Global Data Protection Index: edizione speciale 2024

Risultati principali: ottobre 2023

VansonBourne

DELL Technologies

Focus dei risultati principali

1
Il panorama del rischio della protezione dei dati

2
La crescente minaccia di attacchi informatici

3
L'utilizzo del multicloud

4
La protezione dell'ambiente cloud

Cinque considerazioni principali

Gli attacchi informatici continuano ad aumentare

Il costo degli attacchi informatici è in crescita

Le polizze assicurative non coprono abbastanza il costo degli attacchi

È possibile che il maggiore utilizzo dell'AI generativa determini dati dal valore ancora più elevato

Aumento dei rischi e dell'impatto finanziario degli attacchi informatici

Chi abbiamo intervistato?

1.500 responsabili delle decisioni IT e nell'ambito della sicurezza IT intervistati a settembre e ottobre 2023

Organizzazioni da un'ampia gamma di settori pubblici e privati

Organizzazioni con oltre 250 dipendenti

4 aree geografiche:

Americhe (300)
EMEA (675)
Asia-Pacifico e Giappone (375)
Cina (150)

1. Il panorama del rischio della protezione dei dati

Le preoccupazioni in merito alle misure di protezione dei dati sono diffuse e, data la mancanza di fiducia, le organizzazioni si trovano in una posizione vulnerabile

Il 60%

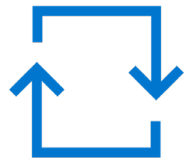
non è **molto sicuro** che la propria organizzazione **rispetti i Service Level Objectives (SLO) di backup e ripristino**

Il 79%

teme la possibilità di **affrontare un evento di interruzione** nei prossimi dodici mesi

Il 75%

teme che le misure di protezione dei dati adottate nella propria organizzazione **non siano sufficienti per fronteggiare le minacce malware e ransomware**

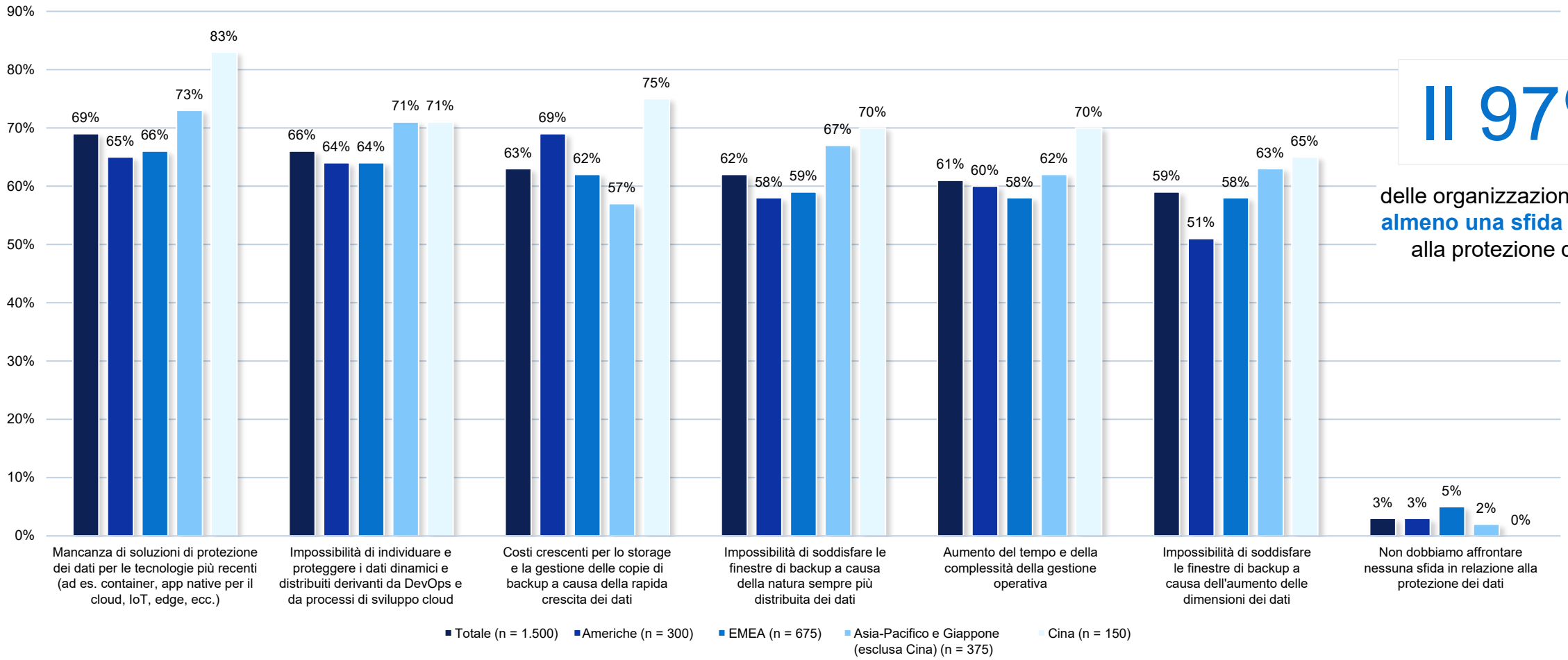


Il 65%

non è **molto sicuro** che la propria organizzazione abbia la possibilità di ripristinare completamente **i sistemi/i dati da tutte le piattaforme** in caso di incidente con perdita di dati

Oltre alle preoccupazioni sulla protezione dei dati, molte organizzazioni si trovano ad affrontare alcune sfide

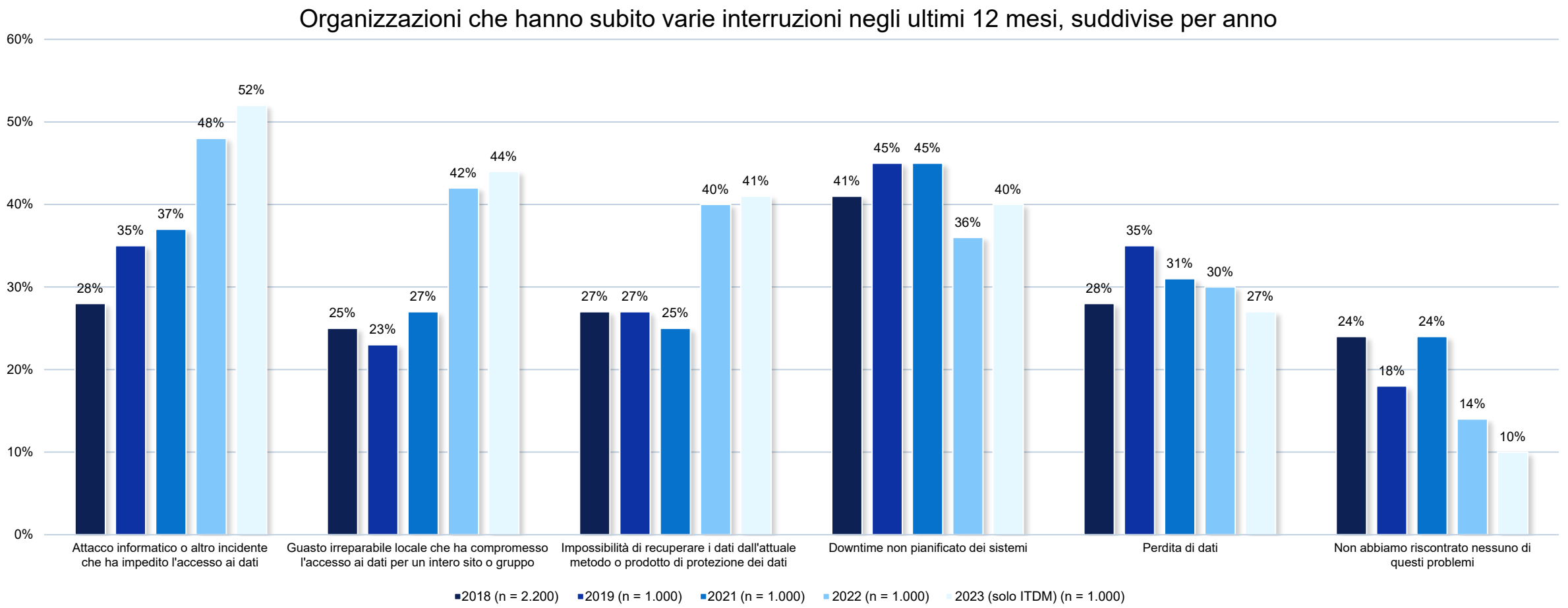
Le prime 5 sfide affrontate in relazione alla protezione dei dati, suddivise per area geografica



