

2025

Rapporto sullo stato della sicurezza del cloud

Approfondimenti e strategie chiave per la protezione degli ambienti cloud



FORTINET®

Introduzione

L'adozione del cloud continua a trasformare l'infrastruttura IT e il panorama della sicurezza, offrendo una scalabilità e una flessibilità senza pari. Le strategie multi-cloud rafforzano ulteriormente questi vantaggi, ma introducono sfide uniche, spingendo le organizzazioni a implementare soluzioni innovative per salvaguardare efficacemente le proprie risorse critiche.

Il Rapporto sullo stato della sicurezza del cloud 2025, basato sulle opinioni di 873 professionisti della sicurezza informatica, fornisce un'analisi approfondita dell'evoluzione del panorama della sicurezza del cloud, evidenziando le tendenze, le sfide e le priorità principali per le organizzazioni che si trovano a navigare in ambienti sempre più complessi. Questo report funge da guida per i professionisti dell'IT e della sicurezza che cercano di rafforzare il loro approccio alla sicurezza ibrida e multi-cloud continuando a innovare.

I risultati principali di questo rapporto includono:

- **Strategie ibride e multi-cloud in crescita:** oltre il 78% degli intervistati utilizza due o più provider di servizi cloud, sottolineando la crescente importanza degli approcci multi-cloud per migliorare la resilienza e sfruttare le capacità specialistiche. Il 54% delle organizzazioni ha adottato modelli di cloud ibrido, integrando ambienti on-premise e di cloud pubblico per ottimizzare flessibilità e controllo.
- **Sicurezza e conformità sono i principali timori:** i problemi di sicurezza e conformità sono i principali ostacoli all'adozione del cloud, citati dal 61% delle organizzazioni che cercano di soddisfare i requisiti normativi e proteggere i dati sensibili.
- **Divario di competenze nella sicurezza del cloud:** il 76% delle organizzazioni segnala una carenza di competenze nella sicurezza del cloud, evidenziando la necessità di automazione, aggiornamento mirato e ottimizzazione delle risorse.
- **Scarsa fiducia nel rilevamento delle minacce in tempo reale:** i dati del sondaggio evidenziano che il 64% degli intervistati non ha fiducia nella capacità della propria organizzazione di gestire il rilevamento delle minacce in tempo reale.
- **Piattaforme unificate per la sicurezza del cloud:** il sondaggio mostra che il 97% degli intervistati preferisce piattaforme di sicurezza del cloud unificate con dashboard centralizzate per semplificare la configurazione delle policy, garantire la coerenza e migliorare la visibilità su tutta l'impronta cloud dell'organizzazione.
- **Rapida adozione della gestione dell'approccio alla sicurezza del cloud (CSPM, Cloud Security Posture Management) e delle piattaforme di protezione delle applicazioni cloud-native (CNAPP, Cloud-Native Application Protection Platform):** per risolvere le configurazioni errate e le lacune di conformità, il 67% degli intervistati sta implementando l'approccio CSPM e il 62% soluzioni CNAPP per proteggere gli ambienti cloud.



Questo rapporto sottolinea l'importanza di soluzioni di sicurezza del cloud unificate che semplificano l'applicazione delle policy, automatizzano il rilevamento delle minacce e garantiscono una protezione coerente negli ambienti ibridi e multi-cloud. Sfruttando questi approfondimenti e best practice, le organizzazioni possono adottare un approccio alla sicurezza del cloud resiliente che si adatta alle minacce e alle esigenze aziendali in evoluzione.

Estendiamo la nostra sincera gratitudine a [Fortinet](#), leader globale nella sicurezza del cloud, per il loro prezioso contributo a questa ricerca. La loro esperienza e i loro approfondimenti sulla sicurezza degli ambienti ibridi e multi-cloud hanno rafforzato in modo significativo i risultati e i suggerimenti presentati in questo rapporto.

Ci auguriamo che questo rapporto sia una risorsa preziosa per i professionisti dell'IT e della sicurezza informatica che si sforzano di proteggere le loro organizzazioni in questa era di rapida espansione del cloud.

Grazie,

Holger Schulze

Fondatore, Cybersecurity Insiders

Cambiamento delle strategie di distribuzione del cloud

La scelta della strategia di distribuzione del cloud di un'organizzazione ha un impatto diretto sulle esigenze di sicurezza, sui risultati operativi e sui requisiti dell'infrastruttura, e ciò la rende una decisione cruciale negli odierni ambienti IT multifaccettati.

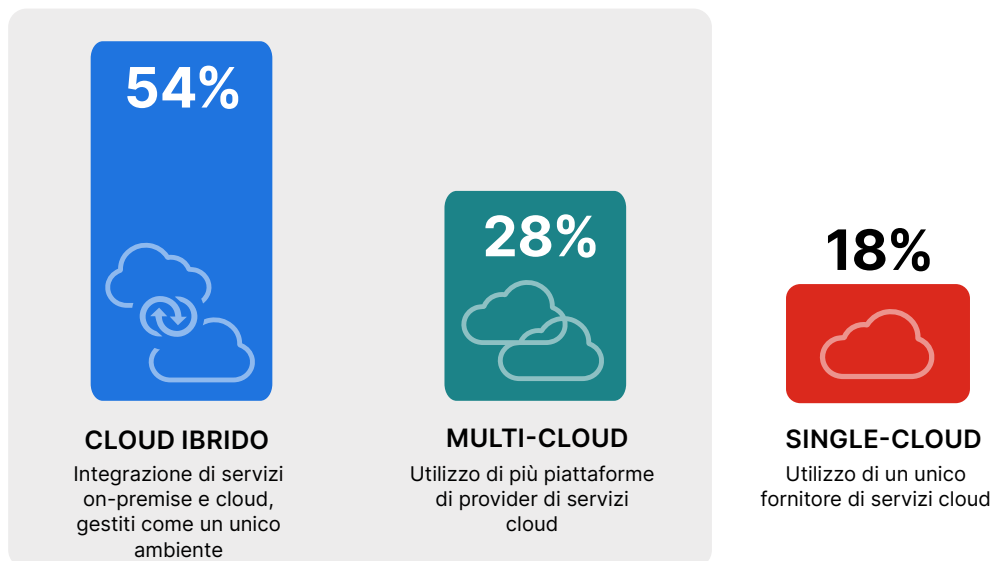
I risultati del sondaggio mostrano che il cloud ibrido è la strategia predominante, scelta dal 54% degli intervistati, in crescita rispetto al 43% dello scorso anno. Questa crescita riflette un forte spostamento da un unico servizio cloud verso l'integrazione di più servizi cloud con sistemi on-premise in ambienti coesivi. Ad esempio, un'azienda di vendita al dettaglio potrebbe utilizzare un cloud pubblico per ospitare le applicazioni rivolte ai clienti, mantenendo al contempo i dati di pagamento sensibili in un sistema privato on-premise per soddisfare i requisiti di conformità come PCI DSS. Tali strategie ibride consentono alle organizzazioni di fruire della scalabilità dei cloud pubblici mantenendo il controllo sui dati critici.

Le distribuzioni multi-cloud, fondamentali per gli scenari in cui le aziende distribuiscono i carichi di lavoro tra i vari provider per evitare la dipendenza da un solo fornitore o per utilizzare funzionalità specifiche, seguono con il 28%. Ad esempio, un'azienda tecnologica potrebbe ospitare le sue applicazioni a uso intensivo di elaborazione su Amazon Web Services (AWS) e utilizzare i servizi IA avanzati di Google Cloud per l'analisi dei dati, assicurandosi di ottimizzare le prestazioni e riducendo la dipendenza da un unico provider.

L'adozione di un unico servizio cloud sta diventando meno comune, con appena il 18% che si affida a un unico fornitore (in calo rispetto al 22% del 2024), spesso riflettendo la semplicità di gestione al costo potenziale di una minore flessibilità. Questo può essere il modello preferito dalle aziende più piccole, come uno studio legale che utilizza esclusivamente Azure di Microsoft per l'archiviazione dei documenti e la gestione dei flussi di lavoro, privilegiando la facilità di gestione rispetto alla diversificazione.

► Qual è la strategia principale della tua organizzazione per la distribuzione del cloud?

