Global Data Protection Index 2021

Risultati principali – luglio 2021

VansonBourne

DELL Technologies

Focus dei risultati principali

1

Il panorama del rischio della protezione dei dati

2

La minaccia posta dagli attacchi informatici

3

Stare al passo con le tecnologie nuove ed emergenti

4

Vulnerabilità della protezione dei dati negli ambienti cloud

5

La crescita di as-a-Service

6

Semplifica la protezione dei dati

Cinque considerazioni principali

L'ampia adozione del lavoro da remoto ha **aumentato la protezione dei dati e i rischi informatici**

Molti non hanno fiducia nella capacità della protezione dei dati della loro organizzazione di difesa e ripresa dalle minacce informatiche

Gli investimenti costanti nelle tecnologie emergenti e nel cloud **possono contribuire a superare le sfide della protezione dei dati**

Molti sono **interessati a sfruttare soluzioni as-a-Service** per aumentare la semplicità e la flessibilità della protezione dei dati

È stato dimostrato che lavorare con **meno vendor di protezione dei dati** può portare a **risultati migliori in termini di protezione dei dati**

Chi abbiamo intervistato?

1.000 responsabili delle decisioni IT sono stati intervistati a febbraio, marzo e aprile 2021

Organizzazioni di un'ampia gamma di settori pubblici e privati

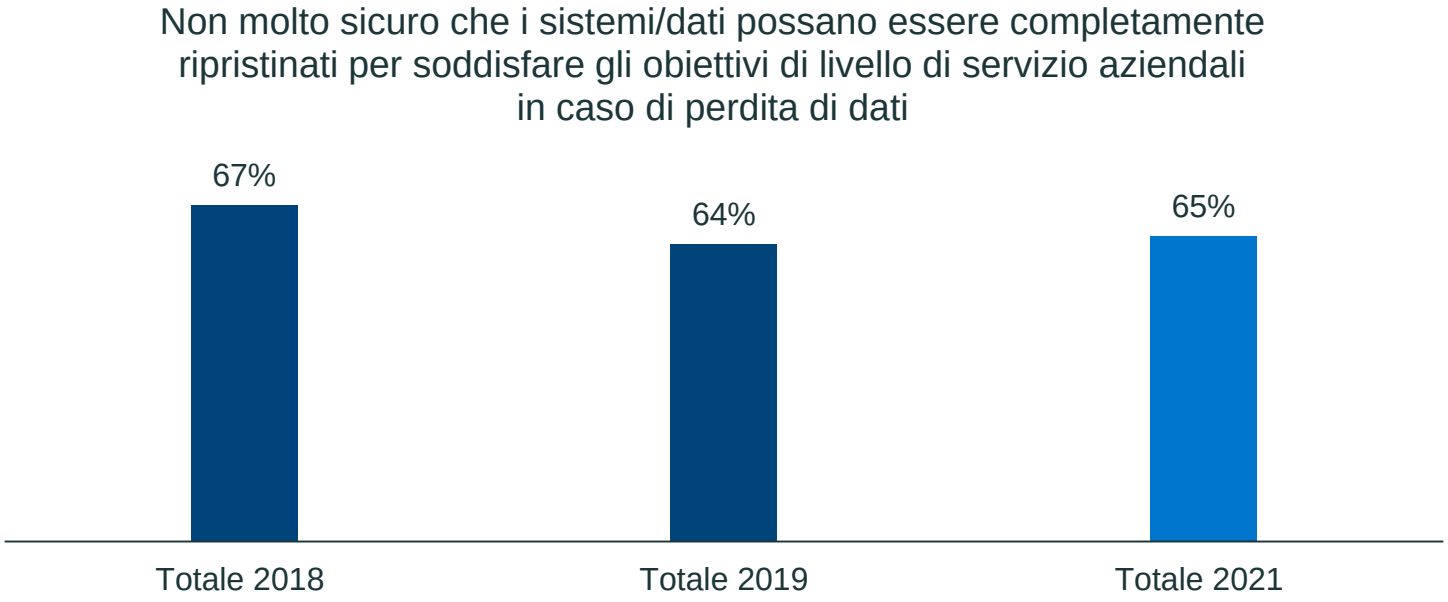
Organizzazioni con oltre 250 dipendenti

4 aree geografiche:

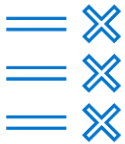
Americhe (200)
EMEA (450)
APJ (250)
Cina (100)

1. Il panorama del rischio della protezione dei dati

I responsabili delle decisioni IT non hanno fiducia nella capacità della loro organizzazione di soddisfare gli obiettivi di livello di servizio di ripristino



Inoltre, la fiducia che le capacità di protezione dei dati siano all'altezza degli standard interni ed esterni è bassa: questo è reso più preoccupante dal fatto che i due terzi credono di dover affrontare un evento di interruzione il prossimo anno



Il 58%

non è molto sicuro che la sua organizzazione stia **soddisfando gli SLO di backup e ripristino**

Il 63%

non è molto sicuro che l'infrastruttura e i processi attuali di protezione dei dati della loro organizzazione siano **conformi alle normative regionali sulla governance dei dati**

Il 64%

è **preoccupato della possibilità di dover affrontare un evento di interruzione** nei prossimi dodici mesi

A questo si aggiunge il fatto che i problemi di perdita di dati e i downtime dei sistemi continuano ad avere un impatto finanziario significativo sulle organizzazioni

$ 959.493

Costo medio della perdita di dati negli ultimi 12 mesi (in USD)

$ 513.067

Costo medio del downtime non pianificato dei sistemi negli ultimi 12 mesi (in USD)

2. La minaccia degli attacchi informatici

Le organizzazioni non sono sicure che le loro misure di protezione dei dati possano mitigare gli effetti degli attacchi informatici. Inoltre, la maggior parte ritiene che l'esposizione sia più elevata con i dipendenti che lavorano da remoto

