

2024

Sicurezza cloud Report



FORTINET®

Introduzione

Oggi è sempre più frequente che le aziende adottino una strategia cloud-first, basando lo sviluppo e il deployment delle applicazioni sul cloud. La scelta di un approccio ibrido o multi-cloud per i diversi casi d'uso e modelli di lavoro della maggior parte delle organizzazioni, ha ampliato notevolmente la superficie d'attacco, rendendo la sicurezza degli ambienti cloud più critica e complessa.

Il report sulla sicurezza cloud 2024, basato su un'indagine condotta su 927 professionisti della cybersecurity in tutto il mondo, offre informazioni essenziali sugli attuali trend della sicurezza cloud. Il report esamina le principali sfide per la protezione di ambienti cloud complessi, le principali soluzioni e strategie adottate dai professionisti della cybersecurity, in che modo questi stanno allocando le loro risorse e quali best practice utilizzano per garantire la sicurezza dei carichi di lavoro cloud.

I risultati principali:

- **Preferenza multi-cloud:** la maggior parte delle organizzazioni (78%) sceglie strategie ibride e multi-cloud per combinare flessibilità, controllo e i singoli vantaggi di vari servizi cloud.
- **Barriere all'adozione del cloud:** i problemi di sicurezza e conformità (59%) costituiscono una delle barriere più significative per accelerare l'adozione di strategie multi-cloud. Le sfide tecniche (52%) e le risorse limitate (49%) rappresentano ostacoli concreti per ottenere visibilità e controllo delle policy in infrastrutture multi-cloud complesse ed evidenziano la necessità di solide competenze di sicurezza del cloud.
- **Carenza di talenti in cybersecurity:** le aziende hanno difficoltà a reperire professionisti qualificati in cybersecurity: il 93% degli intervistati teme di non riuscire a trovare le risorse giuste per proteggere ambienti multi-cloud complessi. Questo influisce direttamente sulla postura di sicurezza e sulle attività strategiche. Questa persistente carenza di competenze nella sicurezza cloud impedisce un'adozione più rapida e diffusa delle strategie multi-cloud.
- **Preferenza per la piattaforma di sicurezza cloud unificata:** il 95% degli intervistati è a favore di un'unica piattaforma per ottimizzare la sicurezza negli ambienti cloud. L'obiettivo è semplificare e automatizzare la gestione della sicurezza, ridurre il divario tra i talenti e rafforzare la sicurezza con un'applicazione coerente delle policy e visibilità, per una migliore gestione dei vari sistemi di sicurezza eterogenei.

Desideriamo ringraziare [Fortinet](#) per il prezioso supporto in questa importante indagine di settore. Ci auguriamo che questo report fornisca una guida pratica che consenta ai leader e agli operatori della cybersecurity di muoversi con efficienza tra le complessità della sicurezza cloud e proteggere l'ambiente cloud della loro organizzazione dall'evoluzione delle minacce informatiche.

Grazie,

Holger Schulze

Fondatore, Cybersecurity Insiders

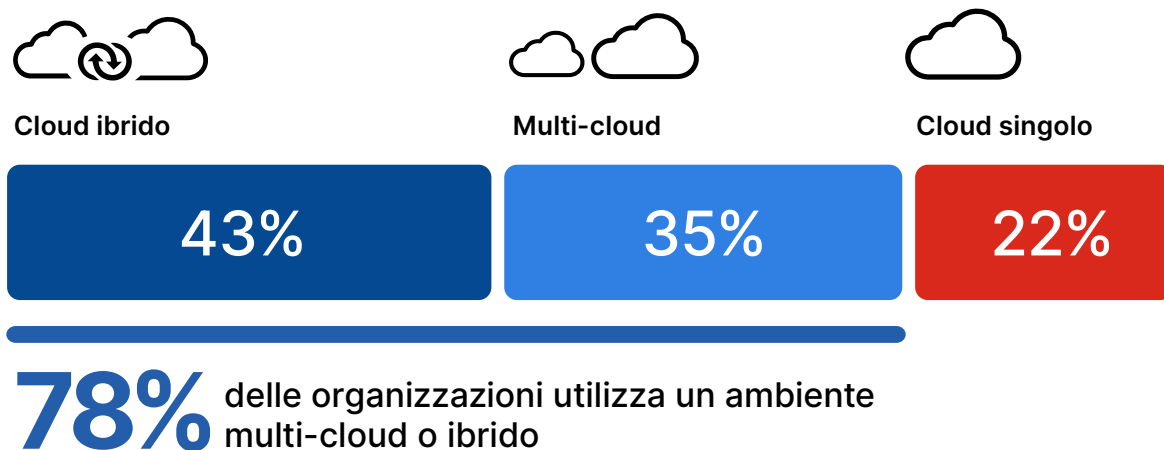
Cybersecurity
INSIDERS

Strategie di distribuzione del cloud

Per massimizzare i vantaggi del cloud computing e ridurre al minimo i relativi rischi, le aziende devono scegliere la giusta strategia di deployment del cloud.

La maggior parte delle organizzazioni (78%) predilige una strategia ibrida o multi-cloud, che integra più deployment in un unico ambiente operativo. Gran parte di queste (43%) utilizza un'infrastruttura ibrida cloud e on-premise. Il 35% delle organizzazioni utilizza una strategia multi-cloud e preferisce sfruttare i punti di forza di più provider di servizi cloud per i diversi casi d'uso. Solo il 22% si affida a un unico cloud provider, perseguendo un approccio mirato che semplifica la gestione ma che può aumentare la dipendenza da un unico fornitore.

► Qual è la strategia primaria della tua organizzazione per l'implementazione del cloud?