Il 97%

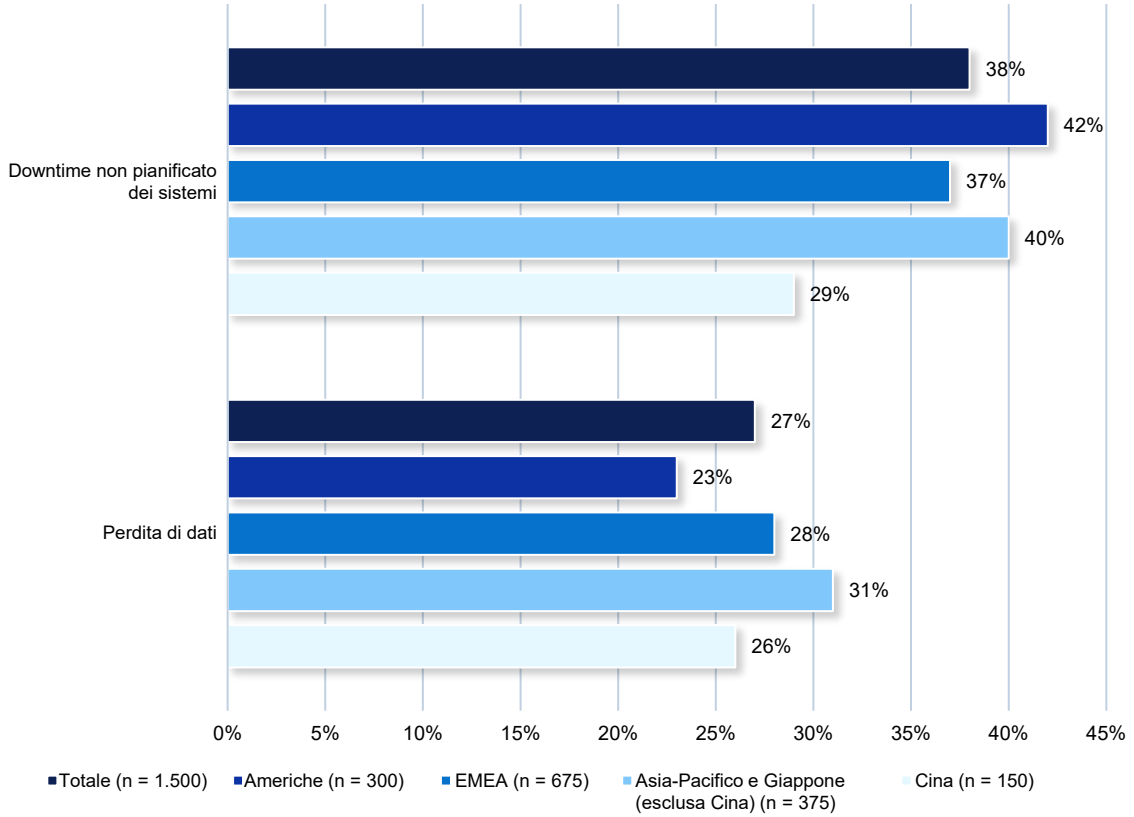
delle organizzazioni **affronta almeno una sfida** associata alla protezione dei dati

Negli ultimi 12 mesi le organizzazioni hanno affrontato notevoli interruzioni, con attacchi informatici che costituiscono una minaccia crescente e sempre presente



La perdita di dati non ha contribuito solo alle interruzioni, ma ha influenzato anche i risultati finali

Percentuale di organizzazioni che hanno riscontrato downtime non pianificato dei sistemi o perdita di dati negli ultimi 12 mesi, suddivisa per area geografica



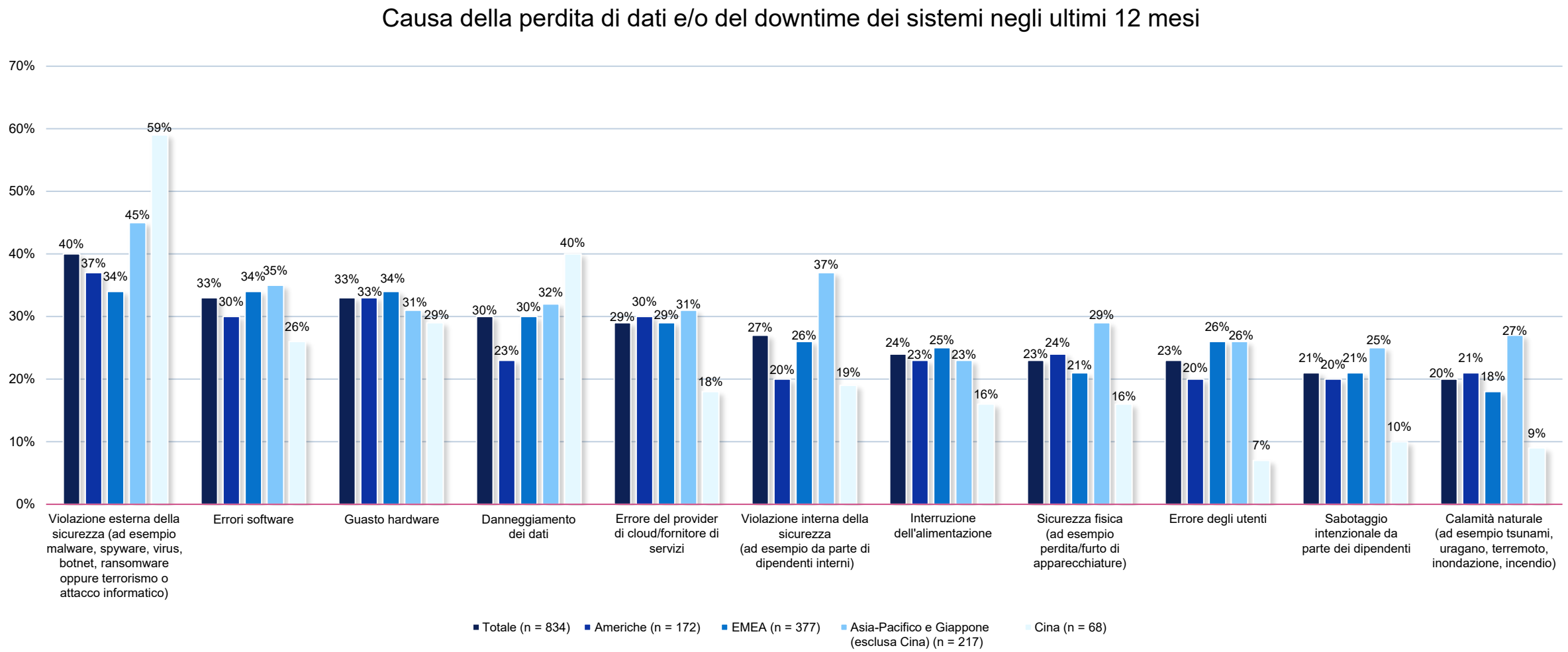
Negli ultimi 12 mesi:

26 ore — **di downtime non pianificato dei sistemi**, riscontrato in media

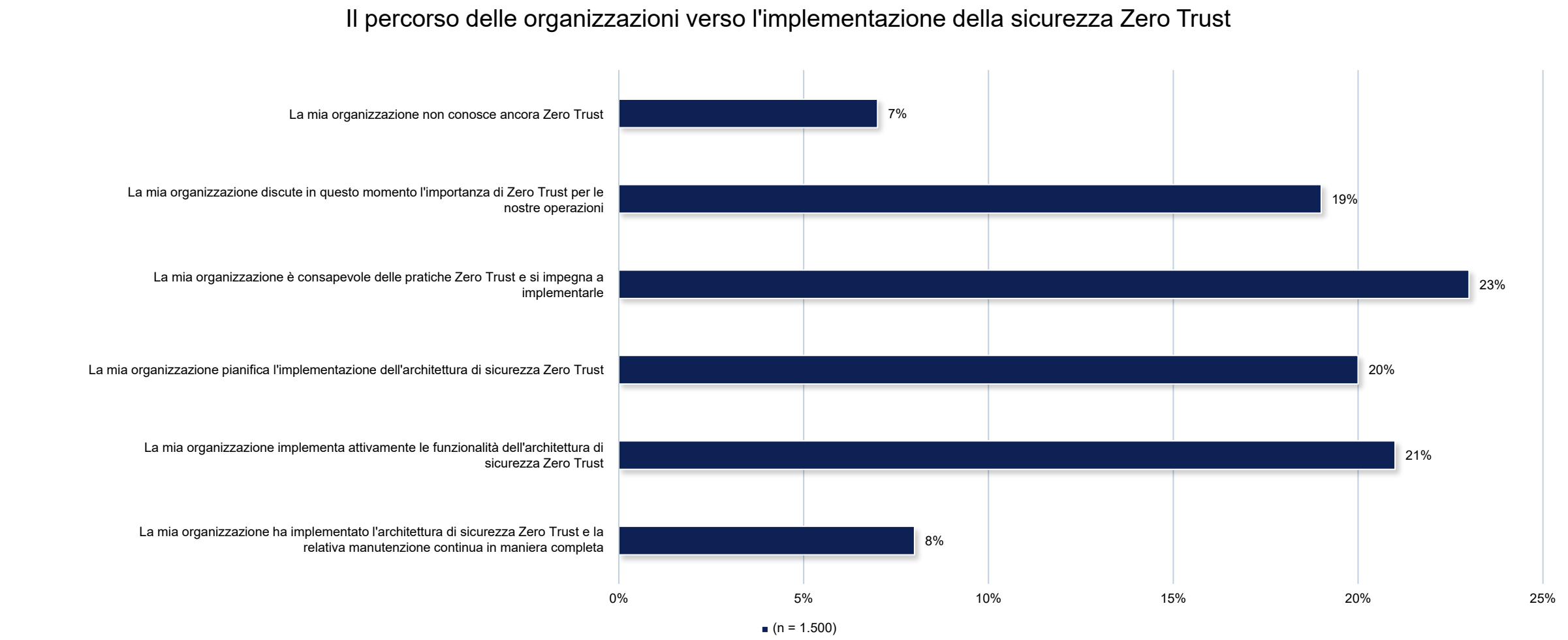
2,45 TB — **di dati** persi, in media

$ 2,61 — milioni, la media **dei costi della perdita dei dati**

Le minacce esterne alla sicurezza sono le cause più comuni di perdita di dati e/o downtime non pianificato dei sistemi negli ultimi 12 mesi



