

Sicurezza fisica di livello enterprise nell'era del cloud

Approfondimenti basati sui dati relativi
a installazione, governance e strategie
cloud a livello enterprise

Approfondimenti dal sondaggio sullo stato del settore
della sicurezza fisica 2026





Sommario

Capitolo 1

Non esiste un unico percorso verso il cloud a livello enterprise 4

Capitolo 2

L'adozione del cloud è una strategia, non una preferenza 5

Capitolo 3

Su scala enterprise, l'affidabilità viene prima della comodità 6

Capitolo 4

Le organizzazioni di livello enterprise privilegiano la stabilità rispetto alle discontinuità operative 8

"La decisione di adottare il cloud per le applicazioni di sicurezza fisica nasce dalla necessità di scalabilità e flessibilità, per poter ampliare le risorse senza investimenti significativi in infrastrutture on-premise."

– Intervistato IT, azienda del settore retail, Brasile
(da 1001 a 10.000 dipendenti), cliente Genetec



Non esiste un unico percorso verso il cloud a livello enterprise

Le dimensioni cambiano tutto. Le organizzazioni cosiddette "enterprise" gestiscono centinaia di sedi, cicli di vita tecnologici lunghi, normative rigorose e responsabilità a lungo termine che vanno ben oltre la fase iniziale di installazione. Ciò che funziona per un'azienda di 50 persone potrebbe non essere adatto per un'organizzazione con 10.000 dipendenti. La realtà è che ottimizzare la sicurezza fisica nel cloud non è un passaggio semplice e immediato per gli ambienti enterprise.

In sintesi? L'adozione del cloud non è una corsa verso un unico risultato finale. Le organizzazioni di livello enterprise affrontano complessità specifiche, si evolvono a velocità diverse e devono mantenere la responsabilità nel tempo.

I dati del Sondaggio sullo stato del settore della sicurezza fisica di Genetec confermano questo scenario. Le organizzazioni di grandi dimensioni non scelgono di vincolarsi a un unico modello di deployment. Vogliono sistemi che supportino supervisione, resilienza e controllo a lungo termine, con la flessibilità necessaria per adattarsi alle esigenze nel tempo.

Per queste organizzazioni, il cloud è un modello operativo per coordinare ed evolvere ambienti complessi su larga scala. Per queste organizzazioni, il cloud è un modello operativo per coordinare ed evolvere ambienti complessi su larga scala.



CONCETTI CHIAVE

Le organizzazioni di livello enterprise operano con più modelli di deployment della sicurezza fisica in parallelo.

Le decisioni sul cloud privilegiano supervisione, cybersecurity e fiducia a lungo termine rispetto a velocità o semplicità.

Su scala enterprise, le installazioni ibride e on-premise sono persistenti e non rappresentano una fase transitoria.

L'adozione del cloud è una strategia, non una preferenza

Non esiste un modello unico per la sicurezza fisica enterprise.

I risultati del sondaggio, raccolti da intervistati di organizzazioni con oltre 1000 dipendenti, mostrano che sono ancora necessari modelli di deployment diversificati. Le configurazioni ibride e connesse al cloud sono sempre più diffuse. Tuttavia, i sistemi on-premise non stanno scomparendo, nemmeno tra le organizzazioni con piani cloud a lungo termine ben definiti.

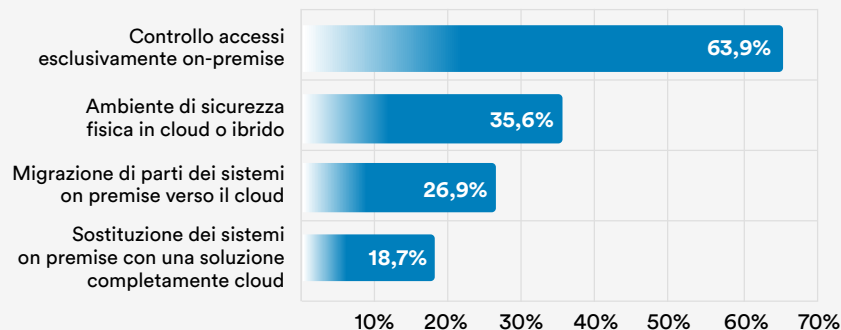
I dati non evidenziano una convergenza, ma piuttosto la persistenza. Questo suggerisce che gli ambienti enterprise si stanno modernizzando in modo consapevole. Le organizzazioni enterprise bilanciano nuove funzionalità con gli investimenti esistenti, il budget, i requisiti normativi e la necessità di continuità operativa a lungo termine.