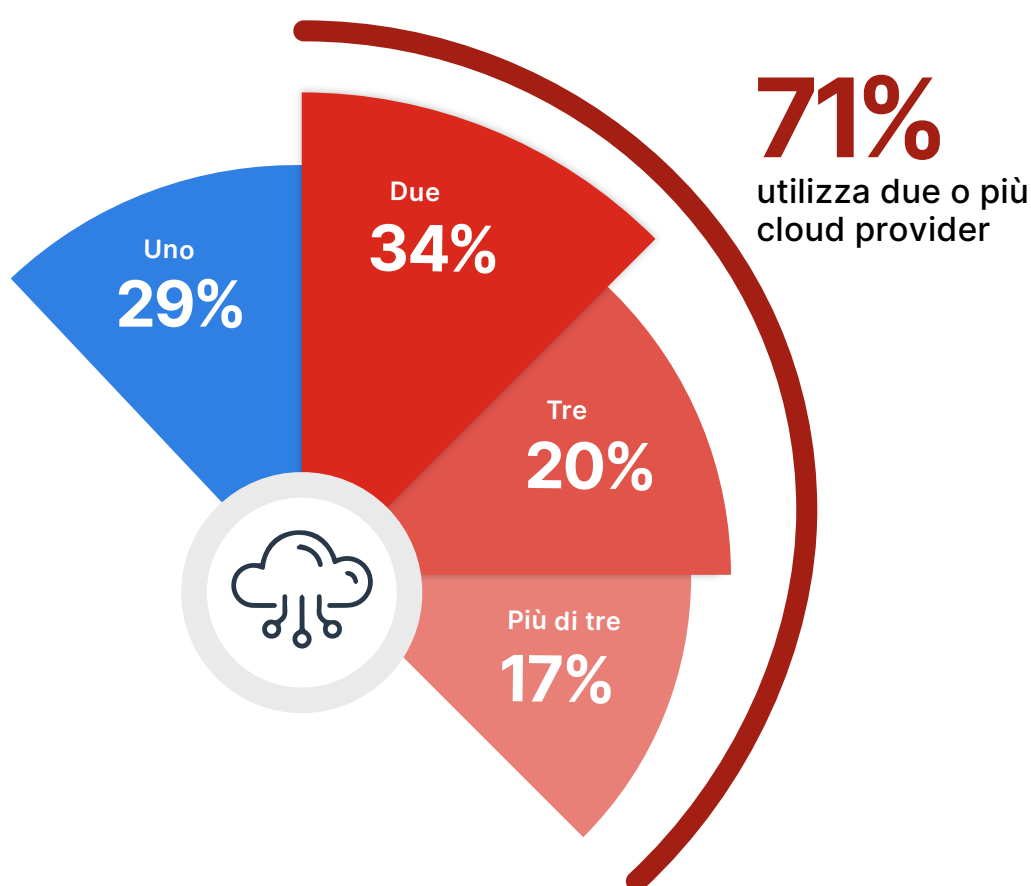
Per gestire al meglio le complessità dei deployment ibridi e multi-cloud, le organizzazioni dovrebbero scegliere un framework di sicurezza integrato che assicuri una protezione continua sull'intero footprint digitale. Questo è essenziale per garantire l'agilità, la scalabilità e la sicurezza necessarie per una difesa solida contro minacce informatiche in continua evoluzione.

Adozione multi-cloud

Il numero di cloud provider utilizzati da un'organizzazione è determinante per la flessibilità operativa, la gestione dei rischi e la complessità delle implementazioni di sicurezza. La maggior parte delle organizzazioni (71%) utilizza due o più provider di servizi cloud, con l'obiettivo di bilanciare flessibilità, controllo e i singoli vantaggi di ogni provider di servizi cloud. L'aumento di 2 punti percentuali rispetto all'indagine dello scorso anno indica il crescente orientamento verso le strategie multi-cloud, generato dalla necessità di servizi cloud specialistici, disponibilità regionale e ridondanza.

È interessante notare che solo il 29% delle organizzazioni usa un unico cloud provider, privilegiando quindi la semplicità e possibilmente una partnership strategica con un unico cloud provider.

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



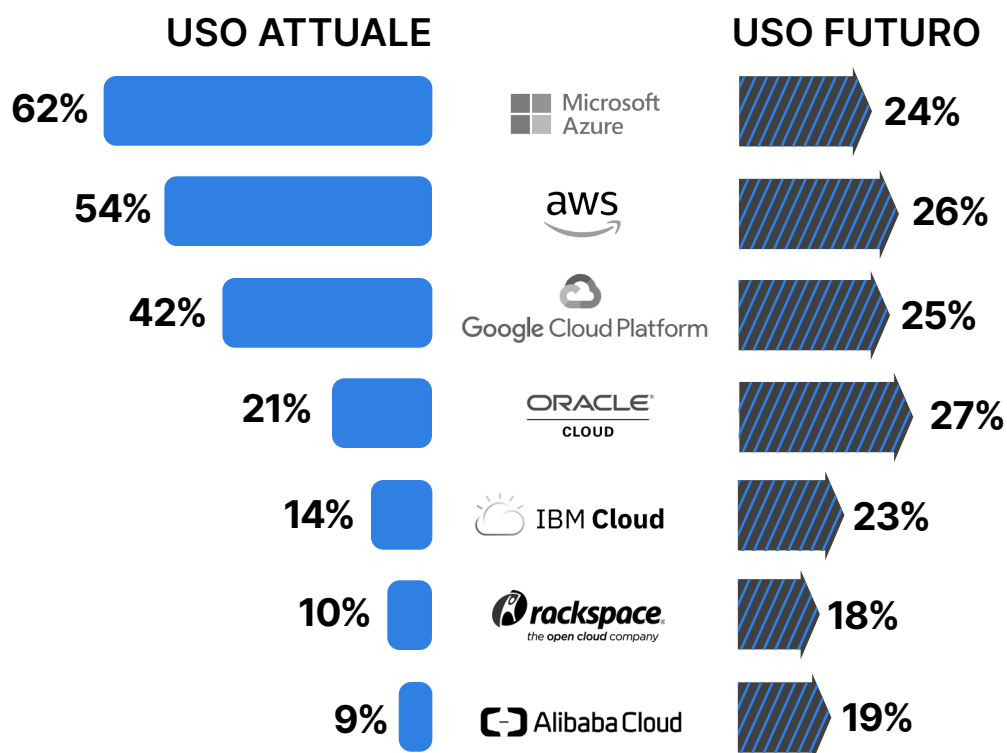
Per proteggere più ambienti cloud le organizzazioni dovrebbero scegliere un approccio integrato e neutrale al cloud, che garantisca policy di sicurezza coerenti e visibilità sull'intero footprint digitale, semplificando e rafforzando i meccanismi di difesa contro minacce informatiche sempre più sofisticate.

Provider cloud preferiti

Abbiamo poi intervistato i professionisti della cybersecurity in merito al loro utilizzo attuale e futuro dei cloud provider, per comprendere meglio le nuove dinamiche di mercato nell'ecosistema cloud. Microsoft Azure si riconferma leader di mercato, con il 62% delle organizzazioni che utilizzano attualmente i suoi servizi, seguita da Amazon Web Services (AWS) con il 54%. È quindi evidente una netta preferenza per questi affermati colossi del cloud.

I risultati dell'indagine rivelano anche un forte interesse in termini di adozione futura per tutti i provider, in particolare Oracle Cloud e Google Cloud Platform, con il 27% e il 25% degli intervistati che prevedono di adottare questi servizi. Il trend è dunque quello di un'adozione del cloud sempre più diversificata.

► Quali provider IaaS cloud utilizzi attualmente o prevedi di utilizzare in futuro? (seleziona tutte le opzioni valide)