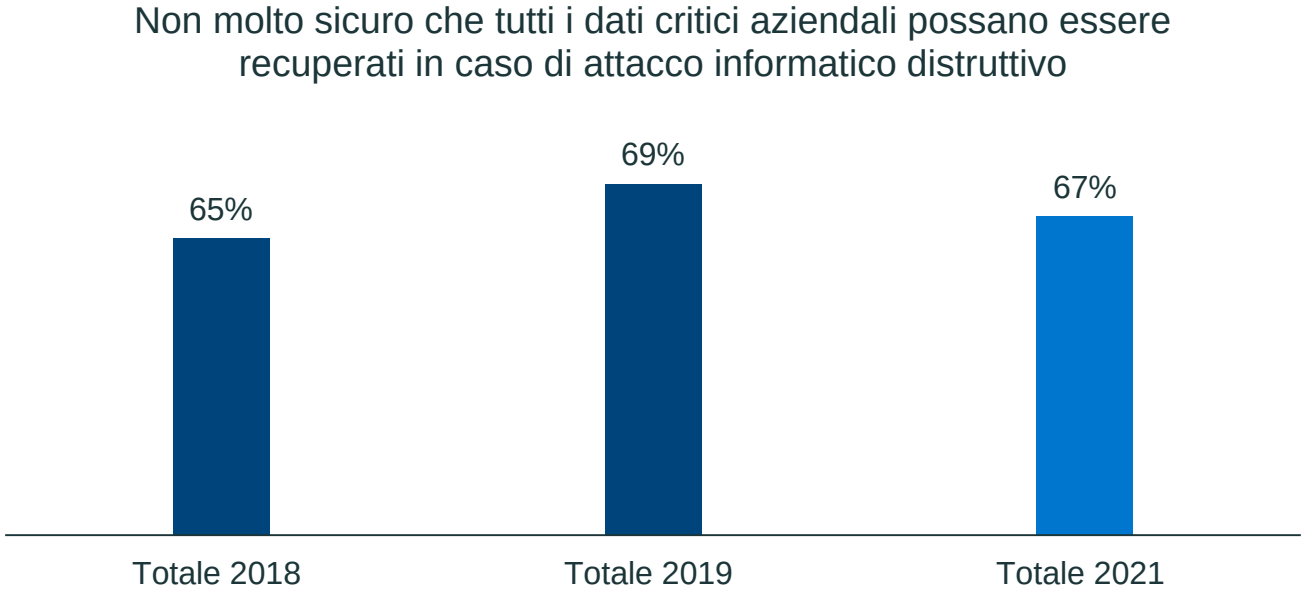
Il 62%

è preoccupato che le misure di protezione dei dati esistenti della propria organizzazione **non siano sufficienti a contrastare le minacce di malware e ransomware**

Il 74%

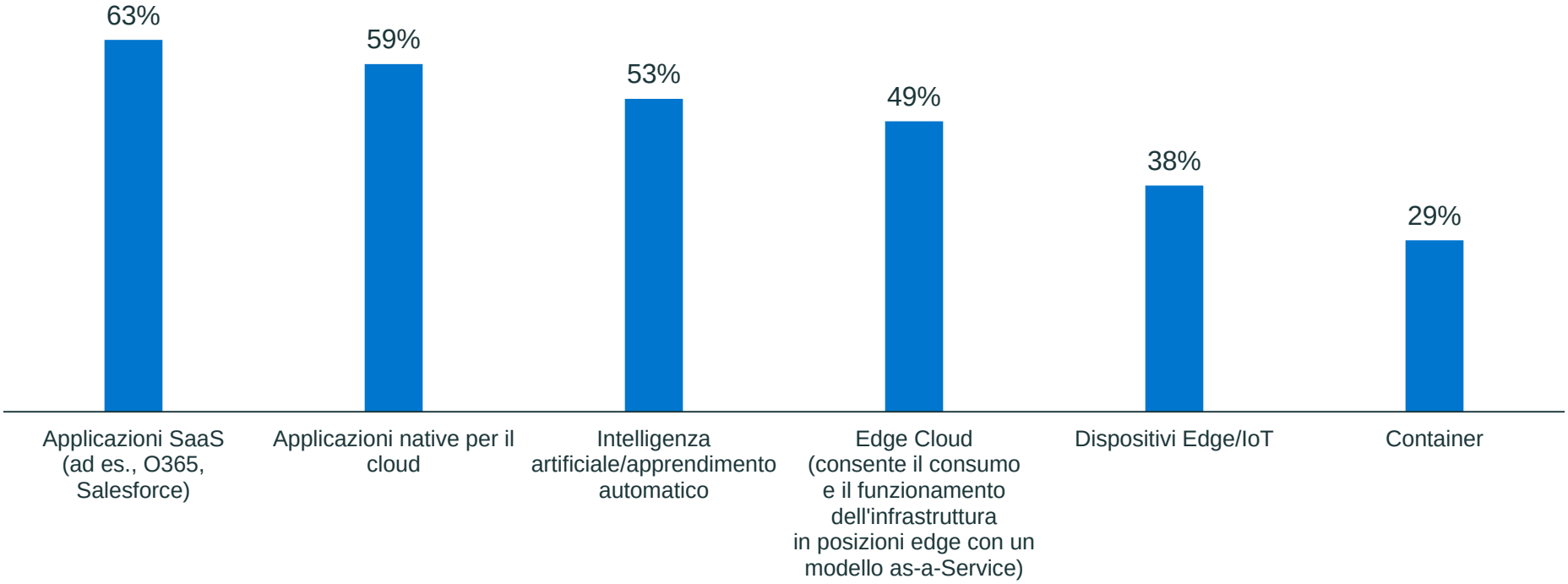
è consapevole della **maggiore esposizione della propria organizzazione alla perdita di dati** causata dalle minacce informatiche con l'aumento dei **dipendenti che lavorano da remoto**

Preoccupazioni crescenti sulla capacità delle organizzazioni di contrastare le minacce di malware e ransomware, molti non hanno fiducia nelle loro capacità di ripristino di tutti i dati critici aziendali in caso di attacco informatico distruttivo