Nonostante le sfide e le preoccupazioni relative alla protezione dei dati, in pochi hanno implementato la sicurezza Zero Trust in maniera completa

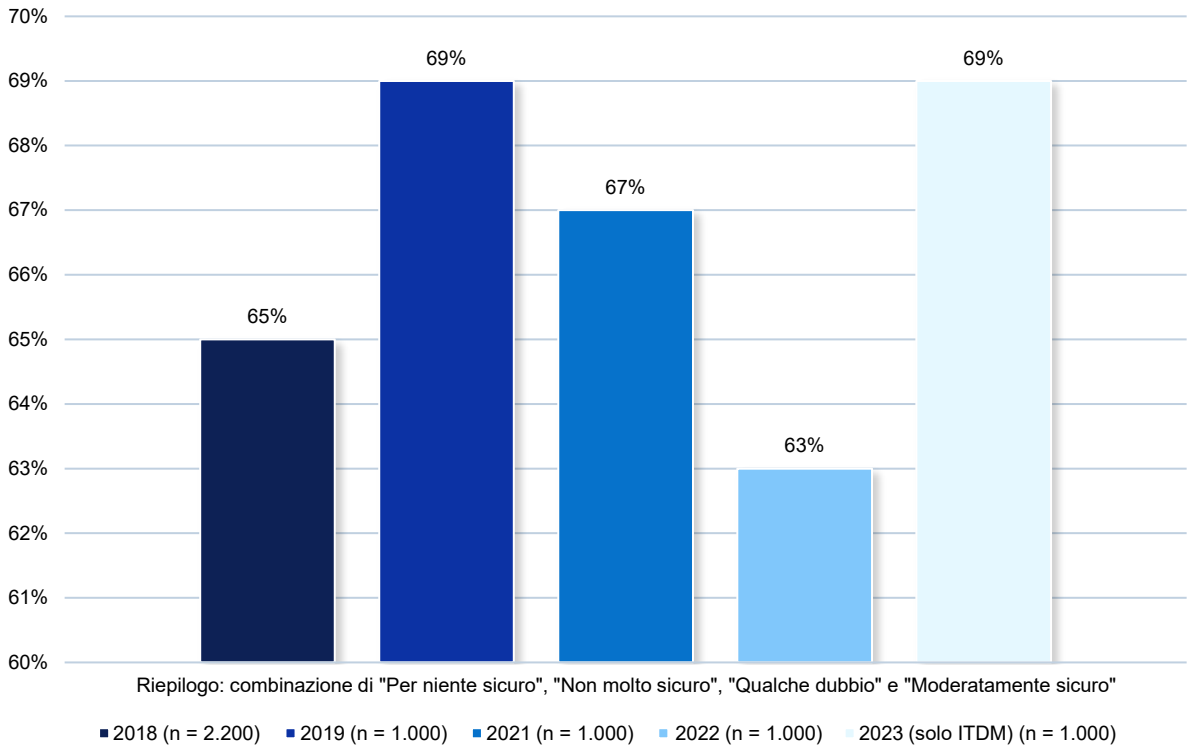


Filtro: dati Suddivisione: area geografica = Totale

2. La crescente minaccia di attacchi informatici

Le preoccupazioni in merito alle misure di protezione dei dati sono diffuse e, data la mancanza di fiducia, le organizzazioni si trovano in una posizione vulnerabile

Non "molto sicuro" della possibilità di ripristinare tutti i dati business-critical in caso di attacco informatico distruttivo, suddivisi per anno



L'81%

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

Il 74%

teme che i dati di backup siano **infetti o danneggiati da attacchi ransomware**

Ad aumentare il rischio, vi è l'eccessiva fiducia riguardante le conseguenze dell'attacco ransomware

Il 72%

concorda sul fatto che il proprio lavoro e i dipendenti all'interno dell'organizzazione **non saranno colpiti da un attacco ransomware**

Il 74%

concorda sul fatto che, se l'organizzazione subisce un attacco ransomware, **ottiene nuovamente tutti i dati** per riprendere l'attività **se paga il riscatto**

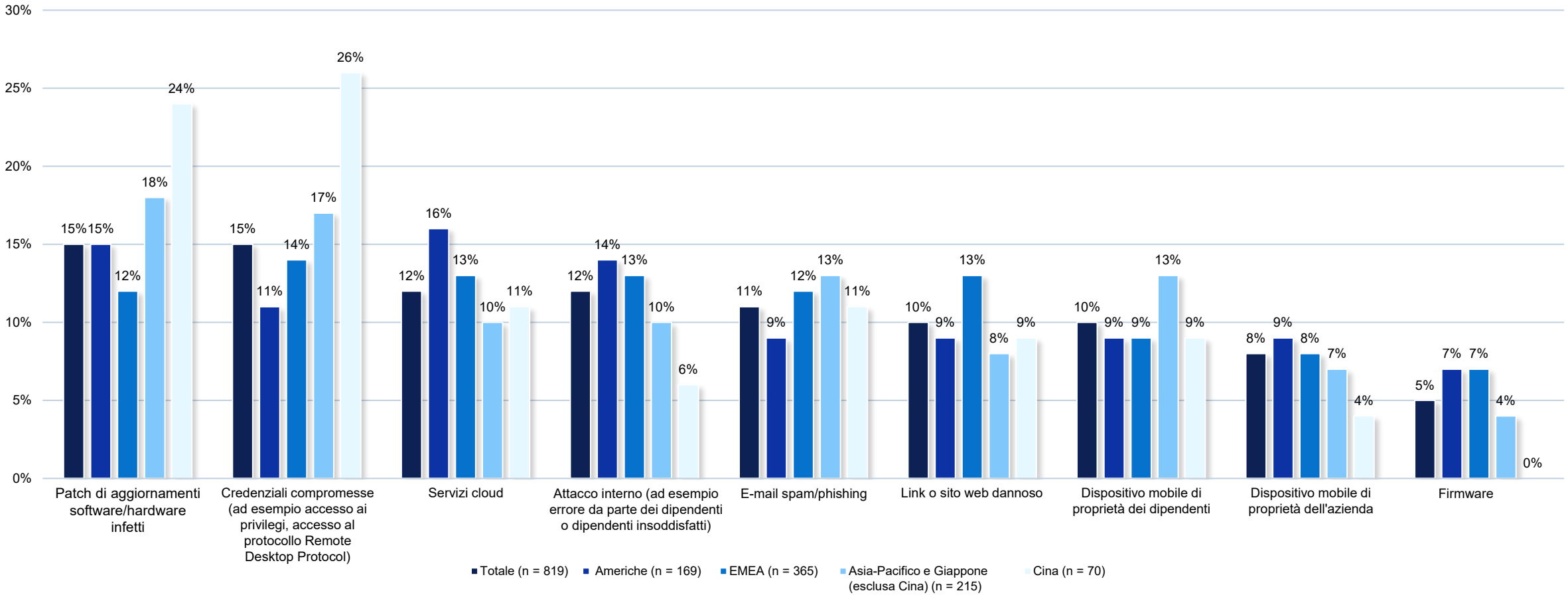
Il 66%

concorda sul fatto che, se l'organizzazione subisce un attacco ransomware, dopo aver pagato il riscatto **non ci saranno nuovi attacchi**