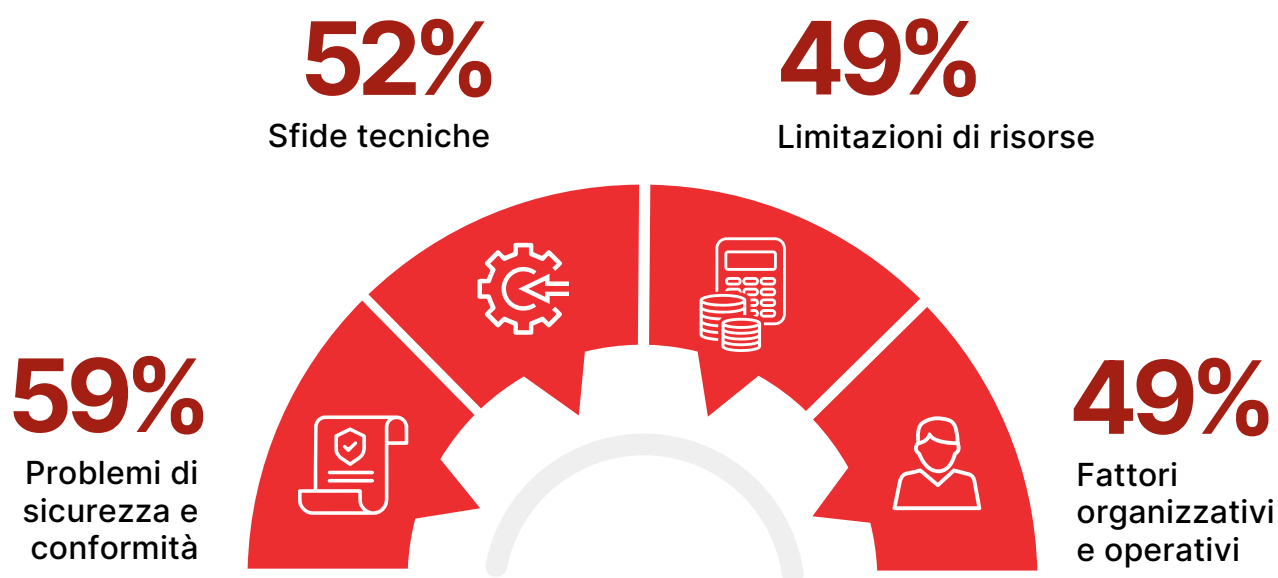
Superare le barriere all'adozione del cloud

Individuare e capire quali barriere ostacolano un'adozione più rapida e diffusa del cloud è essenziale per consentire alle aziende di gestire in modo efficace le complessità della transizione verso le soluzioni cloud.

In primo piano ci sono i problemi di sicurezza e conformità: il 59% degli intervistati li identifica come un ostacolo primario. Questo evidenzia l'importanza di garantire che la sicurezza e la conformità siano parte integrante dell'adozione cloud. Subito dopo si collocano le sfide tecniche con il 52%, a riprova del fatto che la facilità di adozione del cloud non è priva di ostacoli.

Il 49% degli intervistati menziona le risorse limitate, tra cui la mancanza di competenze del personale e le limitazioni del budget, sottolineando la necessità di adeguati investimenti in risorse umane e finanziarie a supporto delle iniziative cloud. Le barriere organizzative e operative (49%) indicano che il cloud computing non è solo una nuova tecnologia, ma anche un nuovo modello operativo che offre metodi di lavoro innovativi e richiede il coinvolgimento del management per gestire la potenziale resistenza al cambiamento.

► Quali sono le principali barriere all'adozione del cloud nella tua organizzazione? (seleziona tutte le opzioni valide)



Ulteriori risposte includono:

Problemi legati ai servizi cloud 28% | Problemi e aspetti legali relativi ai provider 27%

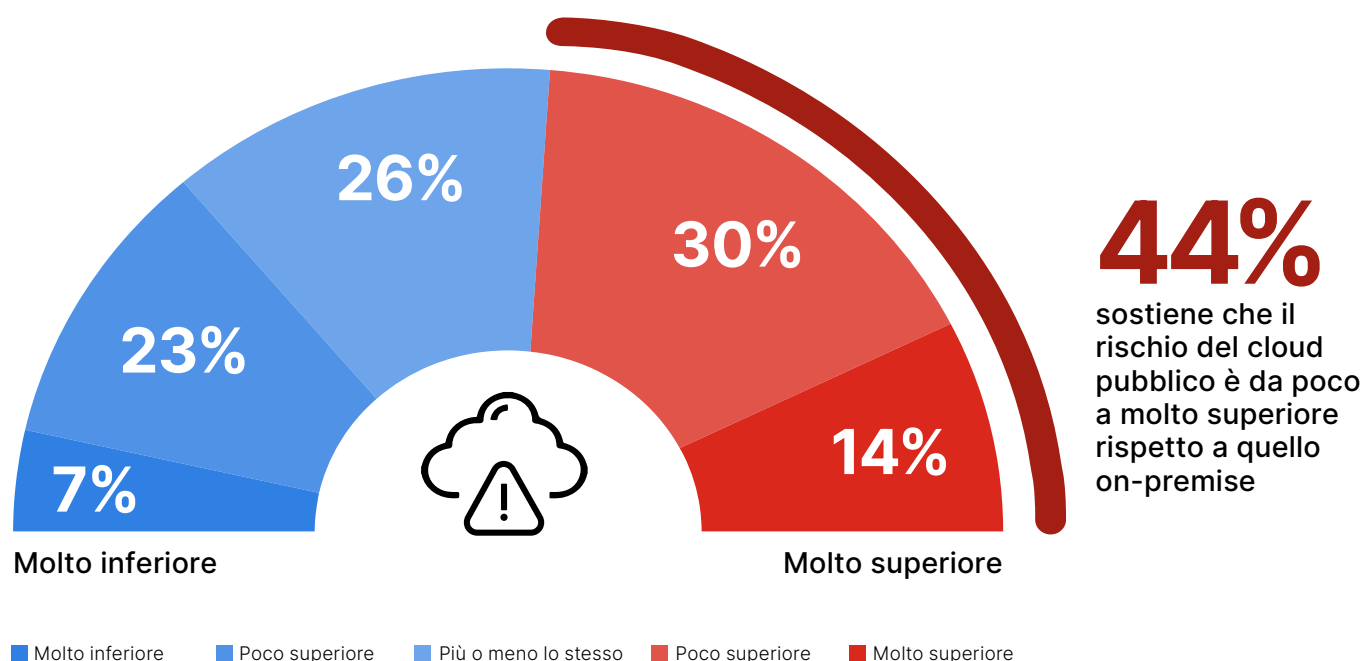
La percezione dei rischi per la sicurezza cloud

La valutazione dei rischi relativi alle violazioni della sicurezza negli ambienti cloud pubblici rivela forti dubbi sui rischi e le sfide esclusive della sicurezza nel cloud computing, rispetto agli ambienti on-premise.

Il 44% degli intervistati percepisce un rischio di violazioni della sicurezza negli ambienti cloud pubblici superiore rispetto agli ambienti IT on-premise tradizionali, con il 30% che lo considera leggermente più elevato e il 14% significativamente più elevato.

Al contrario, il 30% dei partecipanti ritiene che il rischio sia minore negli ambienti di cloud pubblico, e ciò indica fiducia nelle misure e nei progressi della sicurezza dei cloud provider. Un significativo 26% degli intervistati ritiene che il rischio sia uguale, indicando che sebbene il cloud introduca nuove dinamiche, le sfide base della sicurezza si ripresentano in tutti gli ambienti.

► Rispetto ai tradizionali ambienti IT on-premise, pensi che il rischio di violazioni della sicurezza in un ambiente cloud pubblico sia maggiore o minore?



Il cloud pubblico offre alle organizzazioni l'opportunità di adottare un approccio alla sicurezza proattivo e automatizzato. Adottando una mentalità "security-by-design", le aziende possono attenuare efficacemente i rischi e sfruttare la scalabilità, la flessibilità e l'innovazione offerte dal cloud.