82% delle organizzazioni utilizza un ambiente multi-cloud o ibrido

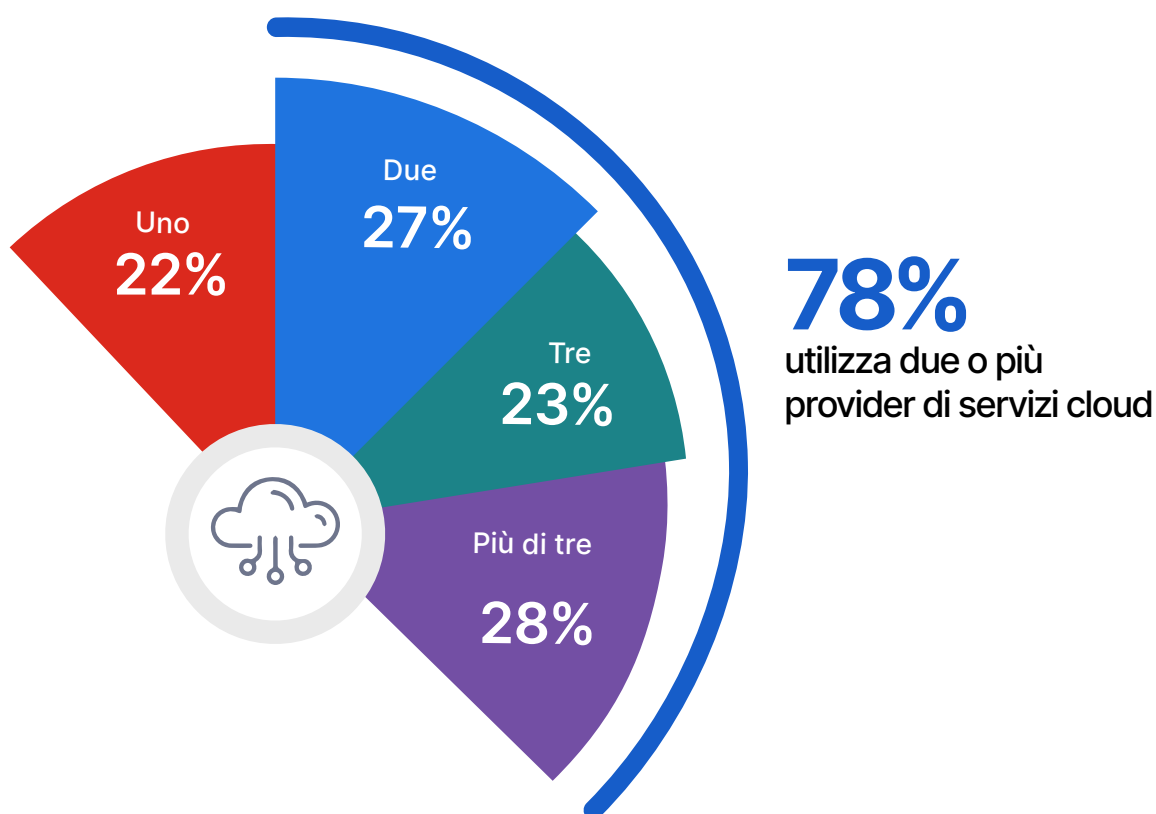


Espansione dell'adozione del multi-cloud

Il numero crescente di provider di servizi cloud utilizzati dalle aziende riflette l'evoluzione della preferenza per le strategie ibride e multi-cloud, nonché la complessità operativa introdotte da queste.

I risultati dell'indagine rivelano che il 78% delle organizzazioni utilizza due o più provider di servizi cloud, rispetto al 71% dello scorso anno, con un aumento di 7 punti che sottolinea il crescente spostamento verso l'adozione del multi-cloud. Ad esempio, un'azienda multinazionale potrebbe utilizzare AWS per la sua rete globale di distribuzione dei contenuti, mentre si affida alle offerte di Microsoft Azure predisposte per la conformità in aree geografiche con leggi rigorose sulla residenza dei dati. L'uso strategico di più provider consente alle aziende di sfruttare capacità specializzate, come i servizi IA di Google Cloud o l'esperienza di Oracle Cloud nel campo dei database, garantendo al contempo la resilienza attraverso la ridondanza.

► Quanti provider di servizi cloud utilizza attualmente la tua organizzazione?



Dominanza dei principali provider di servizi cloud

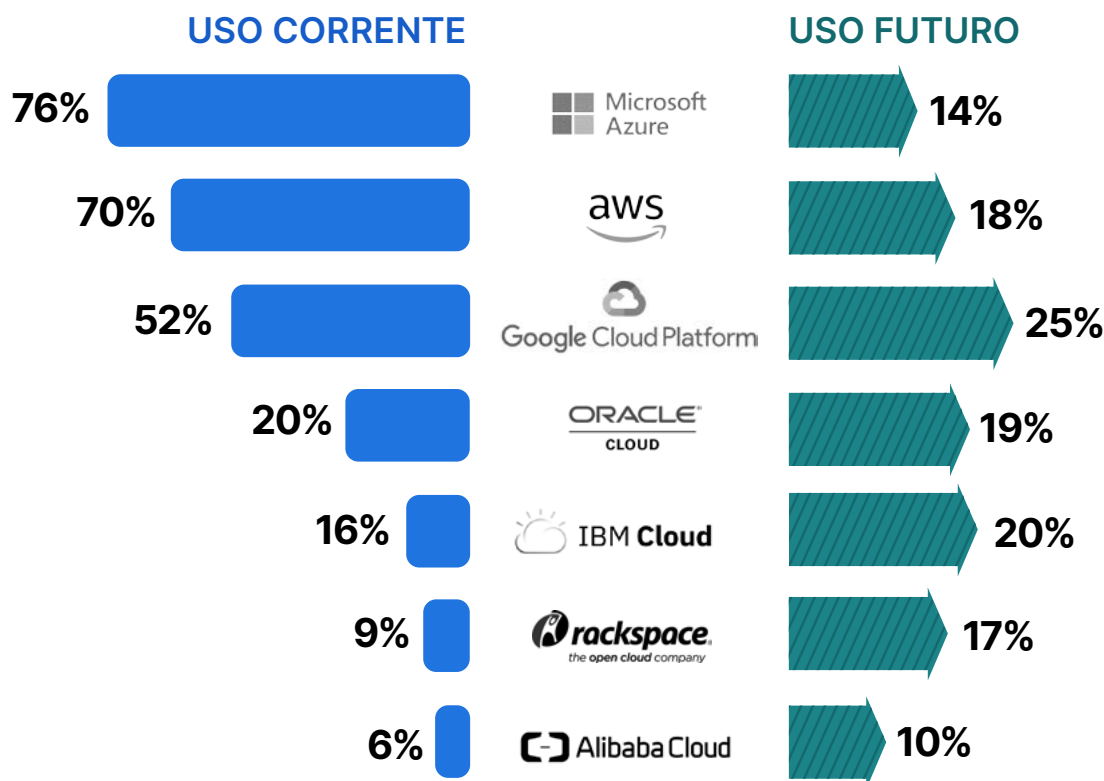
Capire a quali provider di servizi cloud si affidano le aziende attualmente, o quali prevedono di adottare, fa luce sulle preferenze del mercato e rivela come le aziende allineano le loro strategie cloud all'evoluzione dei carichi di lavoro e delle capacità specialistiche.

I risultati confermano la posizione dominante di Microsoft Azure e AWS, rispettivamente con il 76% e il 70% degli intervistati che dichiarano di utilizzarli correntemente.

Attualmente utilizzata dal 52% degli intervistati, la piattaforma Google Cloud sta guadagnando interesse, come dimostra il 25% degli intervistati che prevede di adottarla in futuro.

Nel frattempo, Oracle Cloud e IBM Cloud mantengono quote di mercato più ridotte, ma vedono un notevole interesse futuro, probabilmente grazie alla loro esperienza nell'integrazione con i sistemi legacy aziendali.

- Quali sono i provider IaaS cloud che utilizzi attualmente o che intendi utilizzare in futuro?
(Seleziona tutte le risposte pertinenti)



Superare le barriere all'adozione del cloud

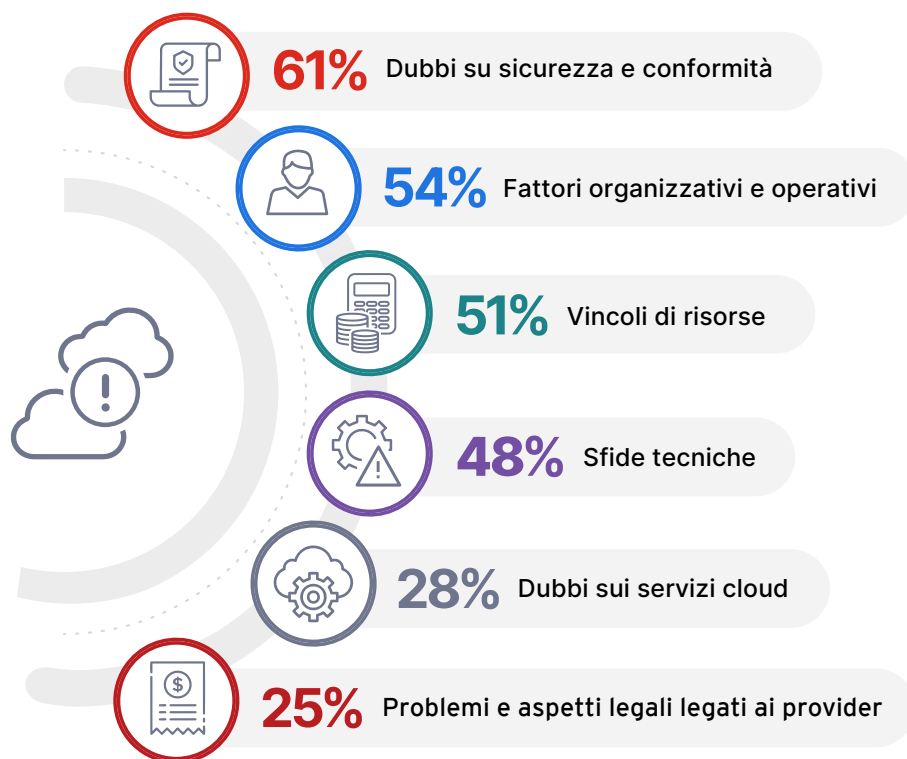
Il sondaggio rivela i principali ostacoli che le organizzazioni incontrano nell'adozione dei servizi cloud, evidenziando le sfide che i team IT e di sicurezza devono affrontare per sfruttare appieno il potenziale degli ambienti cloud.