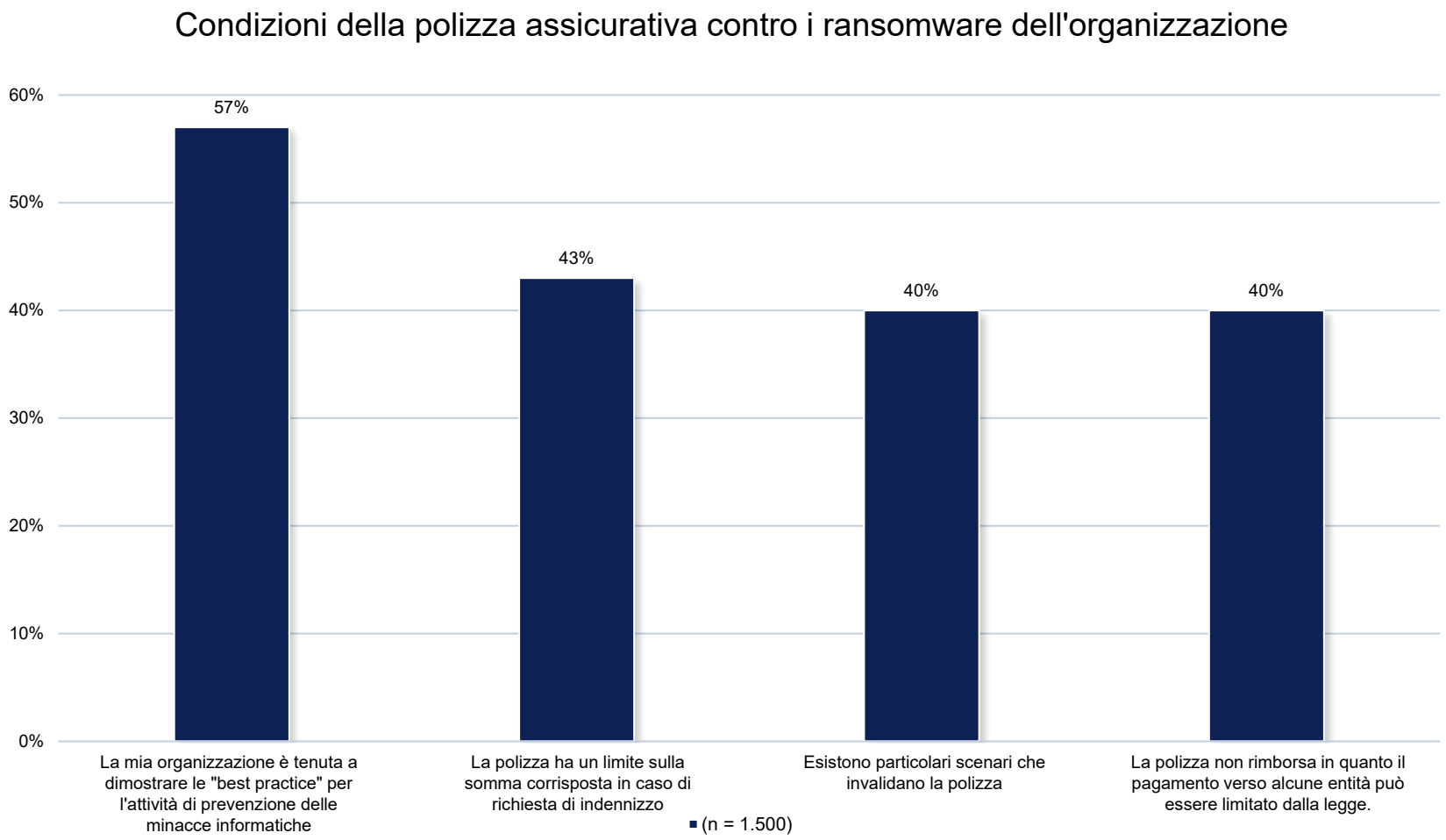
DELL Technologies

I criminali informatici colpiscono vari punti di ingresso, con maggiori probabilità di attacchi provenienti da fonti esterne

Punto di ingresso per il più recente attacco informatico dell'organizzazione, suddiviso per area geografica



Tra le organizzazioni, le polizze assicurative contro i ransomware sono la normalità, ma hanno forti avvertenze

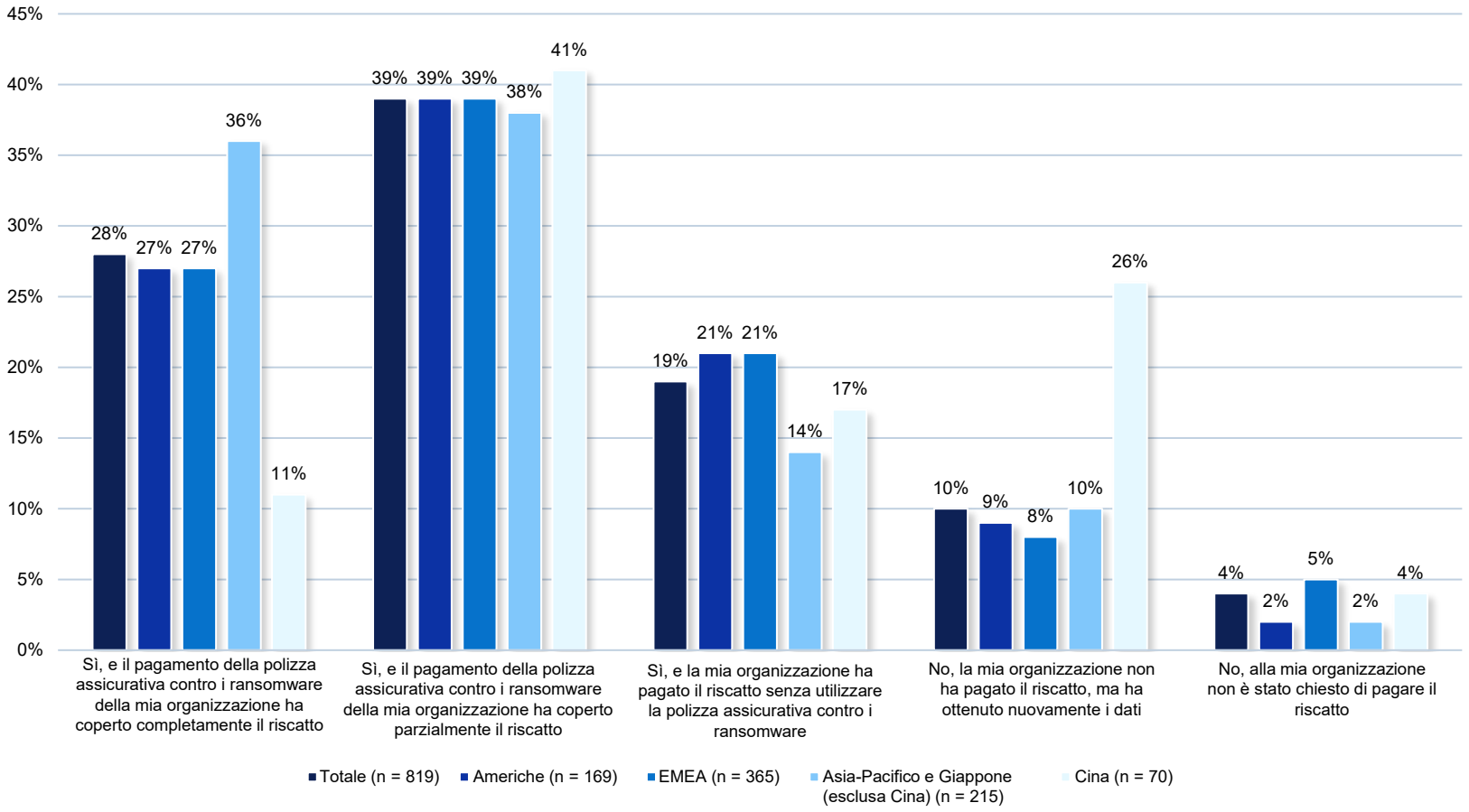


Il 93%

delle organizzazioni **ha una polizza contro i ransomware**

Nonostante molti siano provvisti di polizze contro i ransomware, le organizzazioni sono ancora vulnerabili dal punto di vista finanziario

Pagamento del riscatto per accedere ai dati dell'organizzazione, suddiviso per area geografica