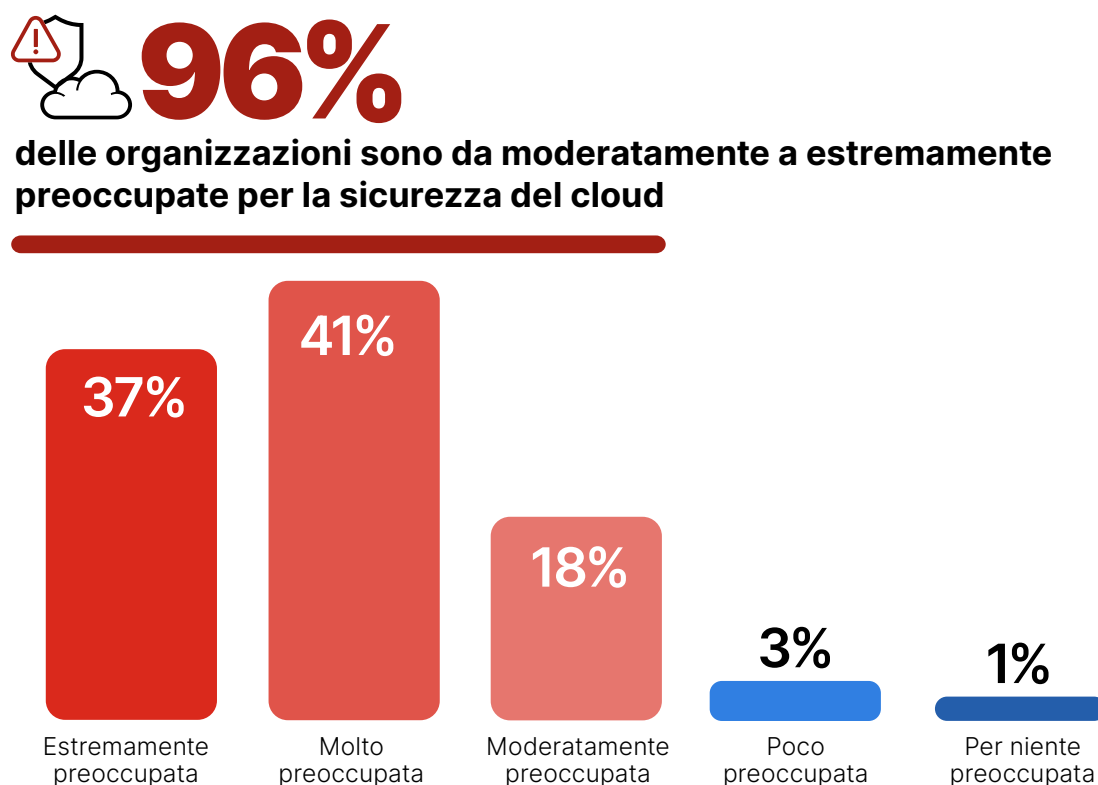
Preoccupazioni per la sicurezza del cloud

Il livello di preoccupazione per la sicurezza del cloud pubblico è un chiaro indicatore della percezione e del grado di preparazione della comunità della cybersecurity verso potenziali rischi e minacce.

Nonostante la crescente adozione del cloud, le preoccupazioni per la sua sicurezza restano elevate: una significativa maggioranza del 96% esprime alti livelli di preoccupazione, con il 37% estremamente preoccupato e il 41% molto preoccupato per la sicurezza del cloud pubblico. L'alto grado di preoccupazione per la cybersecurity, che si è mantenuto costante negli anni, ostacola in modo significativo una più rapida adozione del cloud, perché le organizzazioni devono affrontare rischi percepiti e complessità della protezione degli ambienti cloud. Solo una minoranza (22%) si ritiene moderatamente o per nulla preoccupata, indicando un forte consenso sull'importanza di solide misure di sicurezza nei deployment di cloud pubblico.

Questi dati sono in linea con i risultati precedenti, in cui il 44% degli intervistati ha percepito un rischio maggiore di violazioni della sicurezza nei cloud pubblici rispetto agli ambienti tradizionali on-premise. Ciò conferma che, nonostante i numerosi vantaggi e la crescente diffusione del cloud computing, la sicurezza rimane una preoccupazione assoluta.

► In che misura ti preoccupa la sicurezza dei cloud pubblici?



Per affrontare questi problemi, le organizzazioni non solo devono mantenere un approccio "security-by-design", ma anche investire nel monitoraggio continuo, nell'intelligence sulle minacce e nelle capacità di risposta agli incidenti specifiche per gli ambienti cloud. L'adozione di soluzioni di sicurezza avanzate e lo sviluppo di forti collaborazioni con i cloud provider possono contribuire ad attenuare il rischio percepito e le preoccupazioni associate al cloud pubblico, garantendo un'infrastruttura cloud sicura e resiliente.

Sfide delle operazioni di sicurezza cloud

La gestione delle operazioni di sicurezza cloud quotidiane è una sfida dai molteplici aspetti per le organizzazioni e richiede un delicato equilibrio tra fattori tecnologici, procedurali e umani. La sicurezza e la privacy dei dati sono la prima preoccupazione, con il 58% degli intervistati che considera fondamentale proteggere le informazioni sensibili e prevenire le fughe di dati dal cloud. Questo sottolinea l'importanza di una governance dei dati e di pratiche di crittografia efficaci. Al secondo posto, con il 55%, si posiziona la gestione delle configurazioni che evidenzia la complessità e i potenziali rischi associati alle configurazioni del cloud: una singola configurazione errata può esporre le aziende a rischi significativi per la sicurezza.

Il controllo degli accessi e la gestione delle identità sono un'altra importante sfida riferita dal 54% dei partecipanti, che segnalano la necessità di un controllo rigoroso degli accessi e dei privilegi degli utenti per evitare accessi non autorizzati. Il rilevamento e la risposta alle minacce (50%) e la sicurezza degli endpoint (45%) indicano la continua attività per identificare e attenuare le minacce alla sicurezza in tempo reale e proteggere l'enorme quantità dei dispositivi che accedono ai servizi cloud. La gestione delle policy e della conformità (45%) e la gestione della sicurezza cloud (45%) evidenziano le difficoltà nel garantire policy di sicurezza coerenti tra gli ambienti e nell'allineare le funzionalità della sicurezza cloud con le soluzioni on-premise.

► Quali sono le tue sfide principali nella gestione delle operazioni di sicurezza cloud quotidiane? (seleziona tutte le opzioni valide)



Per risolvere queste sfide nelle operazioni della sicurezza cloud, le aziende devono prioritizzare una strategia di sicurezza unificata basata su automazione, analisi avanzate e piattaforme di sicurezza integrate per ottimizzare la sicurezza dei dati, l'applicazione delle policy, la gestione degli accessi e il rilevamento e la risposta alle minacce. Promuovere lo sviluppo di competenze di sicurezza cloud-native all'interno dei team e una cultura di consapevolezza della sicurezza può migliorare ulteriormente la capacità di un'organizzazione di gestire efficacemente le operazioni di sicurezza del cloud.