Il punto chiave è che gli ambienti misti non sono un segno di indecisione. Riflettono scelte modellate da esigenze e vincoli complessi che variano da un'organizzazione all'altra:

- Il 26,9% degli intervistati enterprise sta effettuando la migrazione di parte dei sistemi on-premise verso il cloud
- Il 18,7% sta sostituendo completamente i sistemi on-premise con soluzioni cloud-based

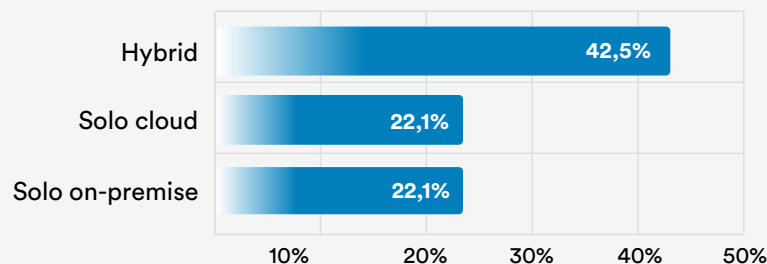
La diversità dei modelli di deployment non è una fase temporanea, ma una caratteristica distintiva degli ambienti di livello enterprise. I sistemi di sicurezza fisica devono resistere all'evoluzione tecnologica continua, supportando al contempo espansioni, audit e cambiamenti normativi. Questo livello di longevità richiede flessibilità, non uniformità.

Installazioni cloud e ibride enterprise:
la situazione attuale*



IL CLOUD STA GUADAGNANDO TERRENO NELLA SICUREZZA FISICA DI LIVELLO ENTERPRISE, MA I SISTEMI ON-PREMISE, IN PARTICOLARE PER IL CONTROLLO ACCESSI, RESTANO AMPIAMENTE DIFFUSI.

Visione del cloud a livello enterprise nei
prossimi cinque anni*



LE STRATEGIE CLOUD A LUNGO TERMINE PRIVILEGIANO LA FLESSIBILITÀ RISPETTO A UN UNICO MODELLO DI DEPLOYMENT.

* Intervistati enterprise, definiti come aziende con più di 1000 dipendenti

Per le organizzazioni i livello enterprise, l'affidabilità viene prima della comodità

A livello enterprise, le decisioni relative al cloud riflettono responsabilità organizzative, non preferenze individuali.

Quando le organizzazioni di grandi dimensioni considerano il cloud, il primo elemento da valutare è la governance. È più probabile che queste associno le decisioni cloud a cybersecurity, compliance e requisiti IT, mentre negli ambienti più piccoli comodità ed esternalizzazione hanno un peso maggiore.

Le decisioni cloud a livello enterprise vengono raramente prese in modo isolato. IT, gestione del rischio e dirigenza contribuiscono a queste scelte e ne restano responsabili anche molto tempo dopo l'installazione. Questo approccio orientato alla governance emerge chiaramente dai dati. Quando abbiamo chiesto di classificare i fattori che determinano l'adozione del cloud, le organizzazioni non enterprise hanno posizionato la possibilità di esternalizzare al secondo posto. Le organizzazioni enterprise, invece, l'hanno collocata al sesto posto, evidenziando la preferenza per controllo e supervisione rispetto alla comodità.



Cosa indicano i dati

26,7%

Percentuale di intervistati enterprise che segnala che la supervisione normativa ha rallentato l'adozione del cloud

42,4%

Indica il coinvolgimento dell'IT nelle decisioni di acquisto della sicurezza fisica

41,7%

Segnala un aumento degli incidenti fisici o informatici nell'ultimo anno

58,7%

Ha registrato un aumento degli attacchi di phishing o smishing

Anche la natura delle minacce è diversa. Gli attacchi di social engineering rappresentano la seconda tipologia di incidente più comune per le organizzazioni enterprise (43,5%). Le organizzazioni più piccole segnalano più frequentemente attacchi di hacking ai dispositivi per ottenere accesso alla rete (43,8%).

Quando si tratta di scegliere installazioni hybrid-cloud, le organizzazioni enterprise considerano la resilienza a lungo termine rispetto alla comodità nel breve periodo:

✓ Scalabilità

39,3% degli intervistati enterprise rispetto al 25,7% dei non enterprise

✓ Ridondanza

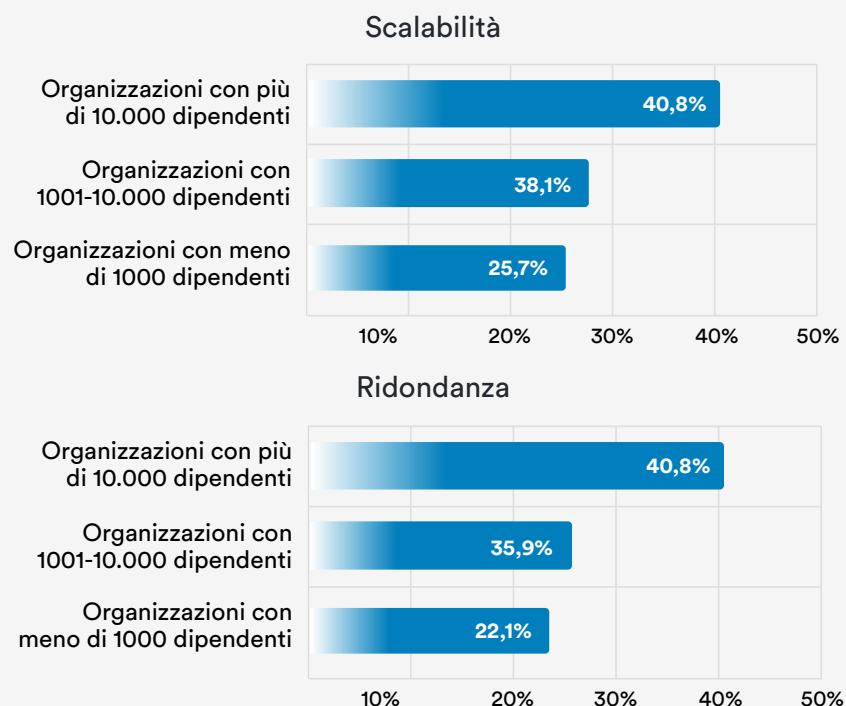
38,1% degli intervistati enterprise rispetto al 22,1% dei non enterprise