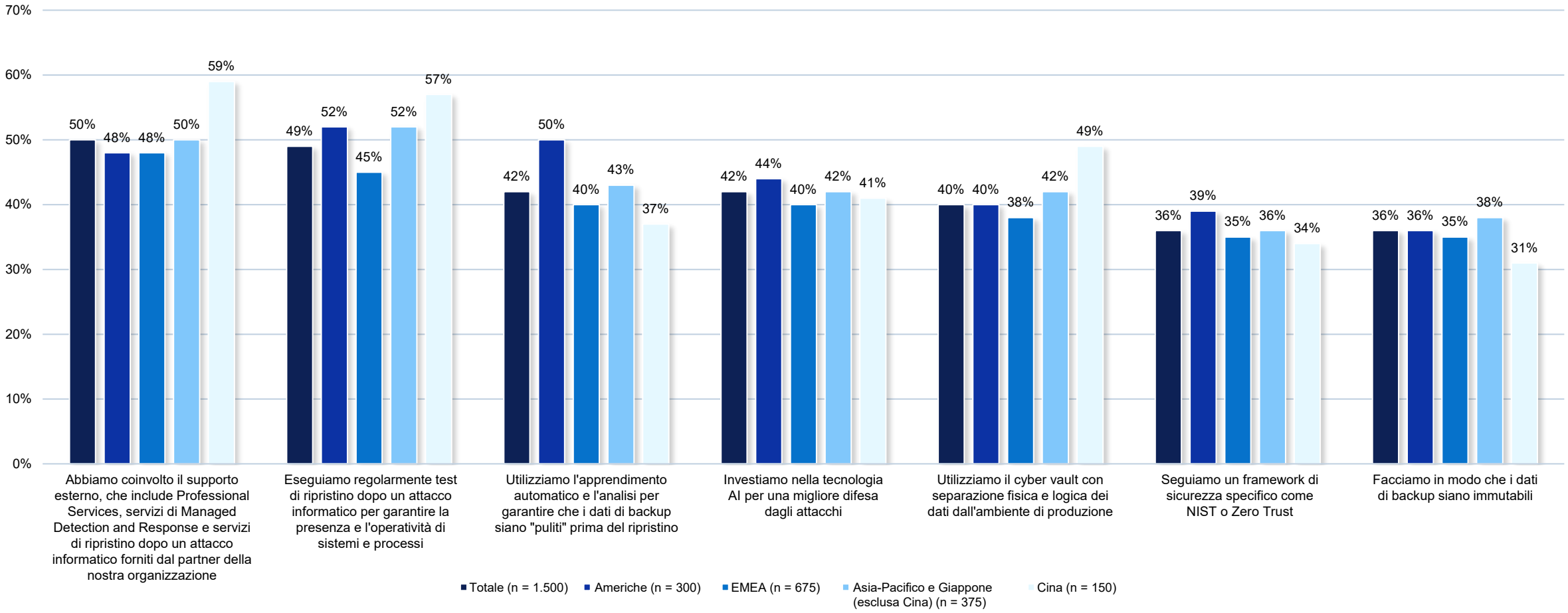


$ 1,92

milioni è stato il costo medio per le organizzazioni negli ultimi 12 mesi, causato da **attacchi informatici e altri incidenti** correlati

In modo incoraggiante, le organizzazioni adottano misure per diventare più resilienti alle minacce informatiche

Provvedimenti intrapresi dalle organizzazioni per migliorare la cyber-resilienza, suddivisi per area geografica

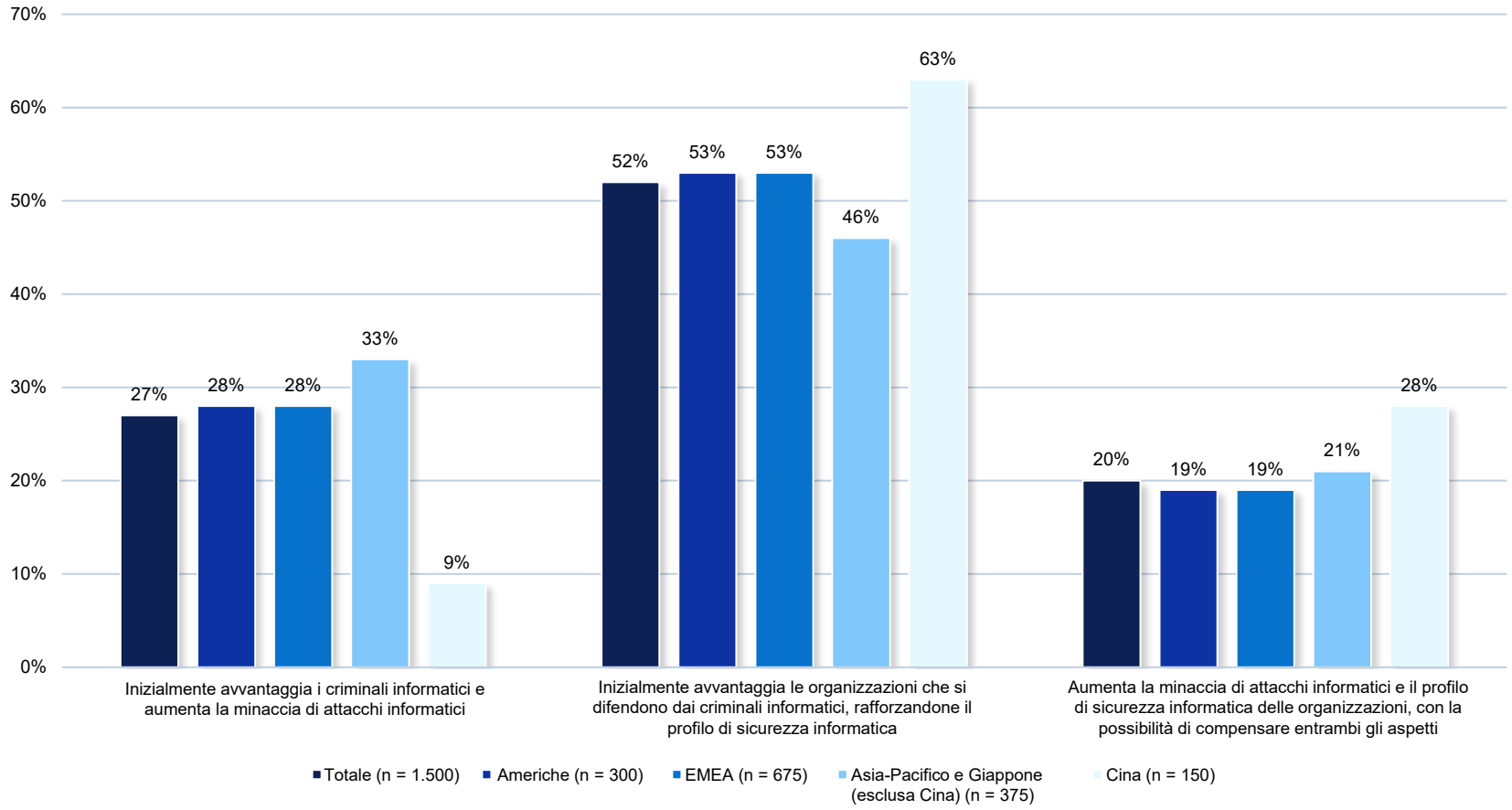


Tuttavia, non tutti ritengono che l'AI generativa sia un vantaggio per la cyber-resilienza

L'81%

concorda sul fatto che le tecnologie emergenti (come AI, IoT, edge) **rappresentano un rischio per la protezione dei dati**

Impatto dell'AI generativa sulle minacce informatiche e sulla sicurezza dei dati, suddiviso per area geografica



In effetti, vista la preoccupazione delle organizzazioni in merito alla protezione dei dati, molti ritengono che l'AI generativa crei nuove sfide

L'88%

concorda sul fatto che l'AI generativa crea grandi volumi di nuovi dati da **proteggere**

L'88%

concorda sul fatto che l'AI generativa aumenta il valore di alcuni tipi di dati che richiedono **livelli di servizi di protezione dei dati più elevati**

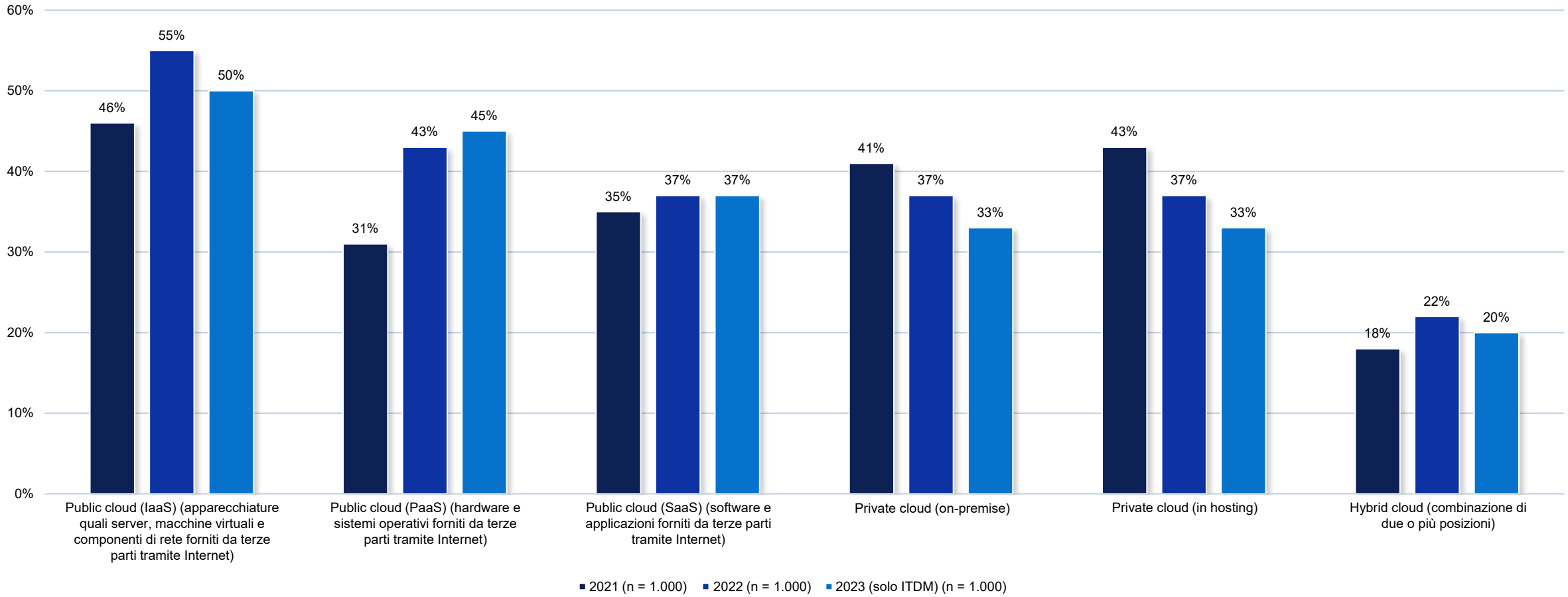
L'85%

concorda sul fatto che, se i data set utilizzati per l'AI generativa sono **danneggiati**, questo influisce **sull'output dell'AI generativa**