Ulteriori risposte includono:

Shadow IT e utilizzo non autorizzato di app 36% | Integrazione e automazione del cloud 35% | Agilità e complessità operativa 32% | Allocazione delle risorse 30% | Pratiche DevSecOps 28%

Sfide per la sicurezza del multi-cloud

Gli ambienti multi-cloud aumentano notevolmente le complessità e le sfide connesse alla protezione dei carichi di lavoro sul cloud. Garantire la protezione dei dati e la privacy in ogni ambiente è stata valutata la sfida più importante per la sicurezza multi-cloud, con il 55% degli intervistati che l'ha indicata come una preoccupazione. Questo riflette l'importanza assegnata in precedenza alla sicurezza dei dati e alla privacy come questioni operative critiche, a conferma della maggiore complessità dovuta alla distribuzione dei dati su più ambienti cloud.

Il 51% dei partecipanti ha identificato come una delle principali sfide la necessità di competenze adeguate per implementare e gestire le soluzioni in tutti gli ambienti cloud, in linea con la richiesta segnalata in precedenza di avere competenze di sicurezza cloud-native per gestire al meglio il complesso scenario della sicurezza cloud. Capire come si integrano le diverse soluzioni e quali sono le opzioni di integrazione dei servizi sono aspetti cruciali rispettivamente per il 47% e il 44% degli intervistati.

Queste risposte segnalano quanto sia complesso ottenere una perfetta integrazione e interoperabilità tra i diversi ambienti cloud, un fattore critico per assicurarsi una solida sicurezza ed efficienza operativa. La sfida legata alla gestione dei costi delle diverse soluzioni, riferita dal 42% degli intervistati, riflette inoltre il bilanciamento operativo e finanziario richiesto da una strategia multi-cloud.

► Quali sono le tue maggiori sfide per proteggere gli ambienti multi-cloud? (seleziona tutte le opzioni valide)



Per affrontare queste sfide in modo efficace, è necessario avvalersi di soluzioni di sicurezza integrate che offrano visibilità e controllo sugli ambienti multi-cloud, supportando standard coerenti di protezione dei dati e della privacy. Le partnership con fornitori che offrono funzionalità di sicurezza multi-cloud complete e lo sviluppo di maggiori competenze aziendali possono aiutare le organizzazioni a semplificare la protezione delle architetture multi-cloud. Questo approccio non solo riduce le sfide indicate, ma sfrutta anche l'intero potenziale degli ambienti multi-cloud per migliorare l'agilità, la scalabilità e l'innovazione.

Ulteriori risposte includono:

Fornire un accesso integrato agli utenti in base alle loro credenziali 38% | Perdita di visibilità e controllo 37% | Selezione del giusto set di servizi 36% | Tenere il passo con il ritmo del cambiamento 33%

Carenza di talenti nella cybersecurity

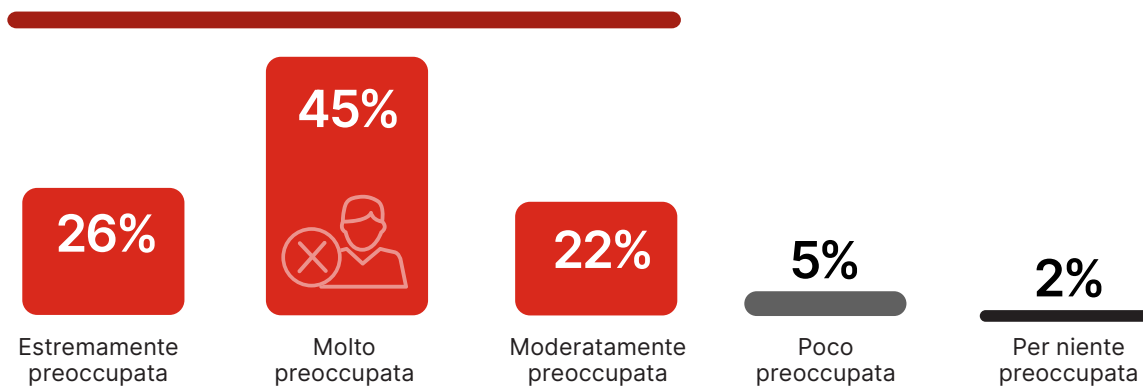
Un problema critico del settore, come visto per le sfide legate alla sicurezza degli ambienti multi-cloud, è la costante carenza di professionisti qualificati per la protezione degli ambienti multi-cloud complessi.

Un'ampia maggioranza del 93% degli intervistati esprime preoccupazione per la carenza di professionisti qualificati nel settore della cybersecurity. Questo livello di apprensione indica una piena consapevolezza del divario tra la crescente domanda di talenti qualificati in cybersecurity e la disponibilità di risorse, con rischi per le vulnerabilità della sicurezza e le sfide operative in un panorama IT sempre più complesso.

► Quanto ti preoccupa la carenza nell'intero settore di professionisti qualificati in cybersecurity?

93%

delle organizzazioni sono da moderatamente a estremamente preoccupate per la carenza nell'intero settore di professionisti qualificati in cybersecurity



Il 74% degli intervistati conferma che la propria organizzazione sta attualmente riscontrando una carenza di talenti nel campo della cybersecurity. Questo dato quantifica in che misura la carenza di competenze influisce sulle operazioni di sicurezza quotidiane e sulle iniziative strategiche delle organizzazioni.

► La tua organizzazione sta riscontrando una carenza di talenti nel campo della cybersecurity?



Per mitigare l'impatto di questa carenza di competenze in cybersecurity, le organizzazioni devono puntare su un approccio integrato che spazi dalla promozione di partnership con le istituzioni accademiche per formare nuovi talenti, fino all'investimento in programmi di formazione e sviluppo per coltivare i talenti interni e adattarsi ai nuovi requisiti della sicurezza cloud. È anche necessario valutare l'introduzione di soluzioni di sicurezza unificate in sostituzione delle singole soluzioni mirate, che integrino l'intelligenza artificiale e riducano la complessità operativa per ridurre il divario di competenze, migliorare il rilevamento delle minacce, le capacità di risposta e la postura di sicurezza complessiva.