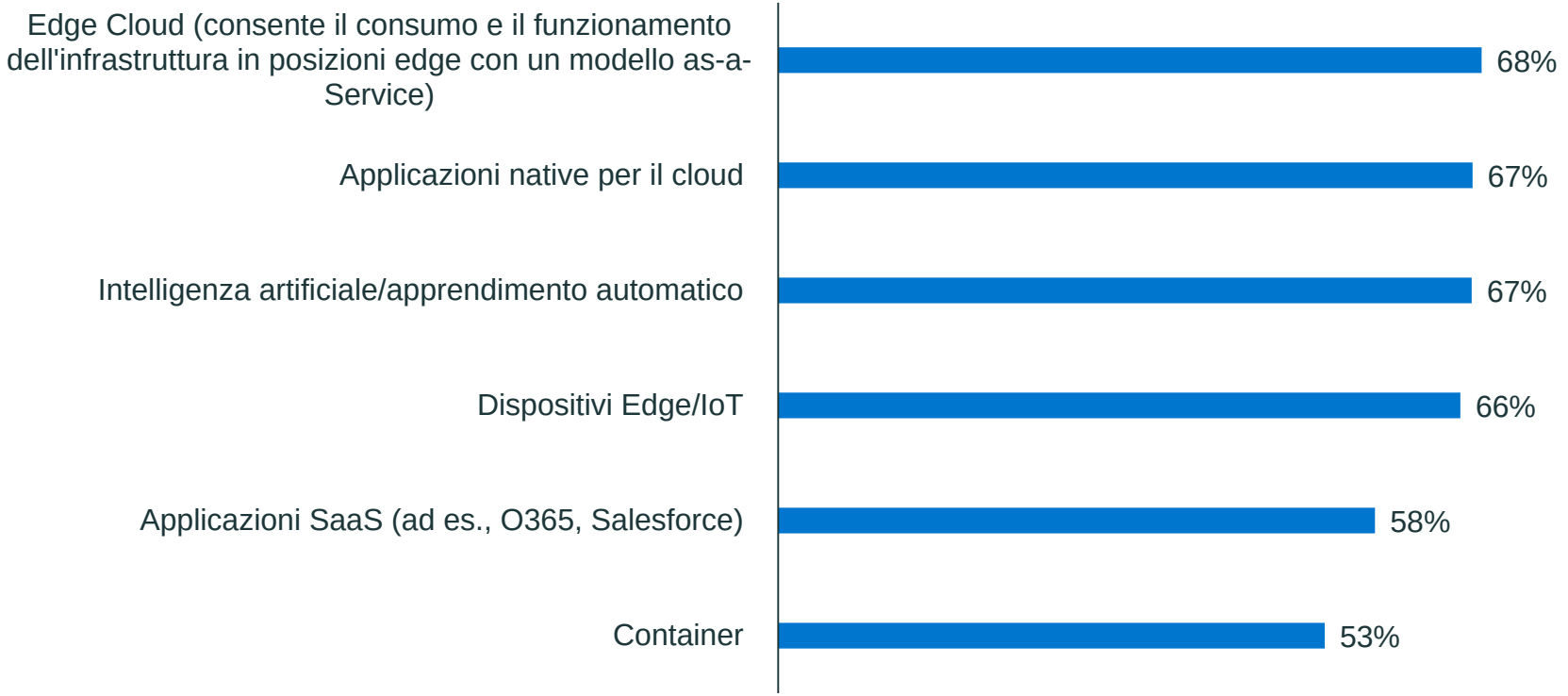


3. Stare al passo con le tecnologie nuove ed emergenti

Le organizzazioni stanno investendo in molte nuove tecnologie, che potrebbero complicare le loro sfide nella protezione dei dati



E molte organizzazioni fanno fatica a proteggere queste tecnologie



La difficoltà di proteggere tecnologie nuove ed emergenti sta probabilmente determinando una scarsa fiducia nel fatto che le soluzioni di protezione dei dati siano orientate al futuro

Molti vedono le tecnologie emergenti come un rischio per la protezione dei dati e la preoccupazione per i futuri eventi di interruzione è alta, soprattutto tra coloro che utilizzano più vendor di protezione dei dati

Le tecnologie emergenti (come l'intelligenza artificiale, l'IoT, l'edge) rappresentano un rischio per la protezione dei dati

Utilizzo di un unico vendor di protezione dei dati

57%

Utilizzo di più vendor di protezione dei dati

64%

Sono preoccupato/a di dover affrontare un evento di interruzione (ad es. perdita di dati, downtime dei sistemi, ecc.) nei prossimi 12 mesi