I problemi di sicurezza e conformità rimangono la sfida principale, citata dal 61% degli intervistati (rispetto al 59% del sondaggio dello scorso anno). Ciò riflette il crescente interesse per questioni come la fuga di dati e la complessità di soddisfare i requisiti normativi. Ad esempio, un'organizzazione sanitaria potrebbe ritardare la migrazione delle cartelle cliniche sensibili dei pazienti nel cloud a causa dell'incertezza sulla conformità con l'HIPAA o altre leggi locali sulla protezione dei dati.

I fattori organizzativi e operativi seguono da vicino con il 54% (salendo al secondo posto dal 49% dell'anno scorso), evidenziando sfide come la resistenza al cambiamento, i problemi di dipendenza da un unico fornitore e gli ostacoli culturali. Un'azienda manifatturiera, ad esempio, può trovarsi di fronte a una resistenza interna quando trasferisce i sistemi legacy nel cloud, per il timore di perdere il controllo sui processi proprietari.

I vincoli di risorse, tra cui le competenze limitate del personale e le restrizioni di bilancio, sono citati dal 51% (in aumento rispetto al 49% del 2024), sottolineando la difficoltà che molte organizzazioni incontrano nella gestione e nella protezione delle funzionalità cloud. Nel frattempo, le sfide tecniche, anche se leggermente meno importanti quest'anno (48%), rappresentano ancora un ostacolo sostanziale, in particolare quando si tratta di integrare ambienti cloud ibridi complessi.

► Quali sono le principali barriere all'adozione del cloud nella tua organizzazione? (Seleziona tutte le risposte pertinenti)



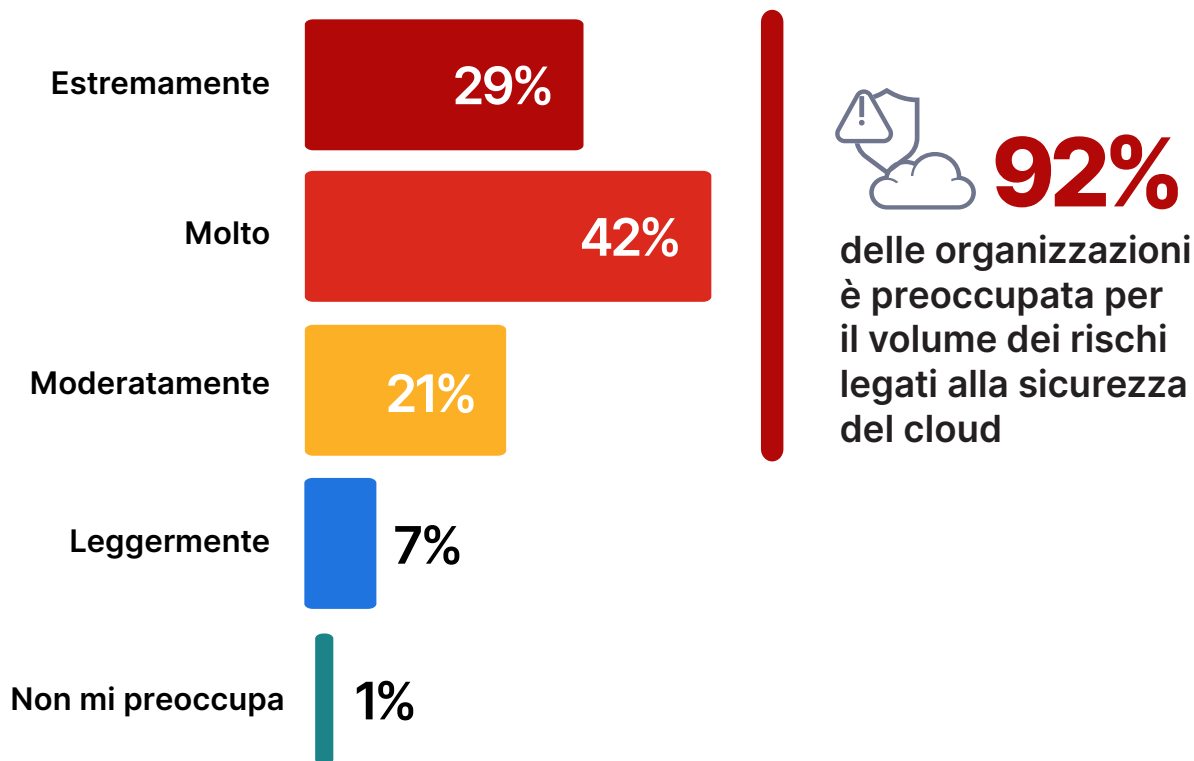
Dubbi sulla sicurezza del cloud pubblico

I persistenti dubbi sulla sicurezza dei cloud pubblici riflettono la sfida continua di bilanciare i vantaggi della scalabilità e dell'agilità con la necessità di una solida protezione.

Il 92% degli intervistati ha espresso dubbi sulla sicurezza del cloud pubblico, sottolineando la sua importanza come area critica di attenzione per i professionisti dell'IT e della sicurezza informatica.

Questa apprensione è in linea con i risultati di questo sondaggio, in cui il 61% ha identificato la sicurezza e la conformità come il principale ostacolo all'adozione del cloud. Ad esempio, un'azienda di servizi finanziari che sta valutando la migrazione al cloud per i dati delle transazioni dei clienti potrebbe esitare per timore di mancata conformità alle normative o di una potenziale esposizione di informazioni sensibili a causa di configurazioni errate. Tali dubbi si estendono a rischi specifici, tra cui la perdita di dati, la confusione sulla responsabilità condivisa e la visibilità limitata sulle attività dei provider di servizi cloud, complicando ulteriormente le decisioni di adozione.

► Quanto ti preoccupa la sicurezza dei cloud pubblici?



Sfide operative nella sicurezza del cloud

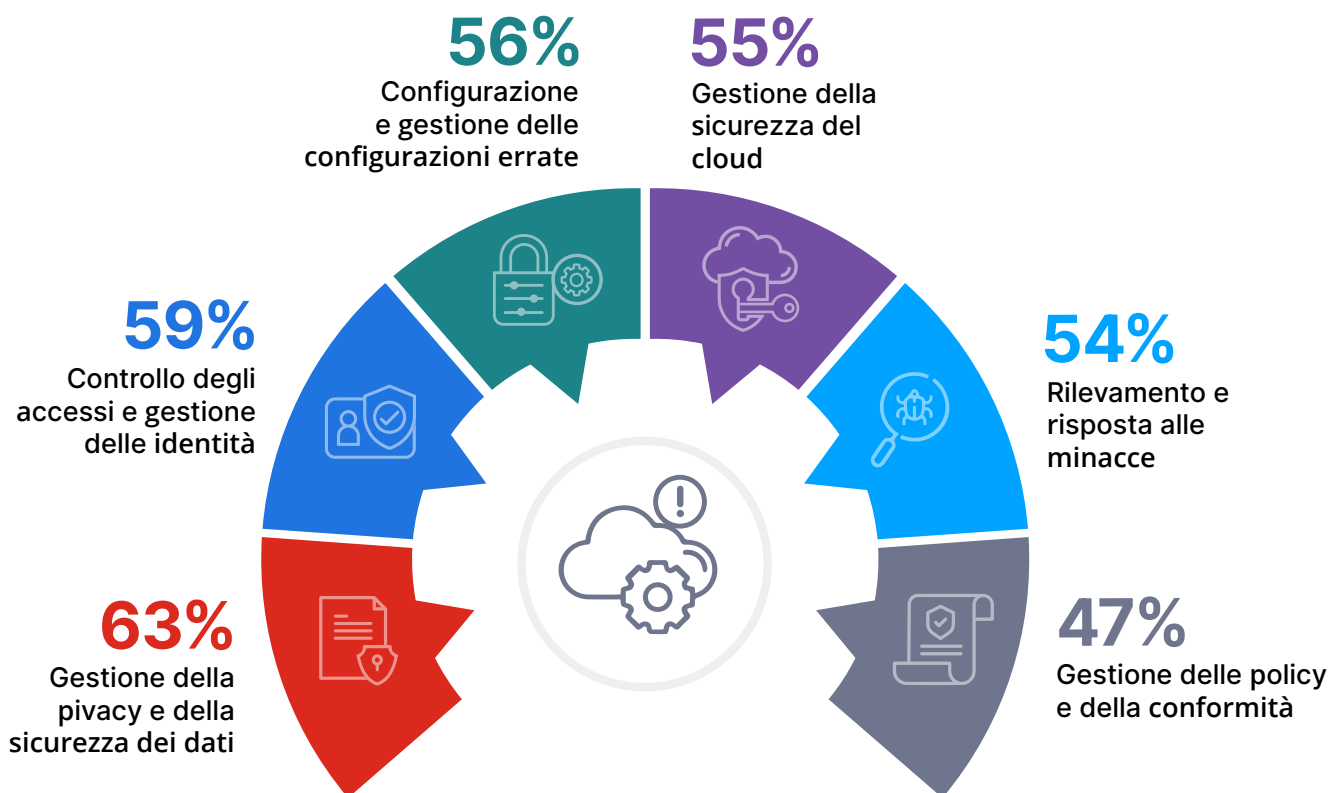
La gestione delle operazioni quotidiane di sicurezza del cloud rivela gli ostacoli complessi e in continua evoluzione che le organizzazioni devono affrontare per proteggere i loro ambienti.