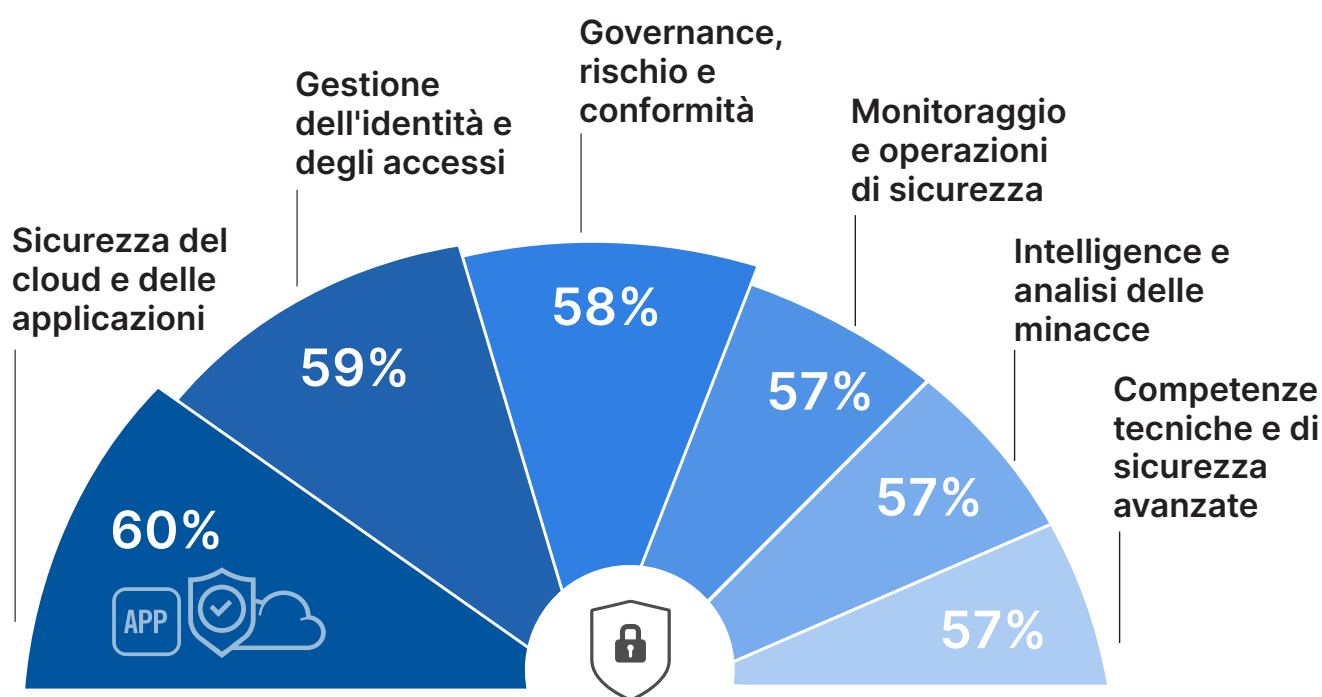
Competenze critiche per la cybersecurity

In questo panorama di evidente carenza di talenti nella cybersecurity, abbiamo chiesto quali fossero le competenze specifiche di cybersecurity più critiche per risolvere le attuali sfide di sicurezza.

Al primo posto troviamo le competenze per la sicurezza del cloud e delle applicazioni, ritenute critiche dal 60% degli intervistati. Questo spiega la più rapida migrazione verso i servizi cloud e la necessità di adottare pratiche di sicurezza solide nello sviluppo e nel deployment delle applicazioni. A seguire, la gestione delle identità e degli accessi (IAM) è essenziale per il 59% delle organizzazioni, a conferma di quanto sia complesso proteggere l'accesso degli utenti in ambienti IT sempre più distribuiti.

Il 58% degli intervistati considera la governance, il rischio e la conformità (GRC) una competenza importante, assegnando un ruolo essenziale alla conformità normativa e ai framework di gestione del rischio nell'attuale panorama delle minacce informatiche. Il monitoraggio e le operazioni di sicurezza, l'intelligence sulle minacce e le competenze tecniche avanzate in sicurezza, tutti e tre al 57%, dimostrano un uguale livello di attenzione per il rilevamento proattivo delle minacce, l'identificazione degli avversari informatici e l'applicazione di tecnologie avanzate per una solida postura di sicurezza.

► Quali sono le competenze di sicurezza più importanti richieste nella tua organizzazione? (seleziona tutte le opzioni valide)



Ulteriori risposte includono:

Risposta agli incidenti e analisi forense 55% | Comunicazione e strategia 39% | Formazione e consapevolezza 38%

Tendenze di bilancio per la sicurezza cloud

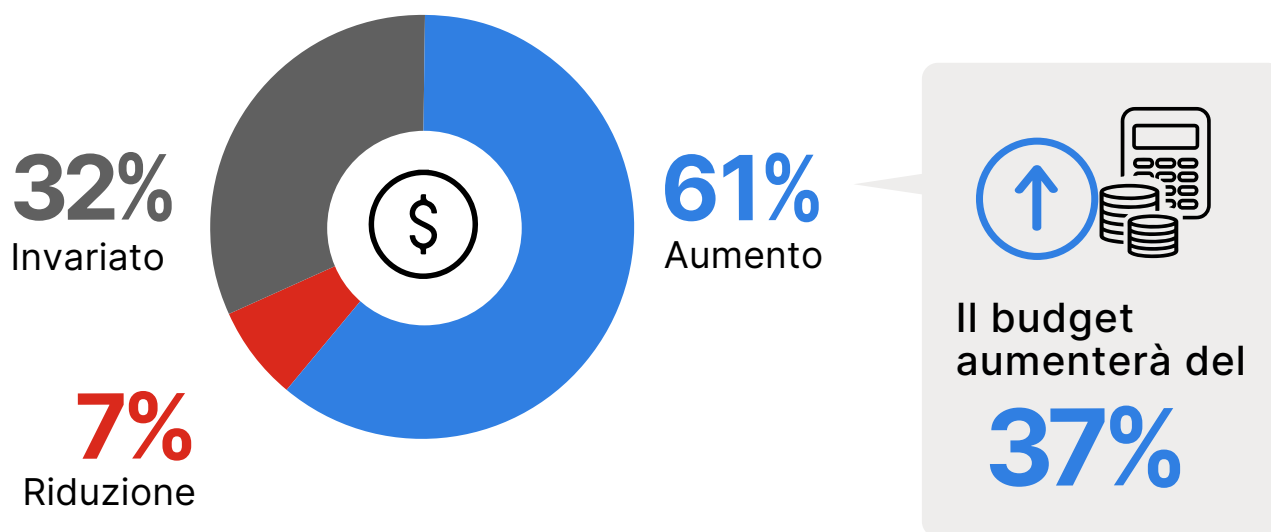
L'allocazione delle risorse per la sicurezza cloud è un indicatore chiave delle priorità aziendali e di quanto sia percepita importante la sicurezza del cloud, rispetto all'evoluzione delle minacce informatiche e ai progressi tecnologici.

Un significativo 61% degli intervistati prevede un aumento del budget destinato alla sicurezza cloud nei prossimi 12 mesi. Questa sostanziale maggioranza riconosce le crescenti sfide della cybersecurity e la necessità di rafforzare le misure di sicurezza negli ambienti cloud, con un conseguente aumento del budget per la sicurezza cloud del 37%.

La volontà di investire fino al 37% in più nella sicurezza cloud dimostra che in un contesto aziendale sempre più orientato al cloud, sono considerati essenziali dei meccanismi di difesa più solidi per salvaguardare i dati sensibili e mantenersi conformi agli standard normativi.

Contestualmente, un terzo delle organizzazioni (32%) prevede che il budget per la sicurezza cloud rimarrà invariato. Solo una piccola parte, il 7%, prevede una diminuzione del budget destinato alla sicurezza cloud.