Utilizzo di un unico vendor di protezione dei dati

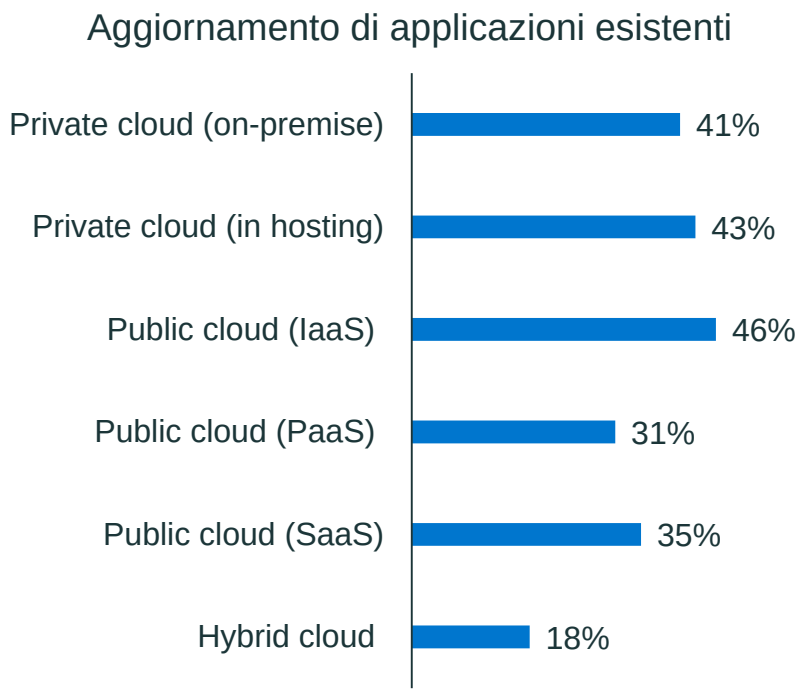
54%

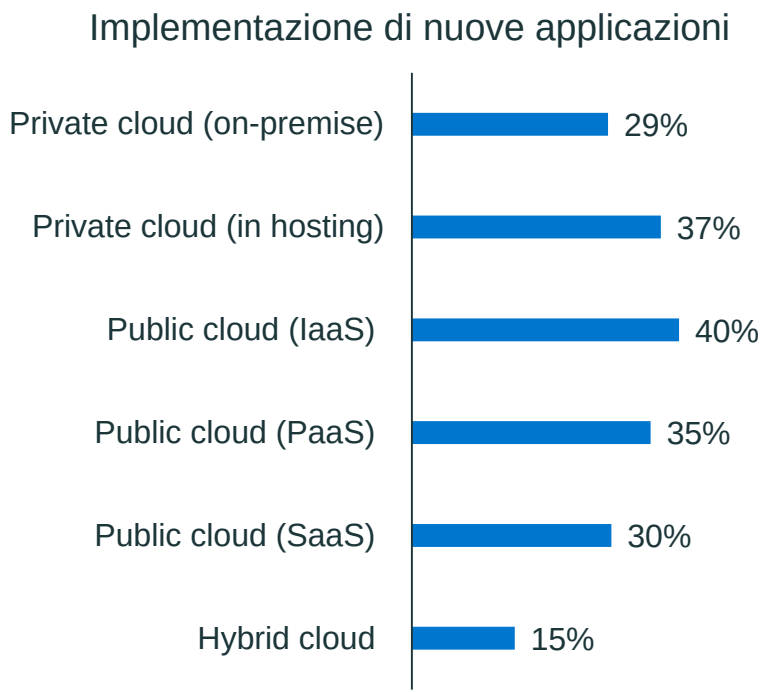
Utilizzo di più vendor di protezione dei dati

68%

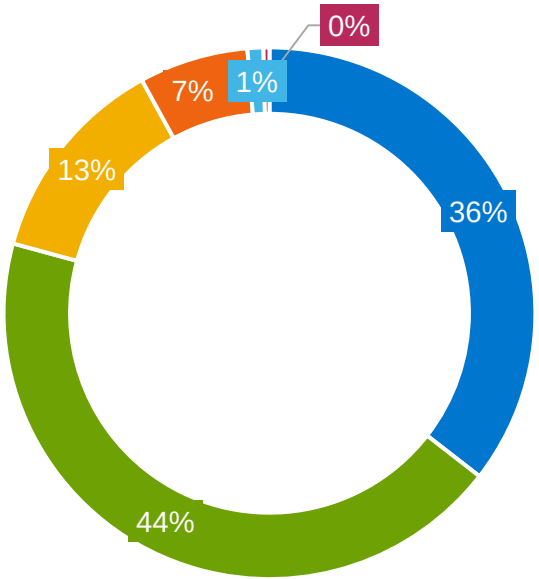
4. Vulnerabilità della protezione dei dati negli ambienti cloud

Le applicazioni vengono aggiornate e implementate in un'ampia gamma di ambienti nelle infrastrutture IT delle organizzazioni