La sicurezza dei dati e la privacy emergono come il principale timore, identificato dal 63% degli intervistati, riflettendo i dubbi attuali legati alla protezione delle informazioni sensibili e alla prevenzione delle fughe di dati. Il controllo degli accessi e la gestione delle identità seguono con il 59%, sottolineando la necessità di una solida gestione dell'autenticazione e dei privilegi negli ambienti cloud distribuiti. Una distribuzione di cloud ibrido, ad esempio, può incorrere in problemi di sincronizzazione delle policy di accesso degli utenti tra i sistemi on-premise e le piattaforme cloud.

La gestione delle configurazioni e delle errate configurazioni si colloca al terzo posto con il 56%, illustrando la difficoltà operativa di garantire una corretta configurazione del cloud, come il monitoraggio dell'esposizione pubblica involontaria dei bucket di storage del cloud, uno scenario che ha causato numerose violazioni di alto profilo.

La gestione della sicurezza del cloud (55%), il rilevamento e la risposta alle minacce (54%) e la gestione delle policy e della conformità (47%) evidenziano collettivamente la necessità di soluzioni coerenti e scalabili per gestire ambienti multi-cloud.

► Quali sono le principali sfide nella gestione delle operazioni quotidiane di sicurezza del cloud? (Seleziona tutte le risposte pertinenti)



Le risposte aggiuntive includono:

Shadow IT e utilizzo di app non autorizzate 46% | Integrazione e automazione del cloud 43% | Sicurezza degli endpoint 40% | Assegnazione delle risorse 38%
Pratiche DevSecOps 31% | Agilità operativa e complessità 25%

Protezione degli ambienti multi-cloud

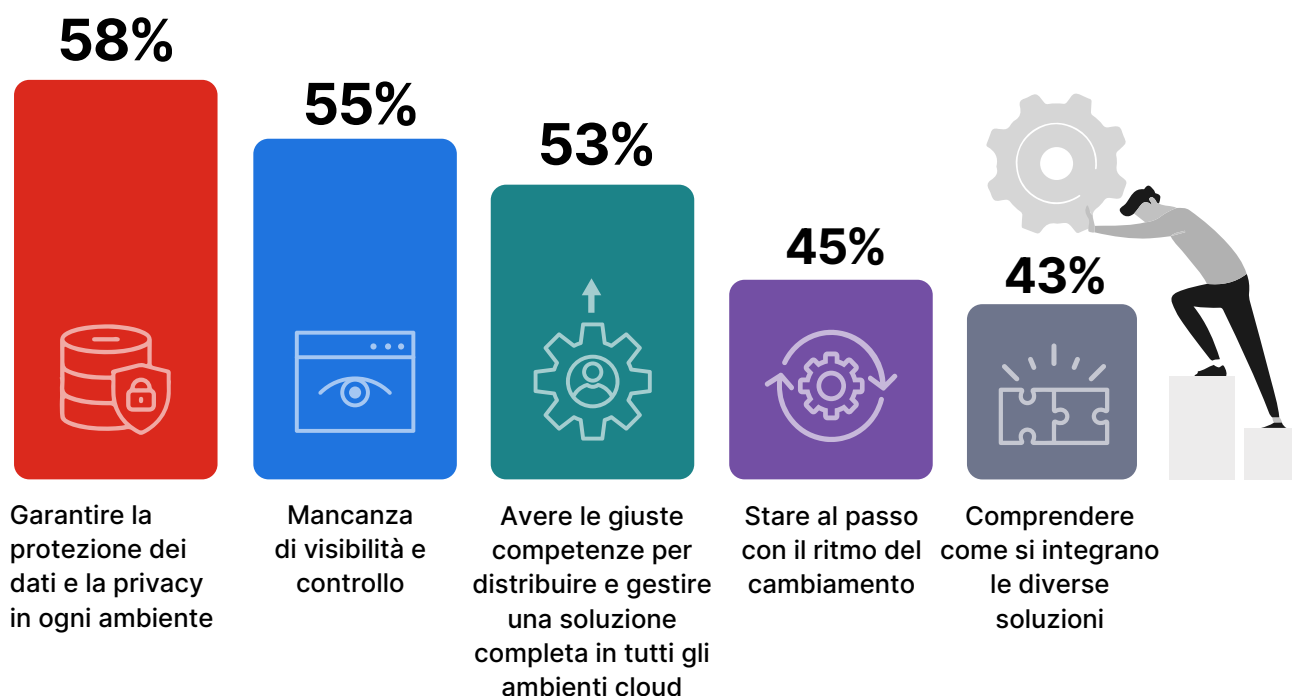
La sicurezza degli ambienti multi-cloud introduce sfide specifiche derivanti dalla loro intrinseca complessità e dalla mancanza di standardizzazione fino alla rapida evoluzione delle tecnologie. Questi problemi hanno un impatto diretto sulla capacità delle organizzazioni di proteggere i dati sensibili, mantenere l'efficienza operativa e gestire ecosistemi cloud diversi.

Garantire la privacy e la protezione dei dati per ogni ambiente continua a essere la sfida principale, citata dal 58% degli intervistati, in aumento rispetto al 55% del 2024. Ciò rispecchia i risultati precedenti del nostro sondaggio, in cui la privacy e la sicurezza dei dati sono state identificate come il principale timore operativo (63%), sottolineando la necessità di salvaguardare in modo coerente le infrastrutture cloud frammentate.

La mancanza di visibilità e controllo, per il 55%, sottolinea la difficoltà di mantenere la supervisione in configurazioni multi-cloud, un timore già emerso in precedenza, quando il 55% ha indicato la gestione della sicurezza del cloud come una sfida quotidiana.

La mancanza di competenze per la distribuzione e la gestione di soluzioni multi-cloud complete è citata dal 53%. Sfide come la capacità di stare al passo con il ritmo del cambiamento (45%) e la comprensione di come le diverse soluzioni si adattano tra loro (43%) riflettono gli ostacoli operativi e strategici della navigazione nella rapida evoluzione delle tecnologie cloud.

► Quali sono le maggiori sfide per la sicurezza degli ambienti multi-cloud? (Seleziona tutte le risposte pertinenti)



Le risposte aggiuntive includono:

Gestione dei costi delle diverse soluzioni 41% | Comprensione delle opzioni di integrazione dei servizi 40% | Disponibilità di un accesso continuo agli utenti in base alle loro credenziali 37% | Selezione del giusto set di servizi 30% | Altro 1%

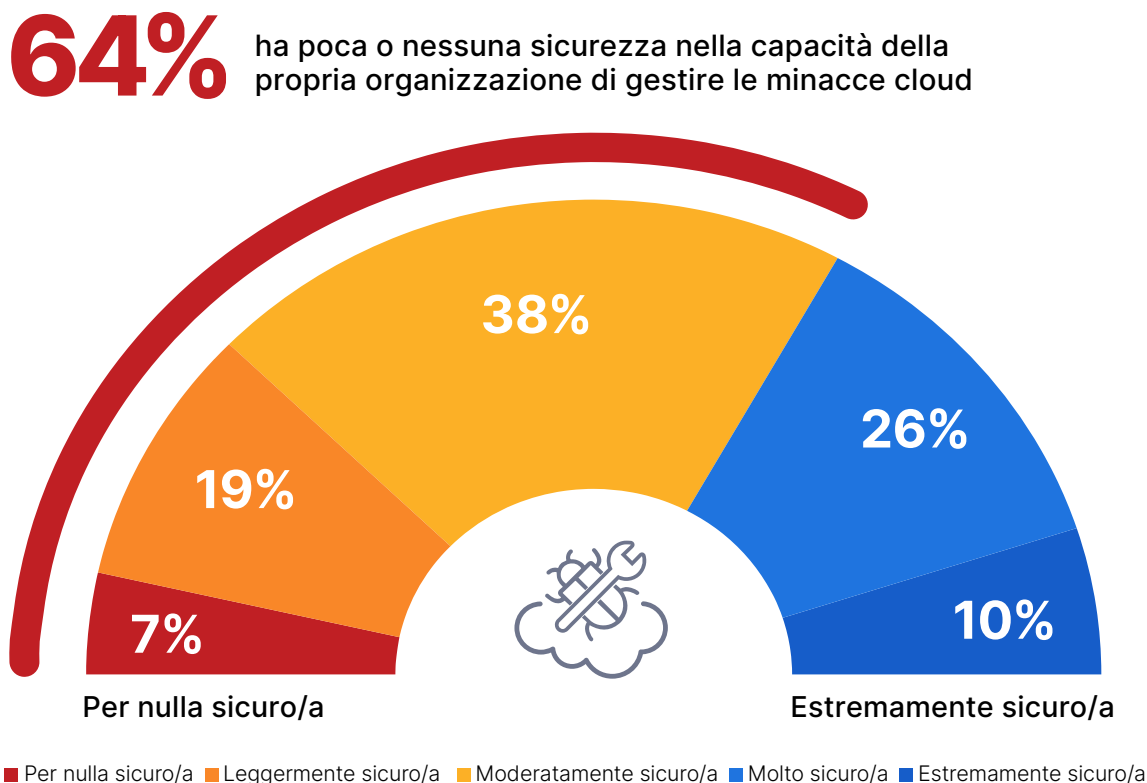
Scarsa fiducia nel rilevamento delle minacce in tempo reale

La capacità di rilevare e rispondere in tempo reale alle minacce negli ambienti cloud è un aspetto critico, in quanto le organizzazioni adottano strategie multi-cloud e ibride sempre più complesse. Queste architetture introducono sfide uniche per ottenere una visibilità continua e una risposta rapida su piattaforme diverse.