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

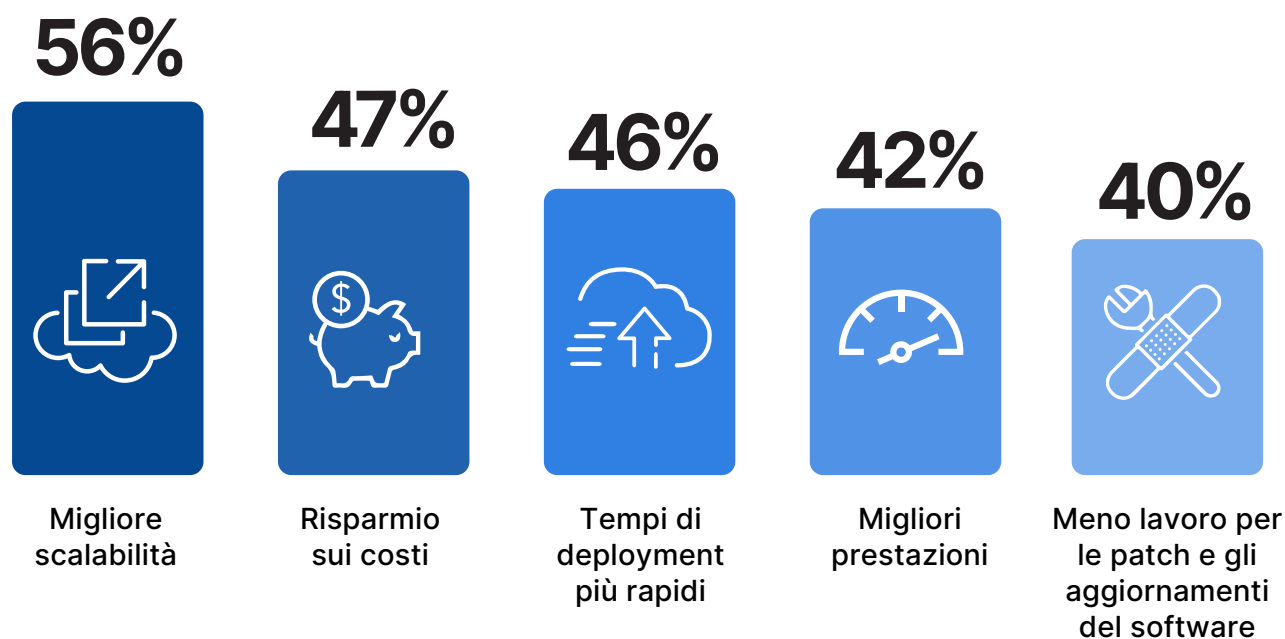


Vista la predominante tendenza all'incremento degli investimenti in sicurezza cloud, le aziende dovrebbero allocare strategicamente più risorse per le aree di maggior rischio e impatto potenziale, come il rilevamento avanzato delle minacce, la gestione di identità e accessi e l'automazione della sicurezza. Questo approccio non solo prepara le aziende a contrastare le minacce informatiche più sofisticate, ma migliora anche la loro postura di sicurezza generale grazie alle ultime innovazioni tecnologiche nel campo della sicurezza cloud.

Adottare le soluzioni di sicurezza basate sul cloud

La scelta di adottare soluzioni di sicurezza basate sul cloud nasce da una serie di fattori in linea con gli obiettivi di agilità, efficienza e maggiore protezione delle organizzazioni. La necessità di una migliore scalabilità, indicata dal 56% degli intervistati, evidenzia la capacità del cloud di adattarsi in modo dinamico alle fluttuazioni della domanda. I risparmi sui costi e la rapidità di deployment, rispettivamente al 47% e al 46%, sottolineano i vantaggi economici e operativi che spingono le aziende verso le soluzioni di sicurezza cloud. Il miglioramento delle prestazioni (42%) e la riduzione delle attività manuali di patching e aggiornamenti del software (40%) rinforzano la spinta verso soluzioni di sicurezza basate sul cloud, soprattutto in un contesto di perenne carenza di competenze in cybersecurity.

► Quali sono i fattori principali che orientano la scelta di soluzioni di sicurezza basate sul cloud? (seleziona tutte le opzioni valide)



Le organizzazioni che stanno valutando soluzioni di sicurezza basate sul cloud dovrebbero prioritizzare la scalabilità, l'efficienza dei costi e la rapidità di deployment per sfruttare i vantaggi operativi ed economici del cloud. Concentrarsi su soluzioni che offrono una gestione semplificata delle policy e una conformità continua può migliorare ulteriormente la postura di sicurezza, aumentando la resilienza all'evoluzione delle minacce e delle normative.

Ulteriori risposte includono:

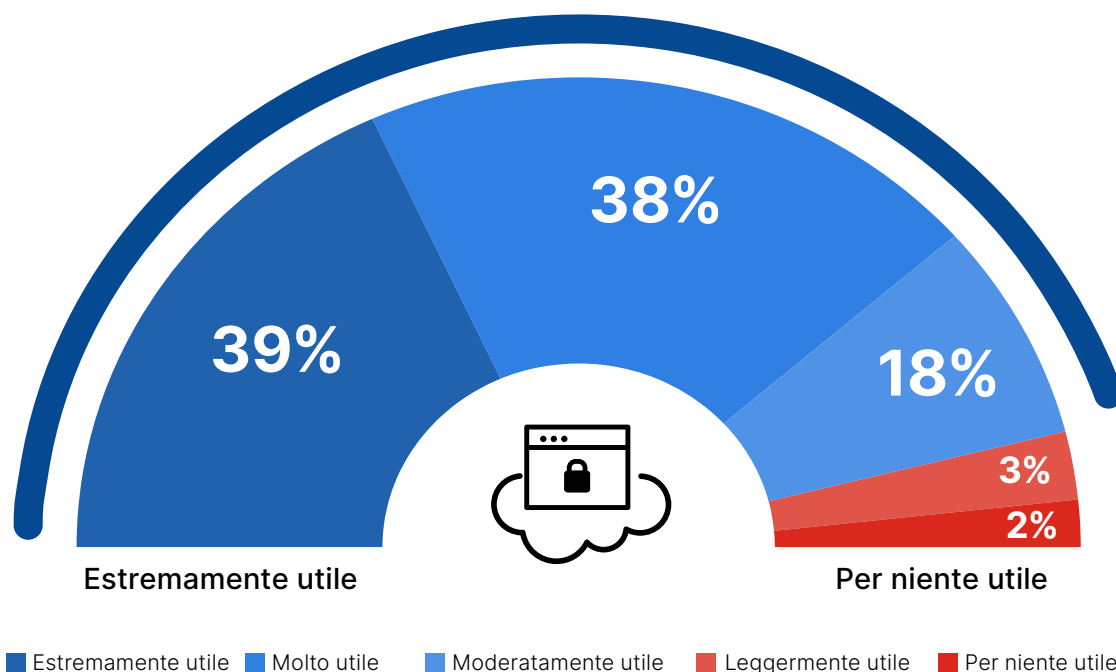
Gestione più semplice delle policy 39% | Migliore uptime 38% | Soddisfare le aspettative di conformità cloud 34% | Migliore visibilità sull'attività degli utenti e sul comportamento del sistema 33% | Necessità di accedere alle app in modo sicuro da qualunque luogo 32% | I nostri dati/carichi di lavoro risiedono nel cloud 28% | Riduzione dell'ingombro delle appliance nelle filiali 27%

Piattaforma di sicurezza cloud unificata

Considerate la complessità, le criticità operative e le sfide già segnalate sulla scarsità di competenze, è chiaro perché le aziende sono alla ricerca di una piattaforma di sicurezza unificata che consenta di semplificare e consolidare la gestione della sicurezza nei diversi ambienti cloud. Per il 95% degli intervistati, una piattaforma di questo tipo sarebbe vantaggiosa per proteggere i dati in modo coerente e completo in tutti i cloud.