3. L'utilizzo del multicloud

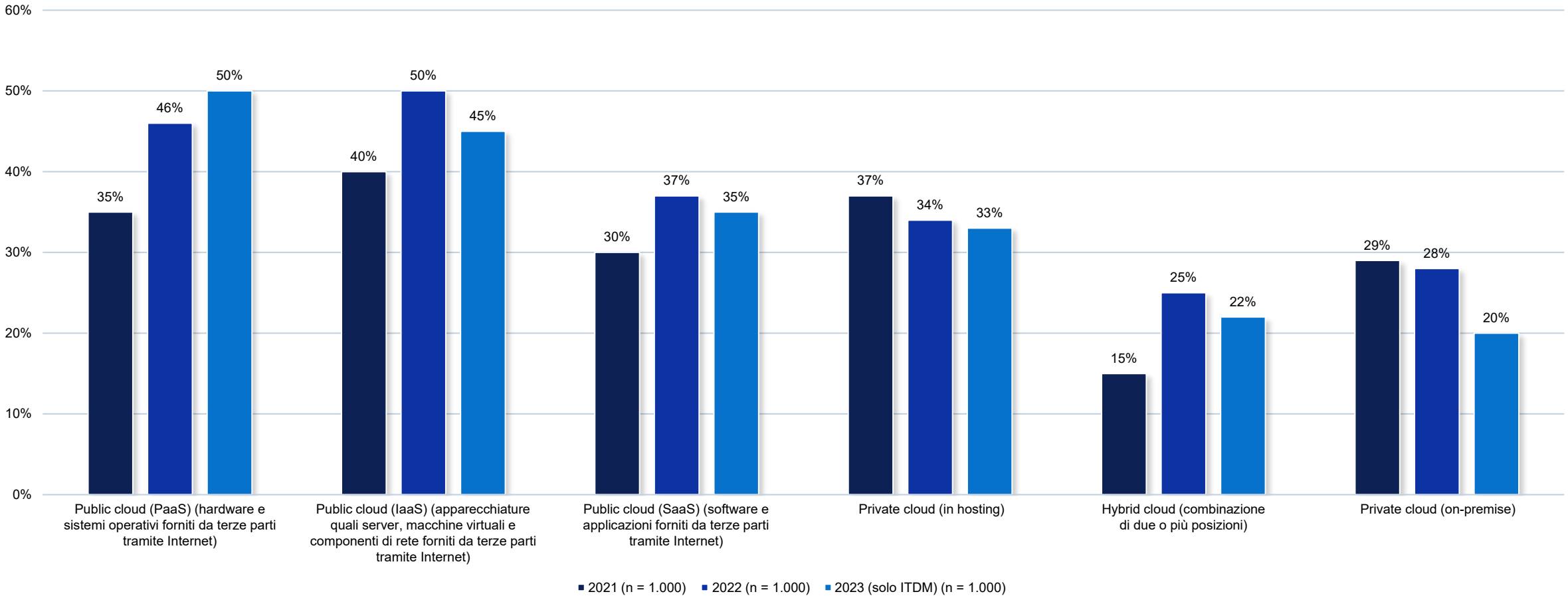
Il public cloud resta la scelta diffusa nell'aggiornamento delle applicazioni esistenti, mentre la preferenza per il private cloud è in diminuzione

Indicazioni da intraprendere nell'aggiornamento delle applicazioni esistenti, suddivise per anno

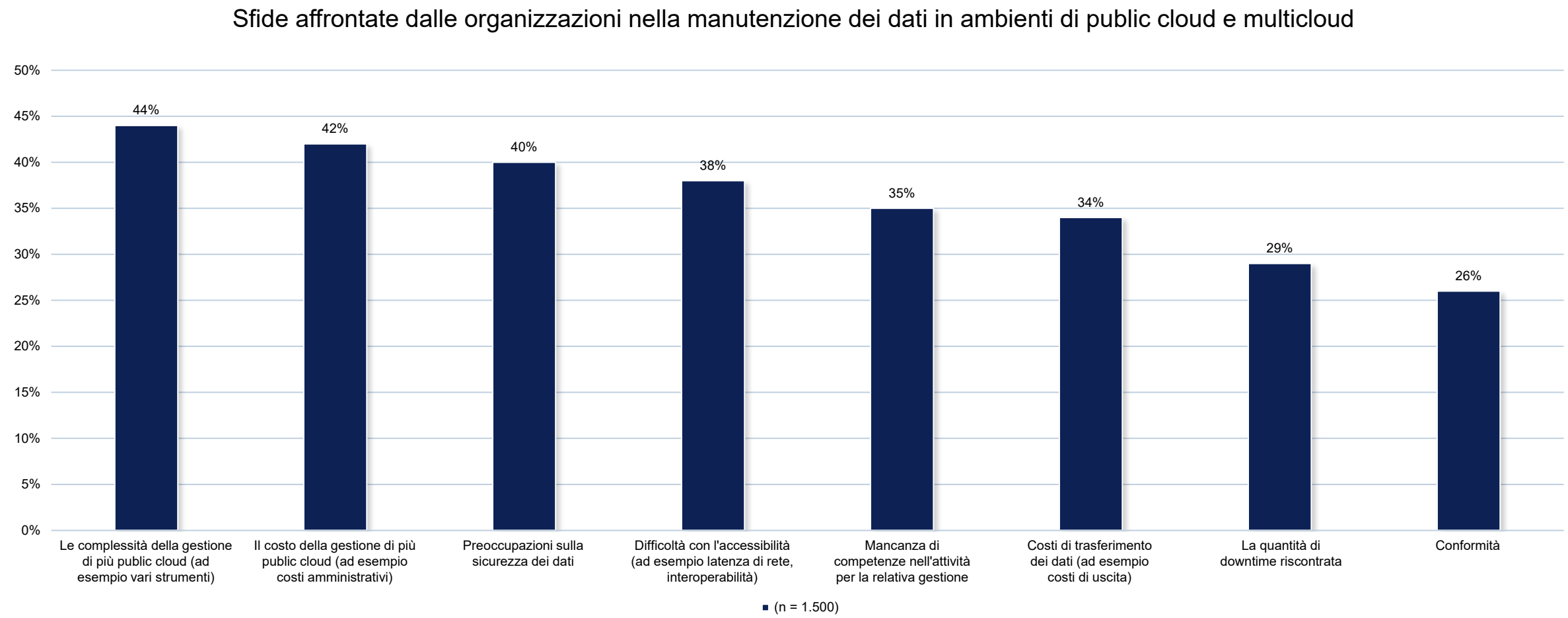


Anche il public cloud resta la scelta diffusa per il deployment di nuove applicazioni, ma il supporto è in calo

Indicazioni da intraprendere nel deployment di nuove applicazioni, suddivise per anno