I dati del sondaggio evidenziano un significativo divario di fiducia, con il 64% degli intervistati che dichiara di non avere fiducia nella capacità della propria organizzazione di gestire il rilevamento delle minacce in tempo reale. Ad esempio, un'organizzazione potrebbe non essere in grado di collegare tra loro una serie di azioni dannose isolate, con conseguenti ritardi significativi nell'identificazione e nella risposta a una potenziale violazione. Questa tendenza suggerisce che, sebbene molte organizzazioni dispongano di misure di sicurezza fondamentali, la crescente sofisticazione delle minacce del cloud e le sfide legate alla gestione di ambienti diversificati le rendono vulnerabili agli attacchi avanzati e alle configurazioni errate. I risultati del sondaggio discussi in precedenza sono in linea con questo dato, mostrando che la perdita di visibilità e di controllo (55%) e le sfide nel rilevamento delle minacce e nella risposta (54%) sono le principali barriere nelle operazioni di sicurezza del cloud.

Solo il 10% degli intervistati si dichiara estremamente fiducioso e un altro 26% si sente molto fiducioso, lasciando meno del 40% ben preparato alle esigenze della moderna gestione delle minacce del cloud.

► Quanto sei sicuro/a della capacità della tua organizzazione di rilevare e rispondere alle minacce in tutti gli ambienti cloud in tempo reale?



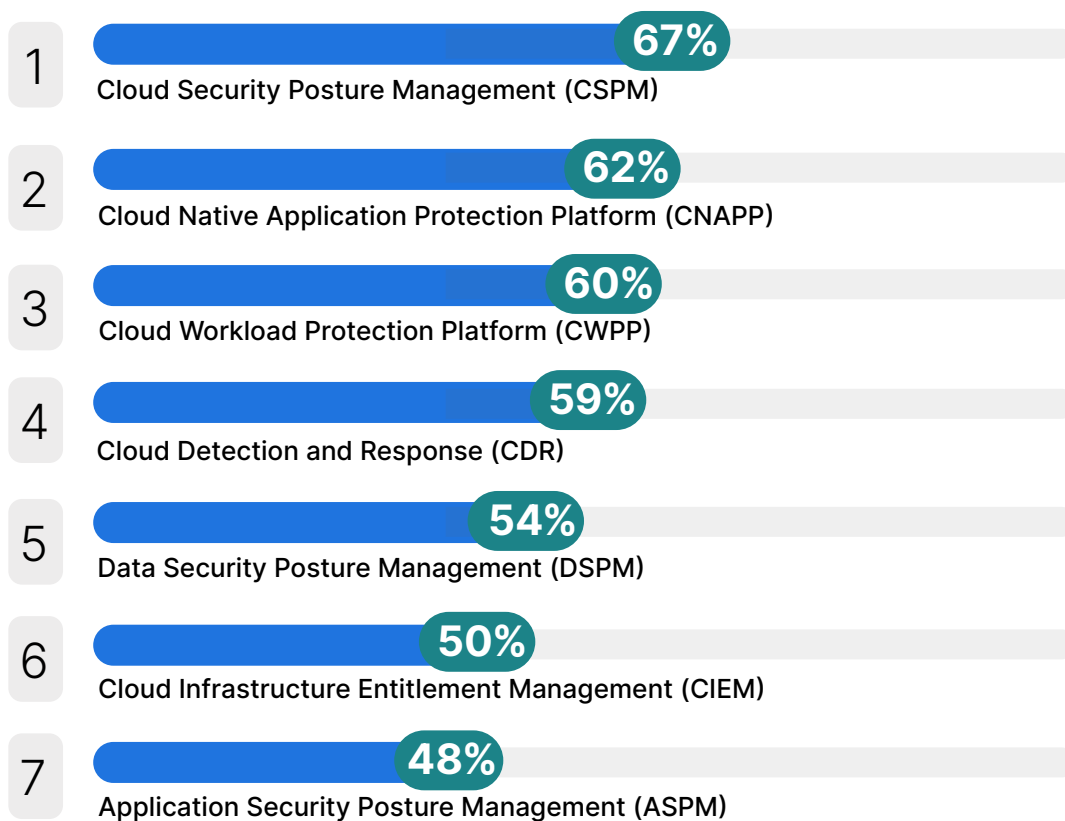
Priorità della sicurezza del cloud

Man mano che le aziende espandono la propria impronta cloud, la distribuzione della giusta combinazione di funzionalità di sicurezza è essenziale per garantire resilienza, conformità ed efficienza operativa di fronte alle crescenti minacce.

Alla domanda sulle priorità di adozione degli strumenti critici per la sicurezza del cloud nei prossimi 12 mesi, il Cloud Security Posture Management (CSPM) è in testa con il 67%, sottolineando il suo ruolo critico nell'identificare e correggere le configurazioni errate negli ambienti cloud. Ad esempio, uno strumento CSPM potrebbe avvisare un rivenditore di bucket di storage esposti pubblicamente in AWS, evitando una costosa violazione dei dati.

Allo stesso modo, le Cloud Native Application Protection Platform (CNAPP), con il 62%, evidenziano il crescente riconoscimento della necessità di una sicurezza end-to-end del ciclo di vita delle applicazioni. Una CNAPP potrebbe segnalare in modo proattivo le vulnerabilità nei carichi di lavoro containerizzati in esecuzione in Kubernetes, identificare attività di runtime dannose e rilevare una catena di eventi che indicano una compromissione. Subito dopo, le Cloud Workload Protection Platform (CWPP), con il 60%, e il Cloud Detection and Response (CDR), con il 59%, evidenziano la crescente attenzione alla sicurezza dei carichi di lavoro e all'attenuazione delle minacce, in particolare nelle configurazioni multi-cloud. L'adozione dell'approccio Cloud Infrastructure Entitlement Management (CIEM), con il 50%, dimostra ulteriormente la richiesta di solidi controlli sugli accessi e sui privilegi tra le diverse piattaforme cloud e la spinta verso l'implementazione del principio del privilegio minimo o l'eliminazione delle credenziali inutilizzate.

► Quali delle seguenti funzionalità stai utilizzando o pensi di utilizzare nei prossimi 12 mesi? (Seleziona tutte le risposte pertinenti)



Colmare il divario nelle competenze di sicurezza informatica

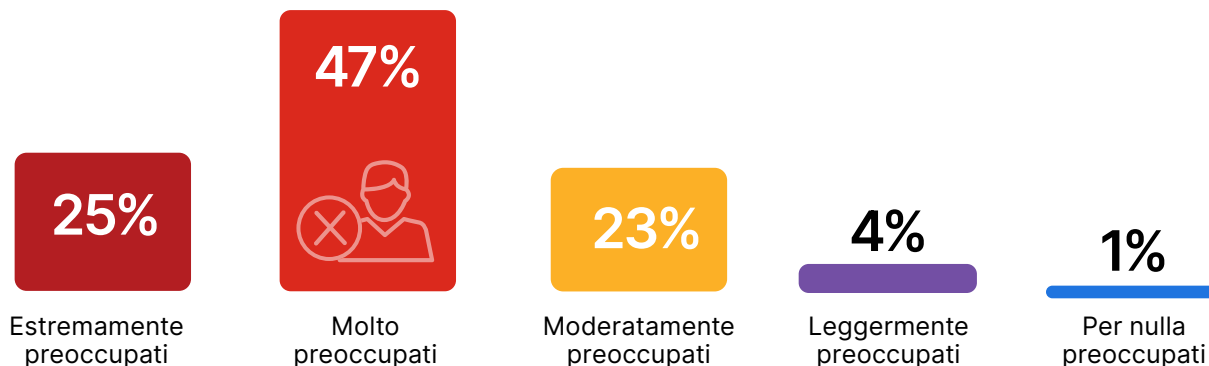
La carenza di professionisti qualificati nel settore della sicurezza informatica continua ad essere un problema critico che ha un impatto diretto sulla capacità di un'organizzazione di proteggere le proprie risorse e di rispondere efficacemente alle minacce in evoluzione.

I risultati rivelano che il 95% degli intervistati è da moderatamente a estremamente preoccupato per l'attuale carenza di competenze in materia di sicurezza informatica, evidenziando la tensione significativa che grava sulle organizzazioni, che faticano ad assumere e a fidelizzare i talenti necessari per affrontare le sfide di sicurezza informatica sempre più complesse. Ad esempio, un fornitore di servizi sanitari che ha difficoltà a implementare controlli di sicurezza multi-cloud potrebbe subire ritardi a causa della mancanza di talenti con competenze specifiche per il cloud, come la gestione della configurazione o l'approccio CIEM.

► Quanto ti preoccupa la carenza di competenze a livello di settore di professionisti qualificati nel campo della sicurezza informatica?

95%

delle organizzazioni è da moderatamente a estremamente preoccupata per la carenza di competenze a livello di settore di professionisti qualificati nel campo della sicurezza informatica



Questo timore è confermato dai dati del sondaggio che mostra come il 76% delle organizzazioni abbia oggi una carenza di talenti nel campo della sicurezza informatica.

► La tua organizzazione ha una carenza di talenti nel campo della sicurezza informatica?