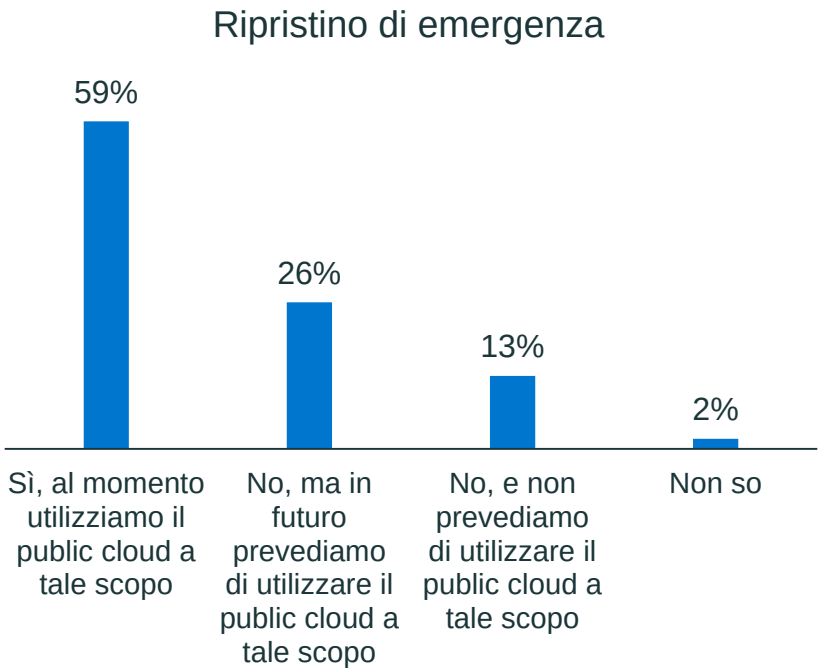


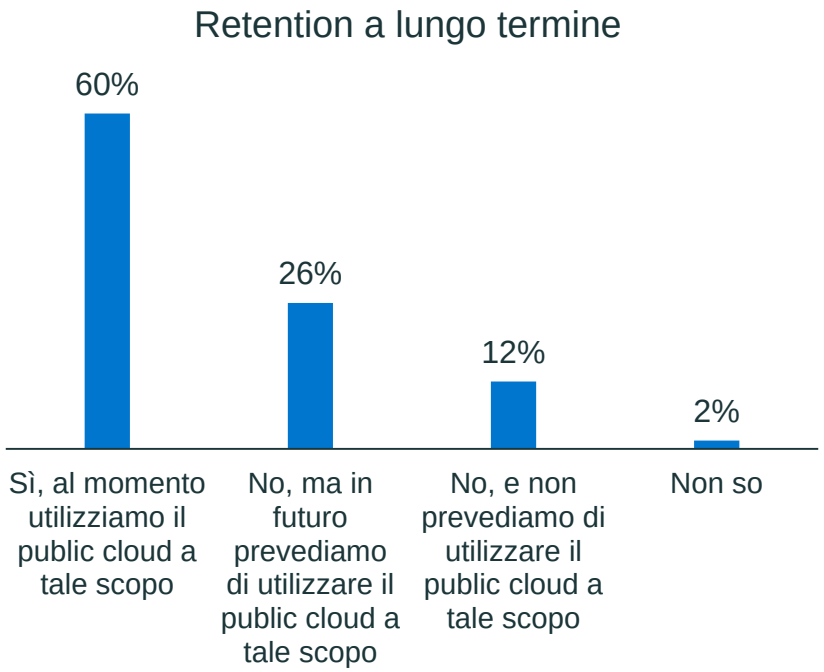
Tuttavia, molti non sono sicuri quando si tratta di proteggere i dati negli ambienti di public cloud



- Molto sicuro: proteggiamo tutti i nostri dati nel public cloud
- Moderatamente sicuro: proteggiamo tutti i nostri dati critici nel public cloud, ma non tutti i nostri dati
- Qualche dubbio: proteggiamo la maggior parte dei nostri dati critici nel public cloud
- Non molto sicuro: proteggiamo alcuni dei nostri dati critici nel public cloud
- Per niente sicuro: non proteggiamo i nostri dati nel public cloud
- Non so

Il public cloud ha un ruolo crescente nelle strategie di ripristino di emergenza e retention a lungo termine delle organizzazioni

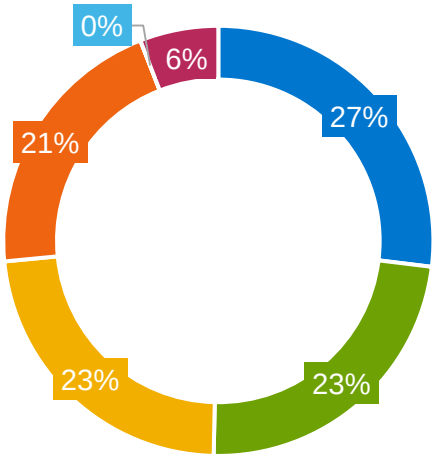




Molte organizzazioni che utilizzano più ambienti cloud non utilizzano soluzioni specifiche per proteggerli

Il 21%

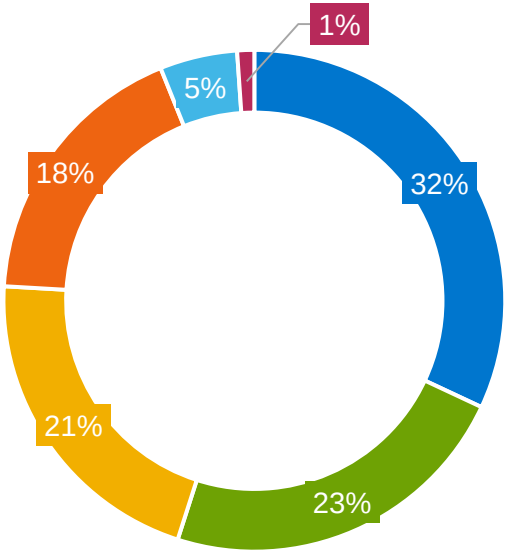
ritiene che quando si utilizzano più ambienti cloud, **ogni cloud service provider** sia responsabile della **protezione dei propri carichi di lavoro**



- Prevediamo di aggiornare la nostra soluzione di protezione dei dati in modo da consentire il backup dei carichi di lavoro su più cloud
- La nostra attuale soluzione di backup ci consente di proteggere i carichi di lavoro eseguiti in più cloud
- Utilizziamo più strumenti di backup per proteggere i carichi di lavoro eseguiti in più cloud
- Ogni cloud service provider è responsabile della protezione dei nostri carichi di lavoro
- Altro
- Non eseguiamo carichi di lavoro in più ambienti cloud

E lo stesso vale quando si considera la protezione dei carichi di lavoro virtualizzati utilizzando VMware nel cloud

- Prevediamo di aggiornare la nostra soluzione di protezione dei dati in modo da consentire il backup dei carichi di lavoro VMware su hybrid cloud
- Il nostro cloud service provider è responsabile della protezione dei nostri carichi di lavoro
- Con strumenti di backup che utilizziamo e gestiamo attualmente on-premise
- Con strumenti di backup disponibili nel marketplace del proprio cloud service provider
- Non stiamo eseguendo o pianificando l'esecuzione di carichi di lavoro virtualizzati utilizzando VMware nel cloud
- Non so