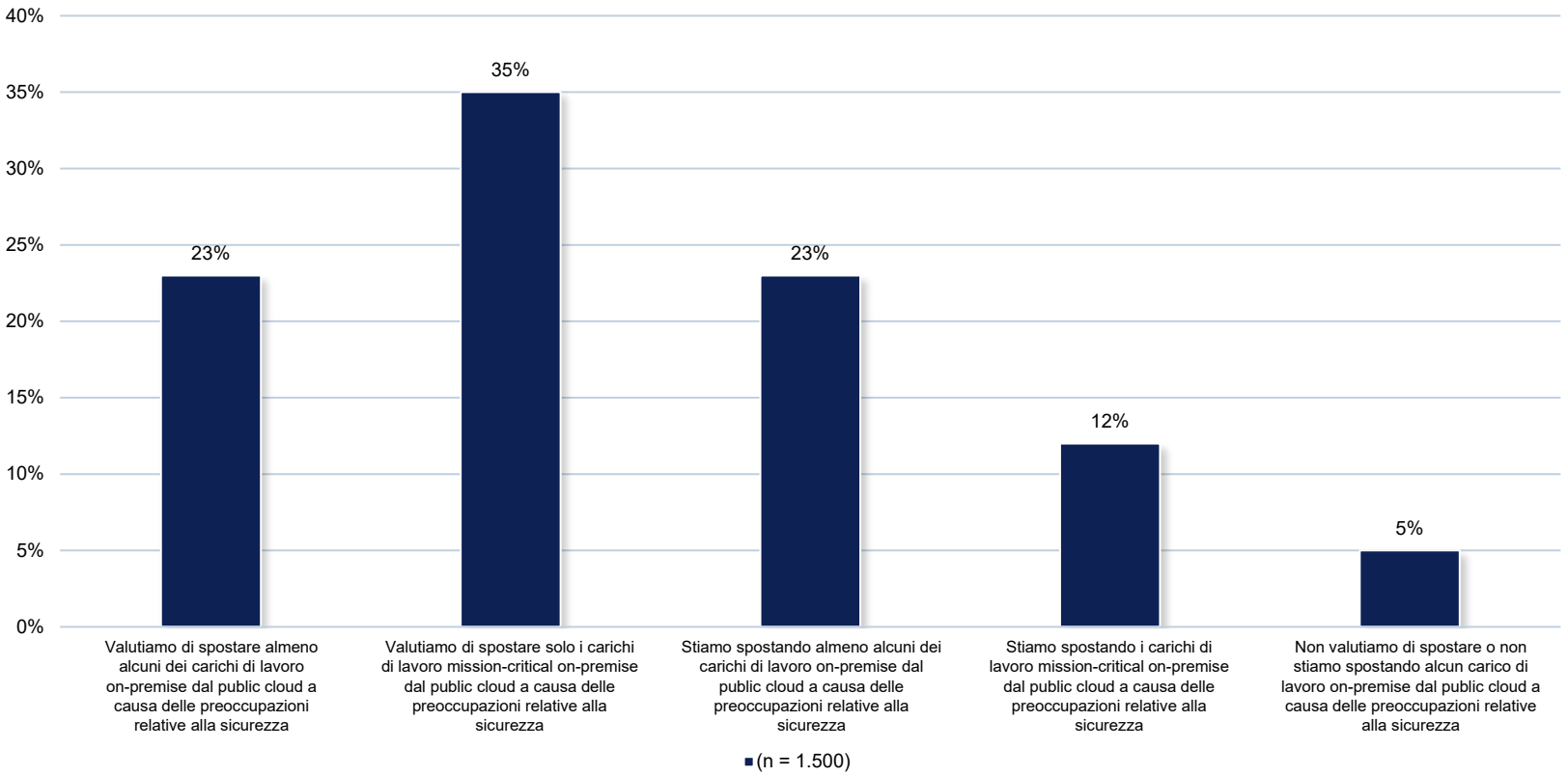
Nonostante la diffusione del public cloud, molte organizzazioni affrontano alcune sfide durante la manutenzione dei dati



Filtro: dati Suddivisione: area geografica = Totale

A causa delle preoccupazioni sulla sicurezza, molte organizzazioni stanno spostando, o valutano di spostare, parte dei propri carichi di lavoro on-premise dai public cloud

Misura in cui le organizzazioni spostano i carichi di lavoro on-premise dal public cloud



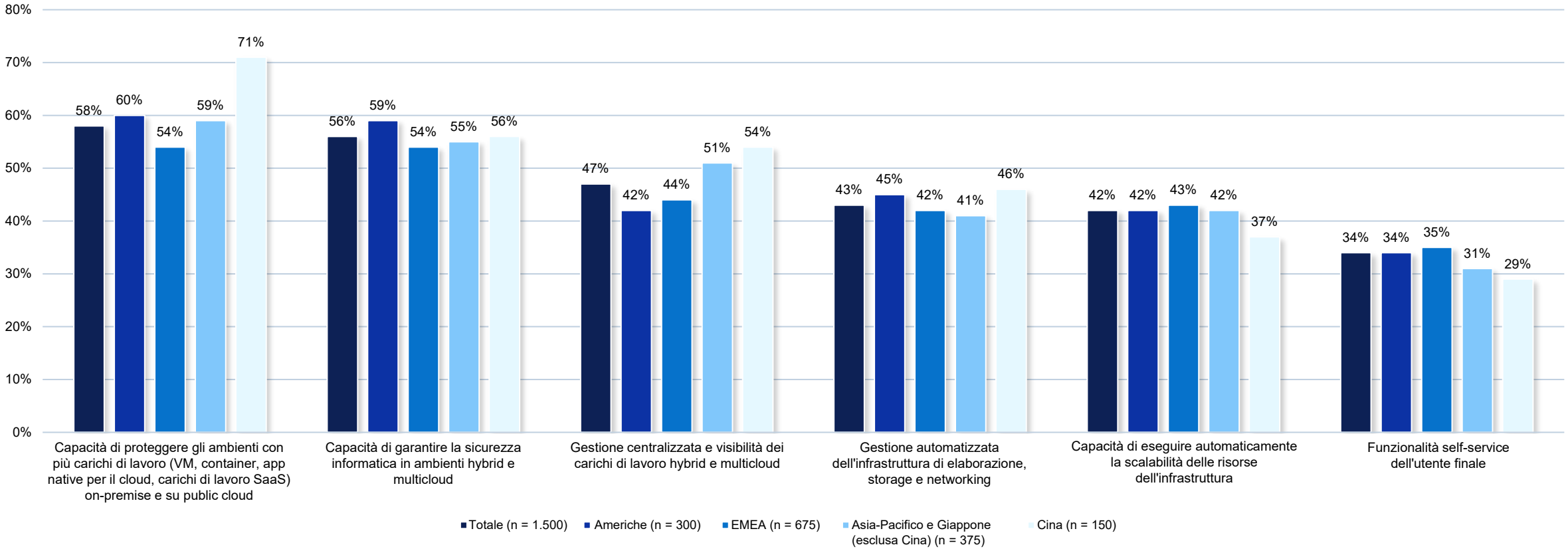
Filtro: dati Suddivisione: area geografica = Totale

Il 79%

non è **molto sicuro** che la propria organizzazione abbia la possibilità di **proteggere tutti i dati** in ambienti public cloud

A causa dell'aumento degli incidenti correlati agli attacchi informatici e della scarsa fiducia nelle strategie di protezione dei dati, molti considerano la sicurezza come la funzionalità più importante quando si tratta di abilitare le operazioni hybrid e multicloud

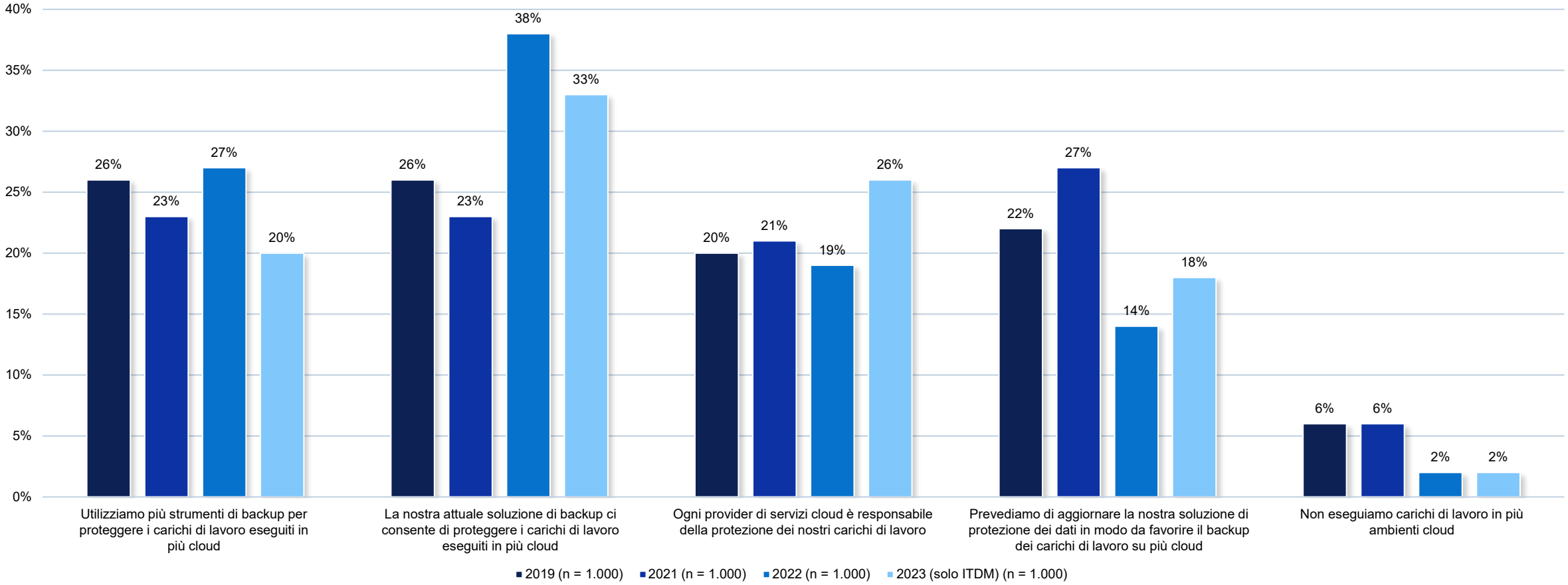
Funzionalità più importanti per l'abilitazione di operazioni hybrid e multicloud, suddivise per area geografica