- **Quanto sarebbe utile disporre di un'unica piattaforma di sicurezza cloud e un unico dashboard in cui configurare tutte le policy necessarie per proteggere i dati in modo coerente e completo nell'intera area cloud?**

95% dei professionisti ritiene che l'utilizzo di un'unica piattaforma di sicurezza cloud con un unico dashboard sia da moderatamente a estremamente utile



La richiesta di un'unica piattaforma di sicurezza cloud integrata è in linea con l'orientamento del settore verso l'unificazione delle piattaforme, con l'obiettivo di migliorare l'efficacia della sicurezza, semplificare l'integrazione e ridurre i costi di gestione. Questo è l'unico approccio efficace per affrontare la carenza di talenti nella cybersecurity e per mitigare attacchi sempre più sofisticati e automatizzati. Una piattaforma unificata di questo tipo riduce il carico operativo generato dall'uso di più interfacce di sicurezza e migliora la sicurezza generale grazie a un'applicazione coerente delle policy e alla visibilità completa su tutti gli ambienti cloud.

Scegliere il cloud in sicurezza: Strategie essenziali per la sicurezza del cloud

Nell'attuale scenario in rapida evoluzione del cloud, le organizzazioni di tutte le dimensioni hanno l'imperativo di garantirne la sicurezza. Questa guida illustra le best practice essenziali per proteggere gli ambienti cloud, dall'unificazione delle piattaforme di sicurezza all'investimento in competenze specialistiche, per far fronte alle sofisticate minacce future.



ADOTTARE UNA PIATTAFORMA DI SICUREZZA UNIFICATA:

Centralizzare il controllo e la visibilità della sicurezza su tutti gli ambienti cloud per semplificare le operazioni e migliorare la visibilità è la strategia preferita dal 95% delle organizzazioni.



SCEGLIERE UNA SICUREZZA INDIPENDENTE DAL CLOUD:

Con il 78% degli intervistati che utilizza ambienti ibridi o multi-cloud, è fondamentale sviluppare strategie adatte alle specifiche sfide di questi ambienti e in grado di garantire policy e applicazione della sicurezza coerenti.



AUTOMATIZZARE LA GESTIONE DI POLICY E CONFORMITÀ:

Implementare sistemi per automatizzare e semplificare le policy di sicurezza negli ambienti cloud e soddisfare in modo coerente i requisiti normativi.



DARE PRIORITÀ ALLA PROTEZIONE DEI DATI:

Implementare una solida governance e crittografia dei dati per proteggere le informazioni sensibili in tutti i servizi cloud, risolvendo la sfida della sicurezza segnalata dal 58% delle organizzazioni.



MIGLIORARE LA GESTIONE DELLA CONFIGURAZIONE:

Gestire attivamente le configurazioni del cloud per evitare configurazioni errate e ridurre l'esposizione alle vulnerabilità della sicurezza.



RAFFORZARE IL CONTROLLO DEGLI ACCESSI:

Adottare una gestione rigorosa di identità e accessi per implementare i principi di Zero Trust e ridurre il rischio di accessi non autorizzati.



POTENZIARE IL RILEVAMENTO E LA RISPOSTA ALLE MINACCE:

Sfruttare le analisi avanzate e le funzionalità di risposta automatizzata per identificare e ridurre le minacce in tempo reale.



INVESTIRE IN COMPETENZE DI SICUREZZA CLOUD-NATIVE:

Con il 93% degli intervistati che esprime grande preoccupazione per la scarsità di competenze in cybersecurity, è essenziale sviluppare competenze specifiche in sicurezza cloud all'interno del proprio team per operare meglio nel complesso panorama della sicurezza cloud.

Metodologia e dati demografici

Il Report sulla sicurezza del cloud 2024 si basa su un'indagine globale condotta nel febbraio 2024 su 927 professionisti di cybersecurity, per scoprire come stanno adottando il cloud le aziende che hanno scelto di usarlo, come vedono l'evoluzione della sicurezza del cloud e quali sono le best practice a cui i leader della cybersecurity IT danno priorità nel passaggio al cloud. Gli intervistati spaziano dai dirigenti tecnici ai professionisti della sicurezza IT, rappresentando così uno spaccato ben bilanciato di organizzazioni di varie dimensioni e di diversi settori.

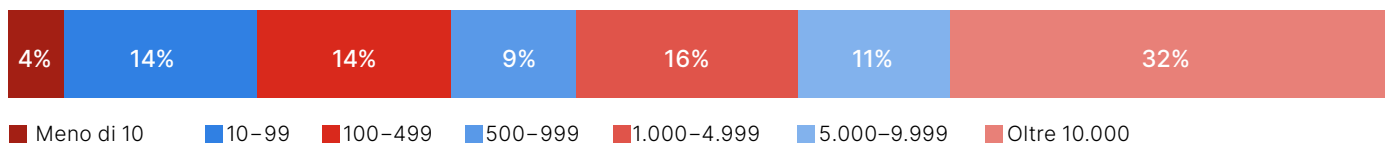
LIVELLO DI CARRIERA



REPARTO



DIMENSIONE AZIENDA



SETTORE



Riutilizzo dei contenuti

Incoraggiamo il riutilizzo dei dati, dei grafici e dei testi pubblicati in questo report come previsto dalla presente [Creative Commons Attribution 4.0 International License](#). È possibile condividere e fare un uso commerciale di questo lavoro a condizione che vengano attribuite al report le informazioni previste dai termini della licenza. Ad esempio: "2024 Cloud Security Report di Cybersecurity Insiders e Fortinet."



Fortinet (NASDAQ: FTNT) protegge le aziende, i provider di servizi e le organizzazioni governative più grandi al mondo. Fortinet offre ai suoi clienti visibilità e controllo completi su una superficie di attacco in costante espansione, nonché capacità di soddisfare requisiti di performance sempre più elevati, oggi e in futuro. Solo la piattaforma Fortinet Security Fabric è in grado di risolvere le sfide di sicurezza più critiche e di proteggere i dati nell'intera infrastruttura digitale, siano essi reti, applicazioni, ambienti multi-cloud o edge. Fortinet è al primo posto tra le aziende con il maggior numero di appliance di sicurezza fornite in tutto il mondo e oltre 730.000 clienti scelgono Fortinet per proteggere la loro azienda.

www.fortinet.com

Cybersecurity

I N S I D E R S

Cybersecurity Insiders si avvale di oltre 600.000 professionisti della sicurezza IT e vendor di tecnologie leader mondiali per facilitare la risoluzione intelligente dei problemi e la collaborazione nel contrastare le più complesse sfide della cybersecurity di oggi.

La nostra strategia consiste nel creare e curare contenuti esclusivi e realizzati per informare i professionisti della cybersecurity sulle ultime tendenze, soluzioni e best practice. Puntiamo a fornire risorse che rispondano in maniera comprovata alle complesse sfide odierne della cybersecurity, da studi di ricerca completi e recensioni imparziali di prodotti fino a guide pratiche, coinvolgenti webinar e articoli educativi.

Contattaci oggi per scoprire in che modo Cybersecurity Insiders può aiutarti a emergere in un mercato competitivo e ad aumentare la domanda, la visibilità del brand e la tua leadership di pensiero.

Invia un'email a info@cybersecurity-insiders.com o visita il sito cybersecurity-insiders.com