Con l'aumentare delle dimensioni organizzative, scalabilità e ridondanza diventano i principali fattori decisionali. Le organizzazioni con oltre 10.000 dipendenti tendono ad adottare modelli hybrid cloud per supportare una crescita sostenuta e la continuità operativa su larga scala.

CONCETTO CHIAVE

L'adozione del cloud in ambienti enterprise riguarda meno il luogo in cui sono attivi i sistemi e più la capacità di mantenere fiducia, resilienza e supervisione nel tempo. Il cloud offre il massimo valore quando consente alle organizzazioni di coordinare ambienti eterogenei preservando al contempo la governance.

Perché le organizzazioni di livello enterprise scelgono l'hybrid cloud



SIA LA SCALABILITÀ SIA LA RIDONDANZA AUMENTANO DI PARI PASSO CON LE DIMENSIONI. CIÒ SIGNIFICA CHE LE ORGANIZZAZIONI PIÙ GRANDI Danno PRIORITÀ ALLA RESILIENZA A LUNGO TERMINE NELLA SCELTA DELL'HYBRID CLOUD.

Maggiore è la dimensione dell'organizzazione, più scalabilità e ridondanza influenzano la scelta di adottare modelli ibridi.

Le organizzazioni di livello enterprise privilegiano la continuità operativa rispetto alle discontinuità

I risultati del sondaggio mostrano che le organizzazioni enterprise non stanno convergendo verso un unico modello cloud. Al contrario, progettano ambienti di sicurezza fisica destinati a durare nel tempo, tenendo conto di cambiamenti normativi, crescita, rischi di cybersecurity e lunghi cicli di vita tecnologici.

Dai dati emergono quattro temi principali:



La solidità conta più dell'uniformità

Le organizzazioni enterprise scelgono architetture che si evolvono nel tempo, evitando sostituzioni che comportano discontinuità operative o una supervisione frammentata.



Il cloud come modello operativo

Il valore deriva dal coordinamento, dalla visibilità e dal controllo tra ambienti eterogenei, non dall'eliminazione dei sistemi on-premise.



Governance e fiducia prima della velocità

Cybersecurity, compliance e capacità di audit prevalgono sulla facilità di installazione o sull'efficienza nel breve periodo.



Crescita del ruolo dei dati di sicurezza fisica

Con l'aumentare della connessione tra sistemi, le organizzazioni enterprise si aspettano che le piattaforme di sicurezza preservino contesto, integrità e responsabilità.

Questi modelli si rafforzano nelle organizzazioni più grandi. Con l'aumentare del numero di sedi, utenti e obblighi normativi, le strategie cloud devono resistere a una pressione operativa costante. In definitiva, è la governance, e non il modello di deployment, a determinare se i sistemi di sicurezza fisica enterprise possono garantire prestazioni affidabili nel tempo.

Cosa segnalano oggi le organizzazioni enterprise

37,4%

Percentuale che utilizza i dati della sicurezza fisica anche al di fuori del team di sicurezza per migliorare l'efficienza operativa in altre aree

26,5%

Percentuale che utilizza piattaforme unificate di controllo accessi e videosorveglianza

19,5%

Percentuale che condivide i metadati delle analisi video con altri sistemi enterprise

Genetec soddisfa i requisiti delle certificazioni più rigorose grazie a un approccio strutturato alla cybersecurity e alla privacy



ISO 27001:2022

Garantisce le buone pratiche per le persone, i processi e i sistemi IT attraverso processi di gestione dei rischi.



RGPD

Normativa europea che disciplina la raccolta, l'utilizzo, la conservazione e la protezione dei dati personali degli individui nell'UE..



ISO 27017

Assicura l'applicazione delle buone pratiche per i fornitori di servizi cloud al fine di mettere in sicurezza l'ambiente e ridurre i rischi di sicurezza



CSA STAR Level 1

Autovalutazione che dimostra che un fornitore cloud rispetta le buone pratiche di sicurezza, rafforzando la trasparenza e la fiducia



SOC2 Type 2

Audit che garantisce la coerenza e l'efficacia nella progettazione e nell'esercizio dei controlli di sicurezza

Cerchi ulteriori approfondimenti sulla sicurezza fisica?

Scarica il Rapporto sullo stato del settore della sicurezza fisica 2026.

Scarica l'edizione integrale del rapporto





Genetec Inc.
genetec.com/it
info@genetec.com
[@genetec](https://twitter.com/genetec)