4. La protezione dell'ambiente cloud

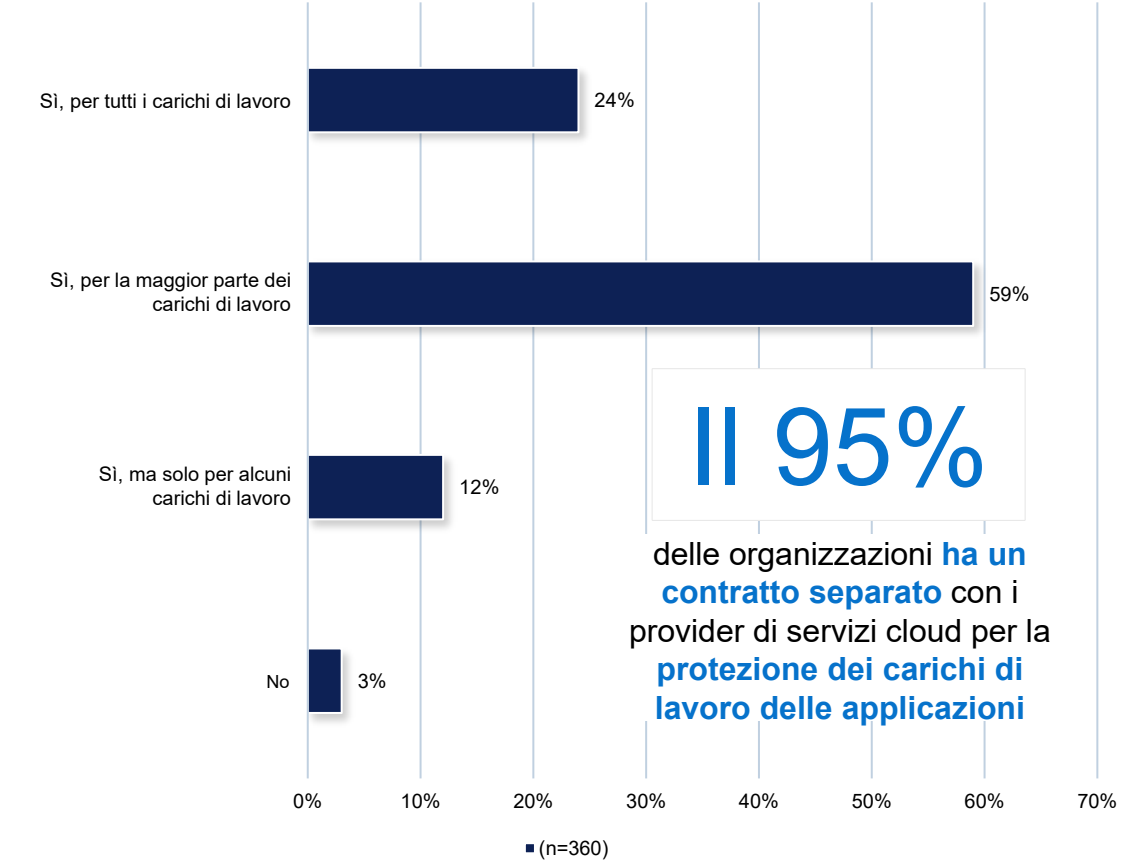
Attualmente, le organizzazioni utilizzano vari strumenti e soluzioni di backup per proteggere i carichi di lavoro, ma sono necessari alcuni upgrade

Soluzioni e strumenti per la protezione cloud, suddivisi per anno



Le organizzazioni si affidano sempre più ai provider di servizi cloud per proteggere i carichi di lavoro negli ambienti cloud

Contratto separato con il CSP per la protezione dei carichi di lavoro delle applicazioni

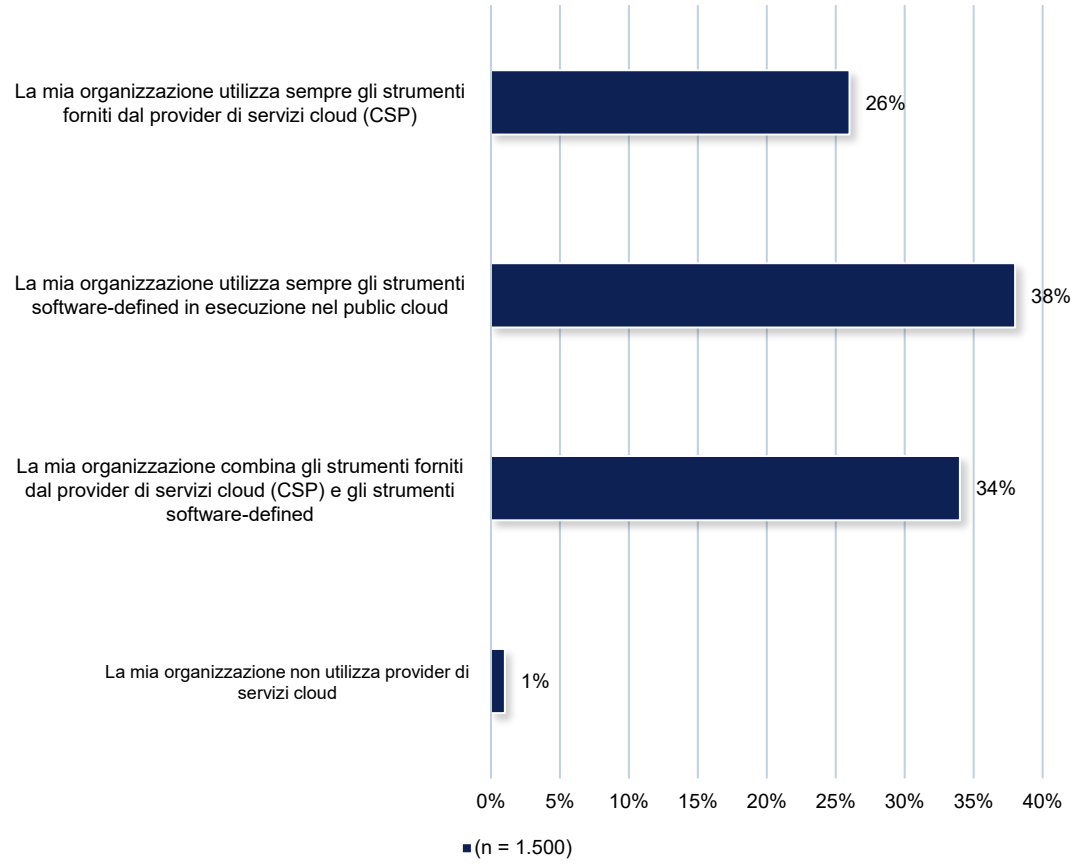


Il 95%

delle organizzazioni **ha un contratto separato** con i provider di servizi cloud per la **protezione dei carichi di lavoro delle applicazioni**

Filtro: dati Suddivisione: area geografica = Totale

Strumenti di backup e ripristino forniti dal provider di servizi cloud



Filtro: dati Suddivisione: area geografica = Totale

Risultati principali in sintesi

Il panorama del rischio della protezione dei dati

- Le preoccupazioni in merito alle misure di protezione dei dati sono diffuse e, data la mancanza di fiducia, le organizzazioni si trovano in una posizione vulnerabile
- Quasi tutte le organizzazioni affrontano sfide relative alla protezione dei dati, molte delle quali hanno subito anche interruzioni significative negli ultimi 12 mesi a causa della perdita di dati e/o del downtime non pianificato del sistema
- Le minacce esterne alla sicurezza sono state le cause più comuni di perdita di dati e/o downtime non pianificato dei sistemi negli ultimi 12 mesi
- Nonostante le sfide e le preoccupazioni relative alla protezione dei dati, in pochi hanno implementato la sicurezza Zero Trust in maniera completa

La minaccia crescente degli attacchi informatici

- Negli ultimi 12 mesi si è verificato un aumento delle organizzazioni che hanno subito attacchi o incidenti informatici, costati alle aziende in media $ 1,92 milioni
- Molte organizzazioni temono la possibilità che le copie dei dati di backup siano infette o danneggiate dagli attacchi ransomware
- Ad aumentare il rischio, vi è l'eccessiva fiducia riguardante le conseguenze dell'attacco ransomware
- Nonostante la diffusione delle polizze assicurative contro i ransomware, queste hanno forti avvertenze, il che rende le organizzazioni vulnerabili dal punto di vista finanziario

L'utilizzo del multicloud

- Il public cloud resta la scelta diffusa nell'aggiornamento delle applicazioni esistenti e nel deployment di nuove applicazioni, ma vi sono preoccupazioni in merito alla sicurezza dei dati
- A causa delle preoccupazioni sulla sicurezza, molte organizzazioni stanno spostando, o valutano di spostare, parte dei propri carichi di lavoro on-premise dai public cloud
- A causa dell'aumento degli incidenti correlati agli attacchi informatici e della scarsa fiducia nelle strategie di protezione dei dati, molti considerano la sicurezza come la funzionalità più importante quando si tratta di abilitare le operazioni hybrid e multicloud

La protezione dell'ambiente cloud

- Attualmente, le organizzazioni utilizzano vari strumenti e soluzioni di backup per proteggere i carichi di lavoro, ma riconoscono la necessità degli upgrade
- Le organizzazioni si affidano sempre più ai provider di servizi cloud per proteggere i carichi di lavoro negli ambienti cloud