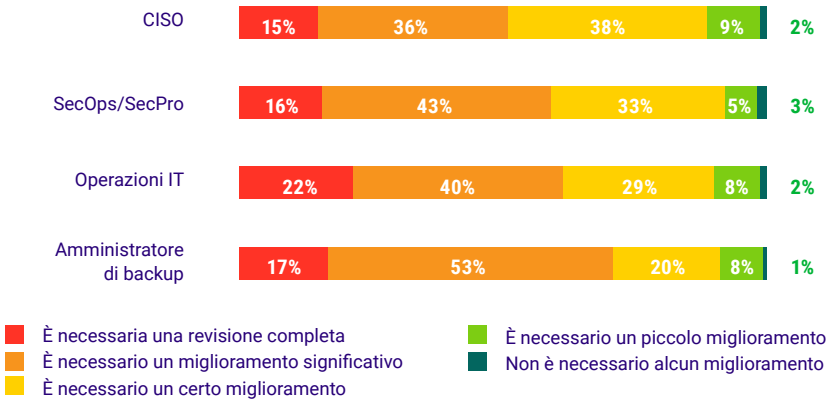


Figura 4.1

Che tipo di miglioramento ritenete sia necessario affinché i team di backup IT e i team di sicurezza informatica della vostra organizzazione siano completamente allineati?

Mentre la maggior parte di queste iniziative di ricerca si concentra sulle tecnologie utilizzate o sui motivi/sulle strategie che guidano le scelte tecnologiche, i dati dell'indagine rivelano inoltre un chiaro e costante disallineamento tra i ruoli coinvolti in queste iniziative.[17]

È importante notare che dei quattro ruoli esaminati nel **Report sulle tendenze nel ransomware 2023**, quanto più il professionista era "vicino" al rimedio dell'evento (ad esempio, amministratore di backup rispetto a CISO) meno era soddisfatto della collaborazione e dell'allineamento tra i team.

Simili disallineamenti sono stati riscontrati tra gli amministratori SaaS e gli amministratori di backup quando si considerano le motivazioni e gli strumenti per la protezione di Microsoft 365, e ancora tra gli amministratori IaaS/PaaS e gli amministratori di backup quando si considerano le strategie e gli strumenti per proteggere server, condivisioni di file e database in hosting nel cloud.

Domande da considerare!

Sulla base della ricerca che ha coinvolto oltre 7.000 intervistati in un periodo di otto mesi, alcune domande chiave da considerare nell'ambito della strategia di resilienza informatica sono:

- I nostri backup sono immutabili e off-site? I backup sono gestiti da un provider con esperienza o li gestiamo noi?
- Potremmo utilizzare l'infrastruttura cloud come sito di disaster recovery? Se la risposta è no, perché no?
- Stiamo eseguendo il backup di tutti i nostri dati in hosting nel cloud, inclusi i carichi di lavoro IaaS, PaaS e SaaS? In tal caso, stiamo utilizzando strumenti separati per cloud o implementati in modo coerente in tutti i nostri cloud (e carichi di lavoro on-premises)?
- In che misura sono allineati i nostri team in relazione al backup on-premises, IaaS, PaaS e SaaS?
- In che misura sono allineati i nostri team tra preparazione informatica e backup dei dati?
- Quando è stata l'ultima volta che abbiamo testato il ripristino dei nostri dati basati su cloud?
- Quando è stata l'ultima volta che abbiamo testato il ripristino di un data center su ampia scala?
- Quando è stata l'ultima volta che abbiamo valutato e aggiornato i nostri playbook di sicurezza informatica e BC/DR?

Per qualsiasi domanda sulla ricerca o sulle sue implicazioni, contattaci all'indirizzo StrategicResearch@veeam.com

Per leggere i report di ricerca completi che sono stati citati qui, dai un'occhiata ai link seguenti:

- **Tendenze nella protezione in cloud 2023**
  Con interviste a 1.700 amministratori IaaS, PaaS e SaaS sulle strategie di protezione dei dati.
- **Report sulle tendenze nella protezione dei dati 2023**
  Con interviste a 4.200 leader IT responsabili delle strategie di protezione dei dati della loro organizzazione.
- **Report sulle tendenze nel ransomware 2023**
  Con interviste a 1.200 CISO/SecPro/professionisti del backup le cui organizzazioni hanno subito un attacco informatico nel 2022.

Il punto di vista di Veeam

La piattaforma di backup e gestione dei dati di Veeam

Ora più che mai, è fondamentale per le aziende essere sicure che i propri dati siano protetti e sempre disponibili, che si trovino on-premises, all'edge o nel cloud. Veeam offre un'unica piattaforma per ambienti cloud, virtuali, fisici, SaaS e Kubernetes. I nostri clienti sono certi che le loro applicazioni e i loro dati sono protetti da ransomware, disastri e malintenzionati e sono sempre disponibili con la piattaforma più semplice, flessibile, affidabile e potente del settore.

Veeam offre ai clienti la sicurezza per accelerare la trasformazione digitale, proteggersi dalla criminalità informatica e promuovere la resilienza aziendale, assicurando che i dati siano sempre protetti e sempre disponibili. Riduci i costi e la complessità e raggiungi i tuoi obiettivi di business con Veeam: il n.1 del Backup e Ripristino.

Per maggiori informazioni, visita **https://www.veeam.com/it**.

Per parlare con un esperto di cloud ibrido Veeam, richiedi una consulenza **http://vee.am/hybridcloudinquiry**.

Le domande relative a questi dati di ricerca e approfondimenti possono essere indirizzate a StrategicResearch@veeam.com

1 Report sulle tendenze nel ransomware 2023, Q29
2 Report sulle tendenze nel ransomware 2023, Q25
3 Report sulle tendenze nella protezione dei dati 2023, Q45
4 Report sulle tendenze nella protezione dei dati 2023, Q46
5 Report sulle tendenze nel ransomware 2023, Q21
6 Report sulle tendenze nella protezione dei dati 2023, Q2
7 Report sulle tendenze nella protezione dei dati 2023, Q13 e Q14
8 Report sulle tendenze nel ransomware 2023, Q9
9 Report sulle tendenze nel ransomware 2023, Q6
10 Tendenze nella protezione in cloud 2023, Q6
11 Tendenze nella protezione in cloud 2023, Q8
12 Tendenze nella protezione dei dati 2023, Q17
13 Tendenze nella protezione in cloud 2023, Q4
14 Tendenze nella protezione dei dati 2023, Q35
15 Tendenze nella protezione dei dati 2023, Q17
16 Tendenze nella protezione in cloud 2023, Q4
17 Report sulle tendenze nel ransomware 2023, Q1