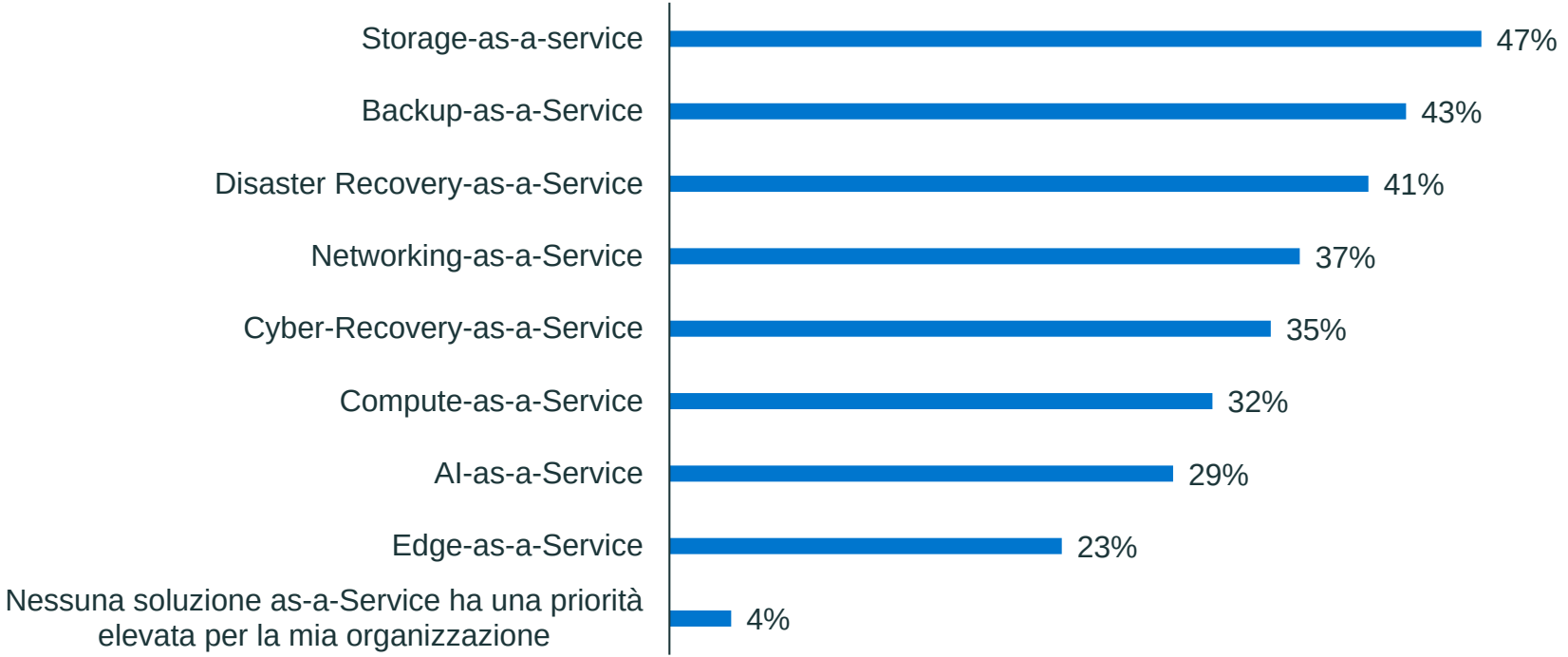


Il 23%

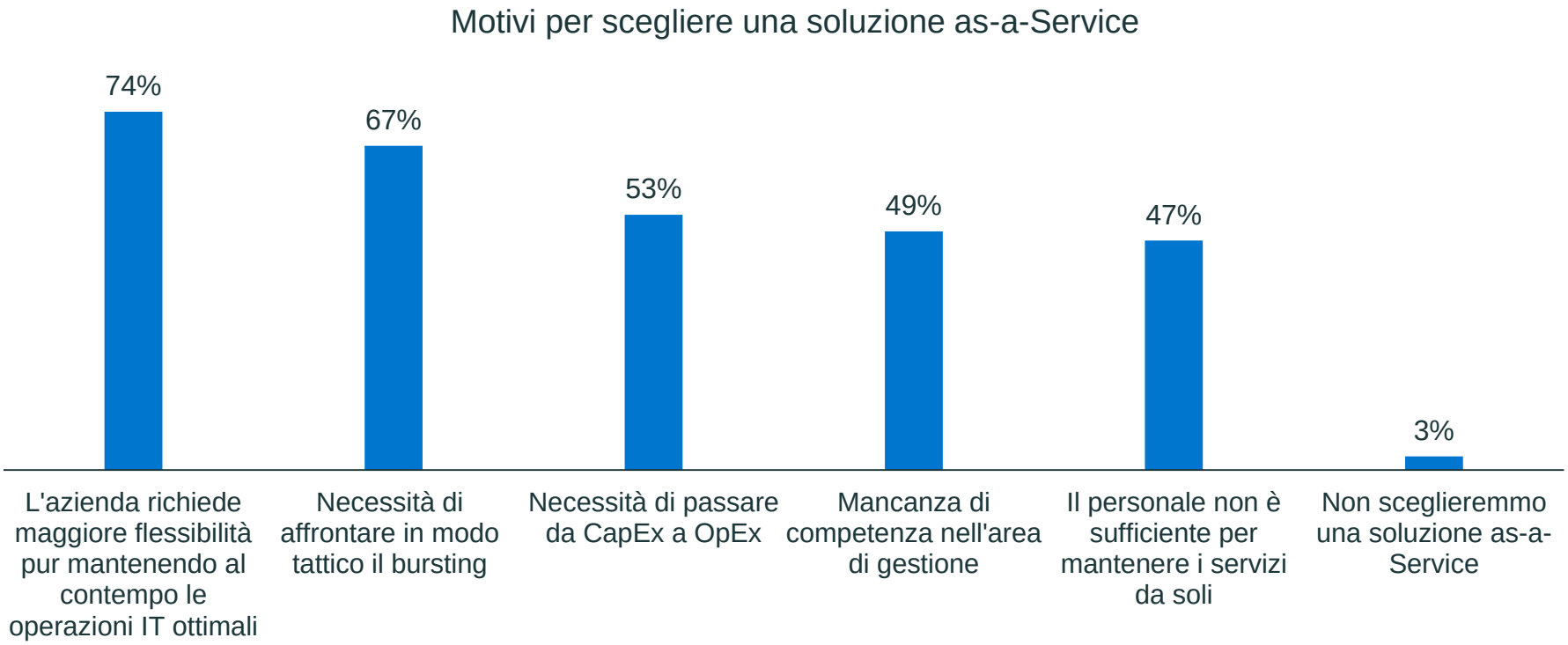
ritiene che il proprio **cloud service provider** sia responsabile della **protezione dei propri carichi di lavoro virtualizzati**