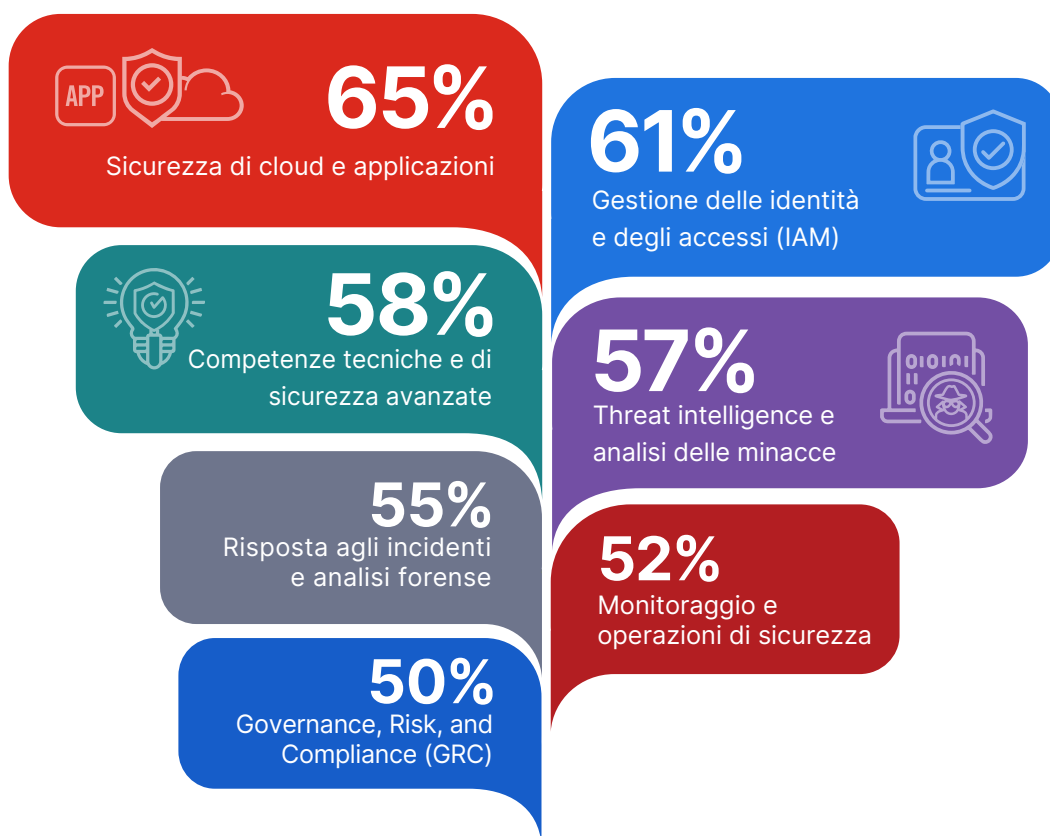
Competenze di sicurezza fondamentali per le minacce odierne

I risultati del sondaggio sulle competenze più importanti in materia di sicurezza evidenziano il know-how diversificato e in continua evoluzione che le organizzazioni richiedono per affrontare le sfide sempre più complesse della sicurezza del cloud.

Le competenze in materia di sicurezza del cloud e delle applicazioni sono al primo posto con il 65%, a testimonianza della priorità che le organizzazioni attribuiscono alla sicurezza delle piattaforme e delle applicazioni cloud. Ad esempio, le competenze in materia di sicurezza specifiche per le piattaforme cloud potrebbero comportare la creazione di protezioni automatizzate e di landing zone scalabili e sicure, tutte disponibili sotto forma di codice per la distribuzione automatizzata.

La gestione delle identità e degli accessi segue a ruota con il 61%, sottolineando la necessità di solidi controlli degli accessi, in particolare negli ambienti ibridi e multi-cloud, dove la gestione unificata dei privilegi degli utenti è essenziale. Le competenze tecniche e avanzate in materia di sicurezza (58%) e la threat intelligence e l'analisi delle minacce (57%) riflettono la crescente domanda di specialisti in grado di sfruttare l'IA e di comprendere le tattiche sofisticate degli avversari, al fine di identificare e attenuare rapidamente le attività dannose, in particolare per quanto riguarda gli account di amministrazione del cloud compromessi. Le competenze in materia di risposta agli incidenti e di analisi forense (55%) rimangono essenziali per attenuare le violazioni, mentre il monitoraggio e le operazioni di sicurezza (52%) evidenziano la necessità di competenze per rilevare le anomalie e accelerare l'attenuazione.

► Quali sono le competenze più importanti in materia di sicurezza richieste nella tua organizzazione? (Seleziona tutte le risposte pertinenti)



Le risposte aggiuntive includono:

Formazione e sensibilizzazione 45% | Comunicazione e strategia 39% | Non so 3%

Tendenze di investimento nella sicurezza del cloud

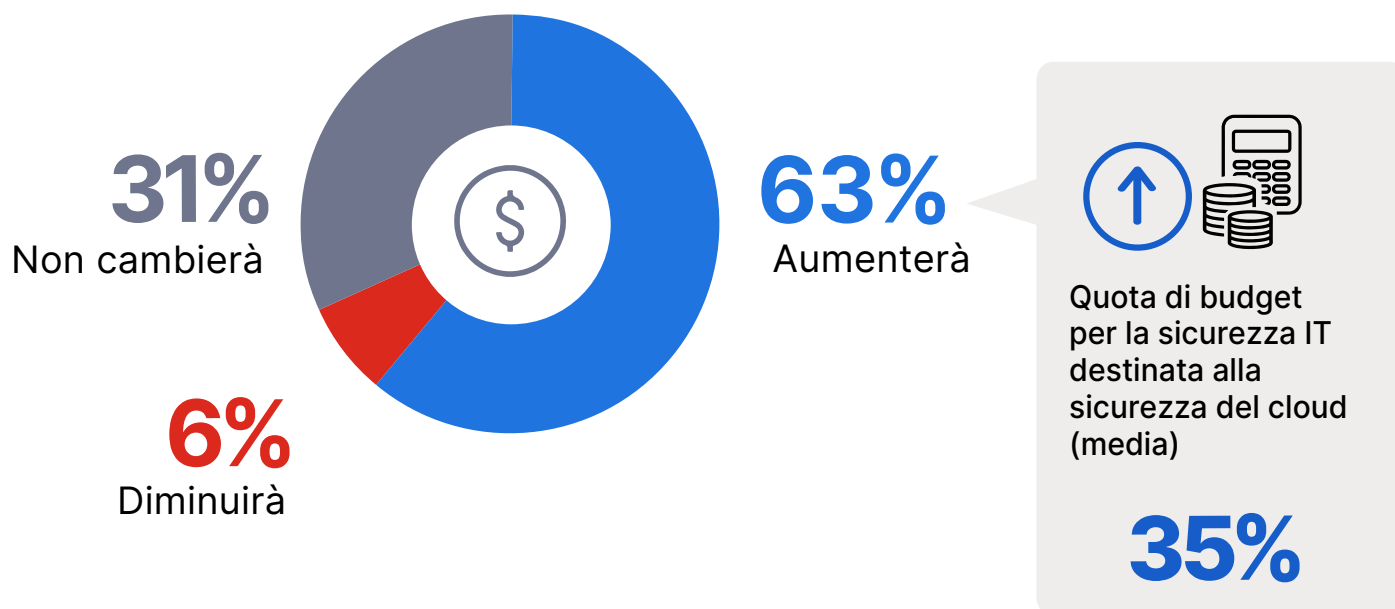
I risultati del sondaggio rivelano nuovi spunti su come le aziende stanno dando priorità alle risorse finanziarie per affrontare le sfide della sicurezza del cloud. La maggioranza rappresentata dal 63% degli intervistati ha dichiarato di voler aumentare il budget per la sicurezza del cloud nei prossimi 12 mesi (rispetto al 61% dell'anno scorso), segnalando un forte riconoscimento della necessità di rafforzare le difese nelle configurazioni ibride e multi-cloud.

Nel frattempo, il 31% indica budget invariati (in calo rispetto al 32% del 2024), il che probabilmente riflette organizzazioni che hanno già investito molto o che stanno gestendo esigenze operative consistenti. Solo il 6% prevede una diminuzione, una tendenza rara in un'epoca di minacce cloud e requisiti normativi in aumento.

In media, il 35% dei budget per la sicurezza IT è destinato alla sicurezza, a dimostrazione del fatto che la protezione del cloud sta diventando un punto focale della spesa complessiva per la sicurezza, in particolare con l'accelerazione dell'adozione del cloud.

Questa crescente enfasi sugli investimenti nella sicurezza del cloud riflette un approccio proattivo per affrontare le lacune in termini di visibilità, controllo degli accessi e rilevamento delle minacce, sfide citate in tutto il rapporto. Le organizzazioni che stanno pianificando un aumento del budget dovrebbero concentrarsi su soluzioni che integrino in modo efficiente le funzionalità chiave, come la CNAPP, per aumentare al massimo l'impatto del loro investimento.

► Come cambierà il tuo budget per la sicurezza del cloud nei prossimi 12 mesi?