5.La crescita di as-a-Service

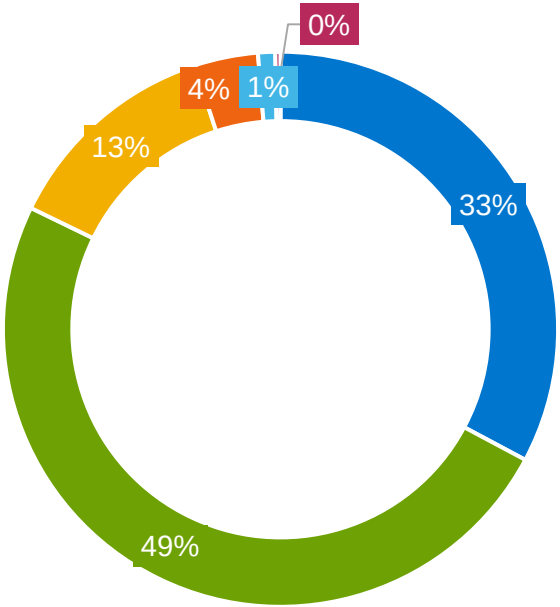
La maggior parte delle organizzazioni dà la priorità alle soluzioni as-a-Service, con Backup-as-a-Service e Disaster Recovery-as-a-Service tra le più comuni



La popolarità delle soluzioni as-a-Service spesso deriva dalla loro flessibilità



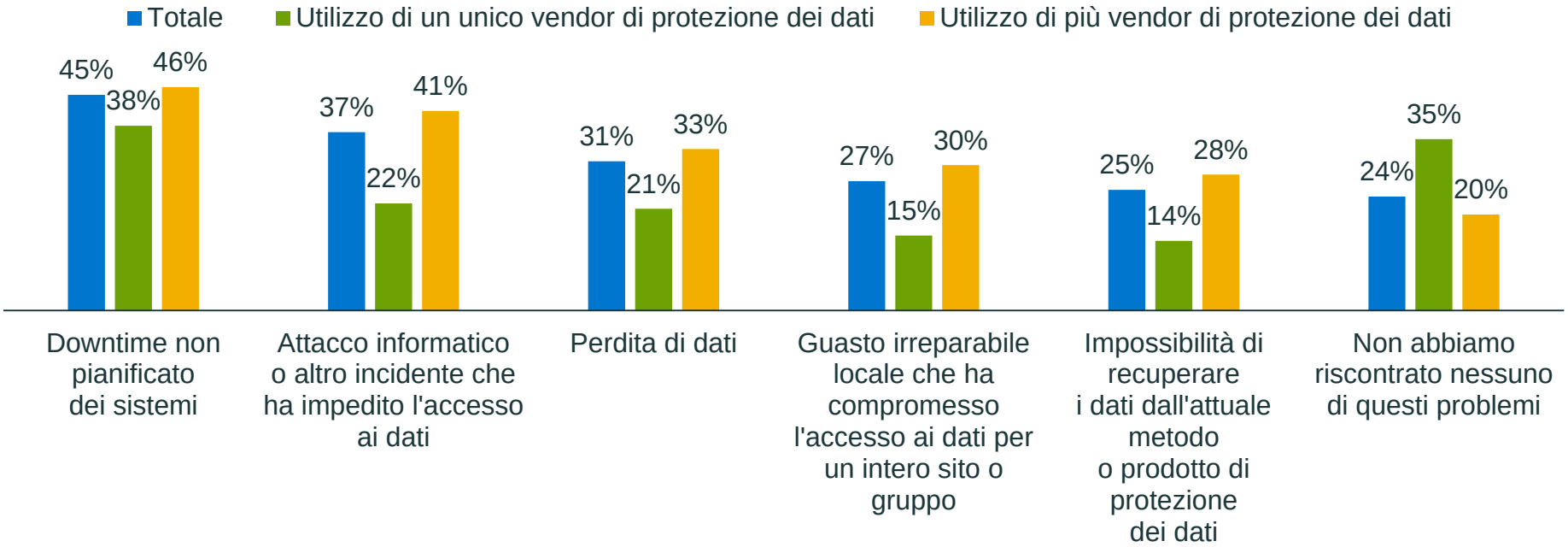
La stragrande maggioranza preferisce lavorare con un vendor che abbia più soluzioni as-a-Service, suggerendo il desiderio di consolidare i propri carichi di lavoro con un numero inferiore di vendor



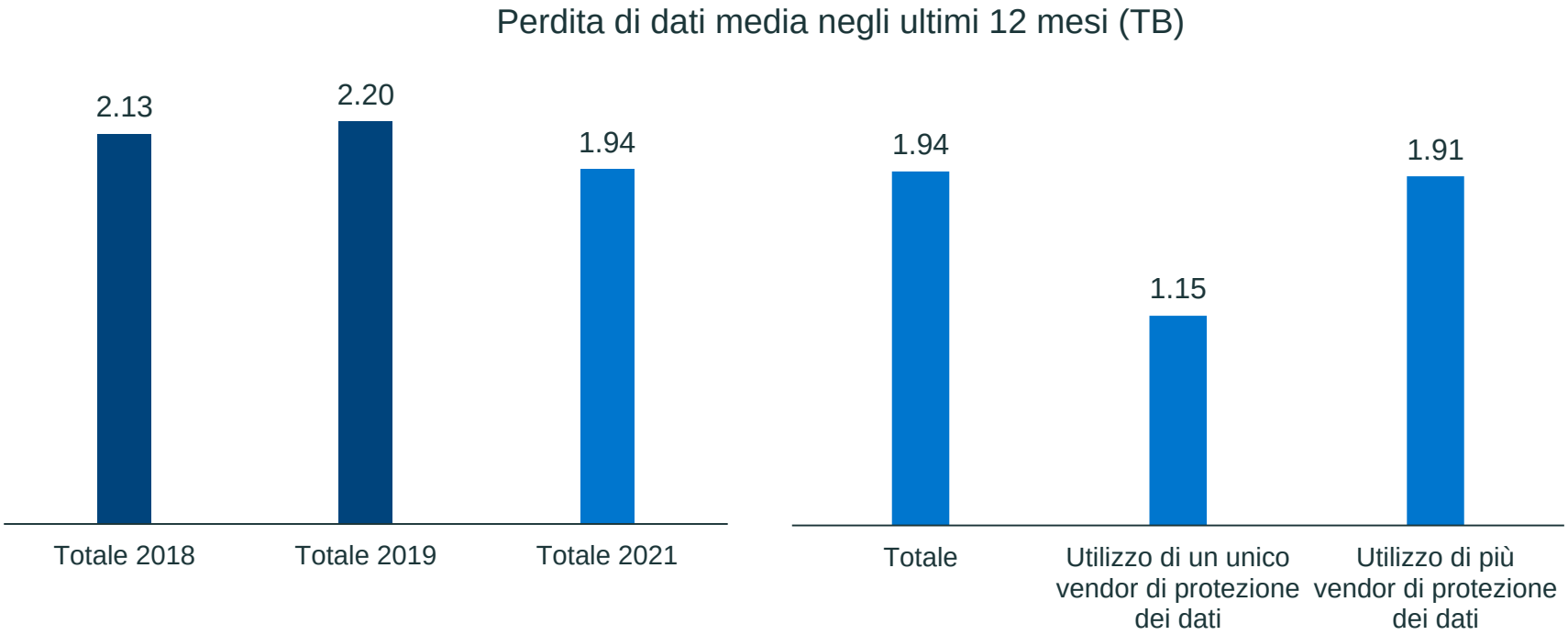
- Siamo molto più propensi a scegliere un vendor che abbia più soluzioni "as-a-Service"
- Siamo leggermente più propensi a scegliere un vendor che abbia più soluzioni "as-a-Service"
- Sono indifferente al fatto che un vendor abbia più servizi "as-a-Service"
- Siamo leggermente meno propensi a scegliere un vendor che abbia più soluzioni "as-a-Service"
- Siamo molto meno propensi a scegliere un vendor che abbia più soluzioni "as-a-Service"
- Non so