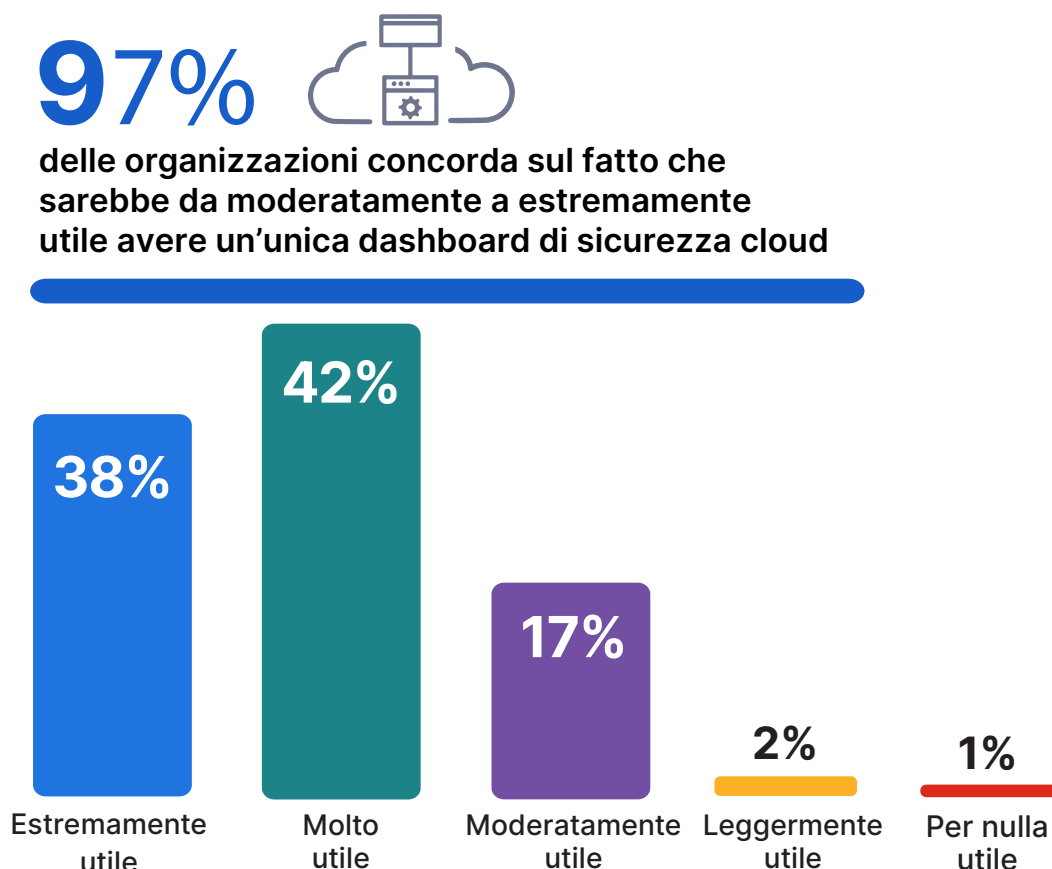


Il valore delle piattaforme di sicurezza del cloud unificate

Il valore di un'unica piattaforma di sicurezza del cloud unificata con una dashboard centralizzata risiede nel suo potenziale di semplificazione della configurazione delle policy, di garanzia di coerenza e di miglioramento della visibilità su tutta l'impronta cloud di un'organizzazione.

I risultati del sondaggio mostrano un forte interesse per questo concetto, con il 97% degli intervistati che ritiene tale piattaforma da moderatamente a estremamente utile. Ad esempio, un'unica dashboard potrebbe consentire a un'organizzazione di servizi finanziari di applicare controlli di accesso uniformi su AWS, Azure e Google Cloud, riducendo la probabilità di errori di configurazione. Ciò è in linea con i risultati precedenti, in cui il 55% degli intervistati ha citato la perdita di visibilità e di controllo come sfida principale negli ambienti multi-cloud e ibridi, sottolineando la necessità di strumenti centralizzati per colmare queste lacune.

- **Quanto sarebbe utile avere un'unica piattaforma di sicurezza per il cloud con un'unica dashboard dove poter configurare tutte le policy necessarie per proteggere i dati in modo coerente e completo in tutto la tua impronta cloud?**



Best practice per una sicurezza ibrida e multi-cloud più solida

Con la crescente adozione da parte delle aziende di ambienti ibridi e multi-cloud, la gestione di diversi provider e il mantenimento di una solida sicurezza diventano sempre più complessi. Per affrontare queste sfide in modo efficace, è essenziale implementare best practice strategiche che siano in linea con gli approfondimenti del settore e sfruttino soluzioni di sicurezza avanzate.

I seguenti suggerimenti offrono passi praticabili per migliorare la il tuo approccio alla sicurezza multi-cloud.

1

AUTOMATIZZA IL RILEVAMENTO E LA CORREZIONE DEI RISCHI DEL CLOUD

Le configurazioni errate sono una vulnerabilità comune, con il 67% degli intervistati che utilizza o prevede di adottare strumenti automatizzati per affrontare questo problema. Il monitoraggio continuo e le soluzioni di correzione in tempo reale possono identificare proattivamente i rischi, come lo storage configurato erroneamente o le autorizzazioni eccessive, e correggerli in modo efficiente. Questi strumenti semplificano anche la conformità alle normative di settore.

2

PROTEGGI I FLUSSI DI DATI TRA GLI AMBIENTI CLOUD

Quando i dati si spostano da un ambiente cloud all'altro, è fondamentale garantirne la sicurezza e l'integrità. Con il 58% degli intervistati che ha indicato la privacy e la protezione dei dati come uno dei principali timori, l'utilizzo di strumenti che forniscono una visibilità completa dei flussi di dati aiuta le organizzazioni a salvaguardare le informazioni durante il transito. Questi strumenti consentono di monitorare i potenziali rischi, prevenire gli accessi non autorizzati e agevolare l'adesione a quadri normativi come il GDPR e il CCPA, migliorando gli sforzi complessivi per la protezione dei dati.

3

IMPLEMENTA MECCANISMI UNIFICATI DI RILEVAMENTO DELLE MINACCE

Oltre la metà degli intervistati (54%) ha evidenziato difficoltà nel rilevare e rispondere alle minacce negli ambienti multi-cloud. Le soluzioni di rilevamento delle minacce unificate centralizzano la visibilità, consentendo ai team di identificare e rispondere rapidamente alle anomalie. Questi strumenti possono correlare i dati tra diversi ambienti cloud per ridurre i tempi di rilevamento e migliorare la precisione delle risposte.

4

INVESTI IN FORMAZIONE SPECIFICA SUL CLOUD PER I TEAM DI SICUREZZA

La carenza di competenze colpisce il 76% delle organizzazioni, limitando la loro capacità di distribuire e gestire le soluzioni cloud-native in modo efficace. L'aggiornamento dei dipendenti in aree come DevSecOps e sicurezza dei container consente ai team di affrontare le sfide emergenti in materia di sicurezza.

5

ADOTTA L'APPROCCIO POLICY-AS-CODE PER UN'APPLICAZIONE COERENTE DELLA SICUREZZA

Poiché il 43% degli intervistati ha segnalato difficoltà nel capire come si integrano le diverse soluzioni, l'utilizzo di approcci di tipo policy-as-code garantisce un'applicazione coerente tra le varie piattaforme. Il concetto policy-as-code semplifica gli audit e consente la gestione automatizzata della configurazione, assicurando che i controlli di sicurezza rimangano allineati ai requisiti organizzativi.

6

ALLINEA GLI INVESTIMENTI IN SICUREZZA AI REQUISITI DEI CARICHI DI LAVORO DELLE APPLICAZIONI

La sicurezza a livello di applicazione è una priorità crescente, con il 62% degli intervistati che prevede di adottare piattaforme di protezione complete. La sicurezza end-to-end per le applicazioni, dallo sviluppo al runtime, garantisce una protezione su misura per i carichi di lavoro, supportando al contempo policy coerenti tra gli ambienti. Le soluzioni che si integrano con gli ambienti containerizzati e le protezioni dei runtime rispondono efficacemente a questa esigenza.

7

STANDARDIZZA I CONTROLLI DI ACCESSO TRA LE PIATTAFORME CLOUD

Il controllo degli accessi e la gestione delle identità rimangono una delle principali sfide per il 59% delle organizzazioni, soprattutto nelle configurazioni cloud distribuite. Le soluzioni centralizzate per il controllo degli accessi possono semplificare la gestione dei privilegi degli utenti e applicare policy di sicurezza coerenti in ambienti ibridi e multi-cloud. L'implementazione di una piattaforma di identità unificata garantisce l'applicazione continua delle policy, riducendo al minimo il rischio di accessi non autorizzati.

8

ADOTTA STRUMENTI DI SICUREZZA BASATI SUL CLOUD PER LA SCALABILITÀ

Con il 54% degli intervistati che ha identificato il cloud ibrido come modello di distribuzione principale, gli strumenti di sicurezza scalabili basati sul cloud sono essenziali. Queste soluzioni consentono una protezione coerente tra i sistemi on-premise e i cloud pubblici, assicurando alle organizzazioni la possibilità di espandere la propria impronta cloud senza compromettere l'efficienza operativa.

Conclusioni

Questo rapporto sottolinea l'importanza di un investimento strategico in strumenti, formazione e processi unificati, adatti alle esigenze in evoluzione della sicurezza ibrida e multi-cloud. Affrontando le sfide (come le configurazioni errate, i divari di competenze e l'assenza di visibilità), le organizzazioni possono adottare un approccio alla sicurezza resiliente.

L'implementazione delle best practice fornite in questo rapporto consente alle aziende di prosperare in ambienti cloud complessi, salvaguardando le risorse critiche e mantenendo agilità e conformità in un'epoca di rapida trasformazione digitale.