6. Semplifica la protezione dei dati

Le organizzazioni che utilizzano più vendor di protezione dei dati hanno maggiori probabilità di aver riscontrato molti problemi legati alla perdita di dati, all'accesso ai dati o ai downtime dei sistemi nell'ultimo anno rispetto a quelle che utilizzano un singolo vendor



E le organizzazioni che utilizzano più vendor di protezione dei dati perdono in media più dati rispetto a quelle che utilizzano un unico vendor



Risultati principali – in sintesi (1/2)

Il panorama del rischio della protezione dei dati

- Molti temono di non essere in grado di ripristinare tutti i sistemi/dati per soddisfare gli obiettivi di livello di servizio in caso di perdita di dati
- È diffuso il timore che le organizzazioni affronteranno un evento di interruzione nei prossimi dodici mesi e che gli effetti di questi eventi di interruzione potrebbero essere devastanti dal punto di vista finanziario
- Le organizzazioni devono intraprendere delle azioni per assicurarsi di essere preparate a rispondere a questi eventi, se si verificano

La minaccia degli attacchi informatici

- La preoccupazione è che le organizzazioni non siano in grado di proteggersi da minacce di malware e ransomware e molti concordano sul fatto che il rischio di attacchi informatici sia aumentato con l'aumento del lavoro da remoto
- Se le organizzazioni dovessero subire degli attacchi, solo alcuni sono sicuri che la loro organizzazione sarà in grado di ripristinare tutti i dati critici aziendali

Stare al passo con le tecnologie nuove ed emergenti

- Le organizzazioni stanno investendo in una gamma di tecnologie nuove ed emergenti, tra cui applicazioni SaaS, intelligenza artificiale/apprendimento automatico e dispositivi Edge/IoT, ma spesso fanno fatica a garantire che la loro protezione dei dati tenga il passo
- Molti ritengono che queste tecnologie rappresentino un rischio per la protezione dei dati e questi rischi potrebbero contribuire al timore che le organizzazioni non siano orientate al futuro e che siano a rischio di interruzioni nei prossimi dodici mesi
- Gli investimenti in tecnologie emergenti sono positivi e dovrebbero essere incentivati, ma le organizzazioni devono garantire che la loro infrastruttura di protezione dei dati supporti queste tecnologie

Risultati principali – in sintesi (2/2)

Vulnerabilità della protezione dei dati negli ambienti cloud

- Le applicazioni vengono aggiornate e implementate in un'ampia gamma di ambienti cloud, ma spesso manca la fiducia quando si tratta di proteggere bene i dati
- Il cloud svolge un ruolo importante nelle strategie di ripristino di emergenza e di retention a lungo termine
- Le organizzazioni devono assicurarsi di disporre di soluzioni specifiche per proteggere i dati in carichi di lavoro multi-cloud e virtualizzati, poiché alcune organizzazioni ritengono ancora che i propri provider di servizi cloud siano responsabili di questo

La crescita dell'as-a-Service

- Le soluzioni as-a-Service interessano la maggior parte delle organizzazioni e probabilmente faranno parte delle soluzioni di protezione dei dati di molte organizzazioni in futuro: la flessibilità è spesso un motivo fondamentale per questo interesse
- La maggior parte preferisce utilizzare soluzioni as-a-Service di vendor con più soluzioni, una scelta che potrebbe contribuire a semplificare la protezione dei dati per queste organizzazioni

Semplifica la protezione dei dati

- Le organizzazioni che utilizzano un unico vendor di protezione dei dati hanno meno probabilità di aver affrontato perdite di dati, problemi di accesso ai dati e incidenti di downtime dei sistemi non pianificati nell'ultimo anno rispetto a quelle che utilizzano più vendor
- Anche quelle che utilizzano un unico vendor hanno perso in media meno dati rispetto a quelle che utilizzano più soluzioni
- Mentre le organizzazioni potrebbero essere tentate di espandere le proprie capacità di protezione dei dati investendo in nuove soluzioni, consolidando le loro soluzioni con un unico vendor, sono più propense ad essere meglio protette dalla perdita di dati e i downtime

Ridurre il rischio e anticipare la concorrenza

Il punto di vista di Dell Technologies

Condurre regolarmente controlli sulla preparazione alla protezione dei dati

Considerare la cyber-resilienza una priorità assoluta

Consolidare le iniziative per la protezione dei dati con Dell

Per ulteriori informazioni, visita il sito https://www.delltechnologies.com/it-it/data-protection/gdpi/index.htm


DELL Technologies