Glossario della sicurezza del cloud

Questo glossario fornisce una rapida panoramica delle tecnologie essenziali per la sicurezza del cloud discusse in questo rapporto, concentrandosi su ciò che fanno, sui problemi di sicurezza che risolvono e sul perché sono importanti per la protezione dei complessi ambienti cloud di oggi.

Gestione dell'approccio alla sicurezza delle applicazioni (ASPM, Application Security Posture Management): l'ASPM fornisce visibilità sulle vulnerabilità delle applicazioni e sui problemi di configurazione durante il ciclo di vita dello sviluppo del software, supporta le pratiche di codifica sicura e integra la sicurezza nei flussi di lavoro DevSecOps. L'ASPM è fondamentale per garantire che le applicazioni rimangano sicure dallo sviluppo alla distribuzione e al runtime.

Rilevamento e risposta nel cloud (CDR, Cloud Detection and Response): il CDR è una tecnologia specializzata che identifica e attenua le minacce negli ambienti cloud. Offre visibilità in tempo reale sulle attività del cloud, consentendo un rapido rilevamento delle anomalie e una rapida risposta agli incidenti. Il CDR è fondamentale per mantenere una solida difesa contro le minacce sofisticate nelle configurazioni cloud distribuite.

Gestione dei diritti di accesso all'infrastruttura cloud (CIEM, Cloud Infrastructure Entitlement Management): si concentra sulla gestione delle autorizzazioni e dei controlli di accesso negli ambienti cloud. Identifica le autorizzazioni eccessive, applica i principi del privilegio minimo e riduce il rischio di abuso dei privilegi. CIEM è importante per mantenere policy di accesso di accesso sicure e conformi nelle architetture multi-cloud.

Piattaforma di protezione delle applicazioni cloud-native (CNAPP, Cloud Native Application Protection Platform): integra diverse funzioni di sicurezza per proteggere le applicazioni cloud-native durante il loro ciclo di vita. Combina protezione dei carichi di lavoro, gestione della configurazione e difesa del runtime per proteggere container, funzioni serverless e altri carichi di lavoro cloud-native. CNAPP è essenziale per le organizzazioni che adottano pratiche di sviluppo moderne come DevOps e microservizi.

Gestione dell'approccio alla sicurezza del cloud (CSPM, Cloud Security Posture Management): è una soluzione progettata per automatizzare il rilevamento delle configurazioni errate negli ambienti cloud. Monitora continuamente l'infrastruttura cloud alla ricerca di rischi per la sicurezza, come i bucket di storage esposti o i controlli di accesso troppo permissivi, garantendo la conformità ai quadri normativi. CSPM è fondamentale per mantenere la visibilità e affrontare le vulnerabilità negli ambienti multi-cloud e ibridi.

Piattaforma di protezione dei carichi di lavoro cloud (CWPP, Cloud Workload Protection Platform): protegge i carichi di lavoro negli ambienti cloud, tra cui macchine virtuali, container e architetture serverless. Fornisce visibilità sulle vulnerabilità, garantisce policy di sicurezza coerenti e protegge i carichi di lavoro dalle minacce avanzate. CWPP è fondamentale per le organizzazioni che gestiscono carichi di lavoro cloud dinamici e diversificati.

Gestione dell'approccio alla sicurezza dei dati (DSPM, Data Security Posture Management): è una soluzione incentrata sui dati che identifica, classifica e protegge le informazioni sensibili negli ambienti cloud. Garantisce la corretta protezione dei dati e l'allineamento con le normative sulla privacy come il GDPR e il CCPA. È fondamentale per affrontare le sfide della salvaguardia delle informazioni sensibili negli ecosistemi cloud complessi.

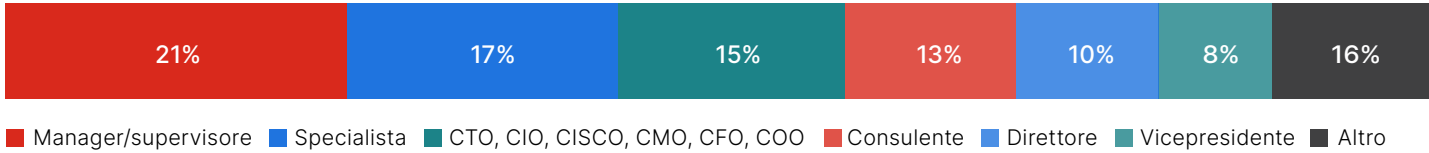
Metodologia e dati demografici

Il Rapporto sulla sicurezza del cloud 2025 si basa su un sondaggio completo condotto alla fine del 2024, che ha raccolto le opinioni di 873 professionisti dell'IT e della sicurezza informatica in diversi paesi e settori, tra cui tecnologia, servizi finanziari, sanità e pubblica amministrazione. Gli intervistati rappresentavano organizzazioni di varie dimensioni, dalle piccole imprese alle grandi aziende, e comprendevano professionisti con ruoli che andavano dagli specialisti ai dirigenti di alto livello.

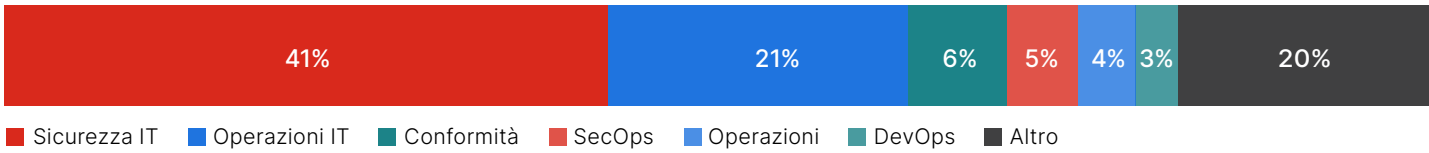
Il sondaggio, condotto online, ha esplorato le tendenze, le sfide e le priorità principali della sicurezza del cloud, fornendo una visione a tutto tondo di come le organizzazioni stiano affrontando le complessità degli ambienti cloud e adottando tecnologie di sicurezza per affrontare le minacce emergenti.

Per le domande che consentono agli intervistati di selezionare più risposte, le percentuali possono essere superiori al 100%, poiché i partecipanti possono scegliere più di un'opzione.

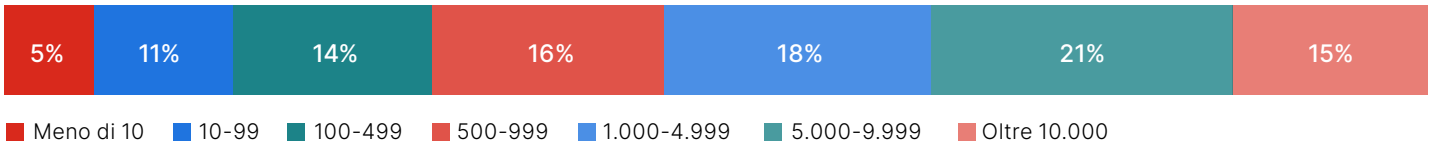
LIVELLO DI CARRIERA



REPARTO



DIMENSIONI DELL'AZIENDA



SETTORE



Riutilizzo dei contenuti

Incoraggiamo il riutilizzo dei dati, dei grafici e dei testi pubblicati in questo rapporto secondo i termini di questa [Licenza internazionale Creative Commons attribuzione 4.0](#). Puoi condividere e fare uso commerciale di quest'opera, a condizione che al rapporto venga fornita l'attribuzione prevista dai termini della licenza. Ad esempio: "Rapporto sulla sicurezza cloud 2025 di Cybersecurity Insiders e Fortinet".



Fortinet (NASDAQ: FTNT) protegge le principali aziende, i più importanti fornitori di servizi e le più grandi organizzazioni governative di tutto il mondo.

Fortinet permette ai clienti di avere una visibilità e un controllo completi su tutta la superficie di attacco in espansione e la capacità di soddisfare requisiti prestazionali sempre maggiori, oggi e in futuro. Solo la piattaforma Fortinet Security Fabric è in grado di affrontare le sfide più critiche per la sicurezza e proteggere i dati in tutta l'infrastruttura digitale, che si tratti di reti, applicazioni, multi-cloud o ambienti edge. Fortinet è al primo posto tra le aziende di sicurezza, con oltre 800.000 clienti che si affidano alle sue soluzioni e ai suoi servizi per proteggere le proprie attività.

www.fortinet.com

Cybersecurity

I N S I D E R S

Cybersecurity Insiders riunisce oltre 600.000 professionisti della sicurezza informatica e fornitori di tecnologia all'avanguardia per agevolare la risoluzione intelligente dei problemi e la collaborazione nell'affrontare le sfide più critiche della sicurezza informatica di oggi.

Il nostro approccio si concentra sulla creazione e la cura di contenuti unici che hanno l'obiettivo di educare e informare i professionisti della sicurezza informatica sulle ultime tendenze, soluzioni e best practice in materia di sicurezza informatica. Da studi di ricerca completi e recensioni di prodotti imparziali a e-guide pratiche, webinar coinvolgenti e articoli educativi, ci impegniamo a fornire risorse che forniscano risposte basate sull'evidenza alle complesse sfide della sicurezza informatica di oggi.

Contattaci oggi stesso per scoprire come Cybersecurity Insiders può aiutarti a distinguerti in un mercato affollato e ad aumentare la domanda, la visibilità del brand e la presenza della leadership di pensiero.

Inviaci un'e-mail a info@cybersecurity-insiders.com o visita il sito cybersecurity-insiders.com