REPORT

# Il panorama della sicurezza dell'identità 2026

La prospettiva di 5.000 IT e Cybersecurity Manager situati in 17 paesi

SOPHOS

# Introduzione

L'identità costituisce il perimetro della cybersecurity, e questo perimetro si sta ampliando per via della continua espansione dell'accesso ai sistemi da parte dell'IA, che può ora aprire e visualizzare i dati aziendali attraverso e-mail, file, applicazioni SaaS e identità sia umane che non umane. Il risultato è un maggiore livello di esposizione: ora le informazioni di natura sensibile sono più accessibili e facili da trasferire.

Con organizzazioni che continuano ad accelerare l'adozione del cloud e dello smart working, unite al proliferare di applicazioni e servizi che si basano sulle connessioni machine-to-machine (M2M), la quantità di identità digitali umane e non umane ha subito un'impennata. Ogni credenziale utente, chiave API, account di servizio e token OAuth rappresenta un potenziale punto di accesso per i cybercriminali. Di conseguenza, la sicurezza dell'identità è oggi uno degli ambiti più critici e problematici dei moderni sistemi di difesa informatica.

Gli autori degli attacchi hanno notato questa evoluzione. Le credenziali rubate, gli account di servizio compromessi e gli attacchi di social engineering rivolti ai dipendenti sono ormai tra i vettori di accesso iniziali più comuni nelle violazioni di sicurezza a livello mondiale. I cybercriminali stanno sfruttando IA e automazione per muoversi più rapidamente e per attaccare un maggior numero di sistemi. Le conseguenze vanno da furto di dati ed estorsione, fino a veri e propri attacchi ransomware in grado di bloccare completamente le attività aziendali per giorni o settimane intere.

Per comprendere la reale portata e il vero impatto delle minacce legate all'identità, Sophos ha sponsorizzato un sondaggio indipendente condotto tra 5.000 IT e Cybersecurity Manager in 17 paesi. Le domande si concentravano sulle esperienze e sulle conseguenze delle minacce all'identità nel 2025. Questo report presenta i risultati di questa ricerca, esaminando la frequenza degli attacchi all'identità, la capacità delle organizzazioni di rilevarli e bloccarli, le conseguenze che ne derivano, le cause all'origine delle violazioni andate a segno, l'impatto economico e il panorama generale dell'igiene della sicurezza dell'identità.

I risultati dipingono un quadro preoccupante: le minacce all'identità sono onnipresenti, causano gravi conseguenze e sono strettamente legate al ransomware. Le organizzazioni che non investono nella sicurezza dell'identità mettono a rischio le proprie attività operative, la stabilità finanziaria e la loro reputazione.

**5.000**

IT e Cybersecurity Manager in 17 paesi hanno partecipato a un sondaggio globale agnostico rispetto ai produttori

# I risultati più importanti, in breve

- **Il 71% delle organizzazioni ha subito almeno una violazione di sicurezza legata all'identità** negli ultimi 12 mesi, con una media di 3 attacchi per ogni azienda colpita.
- **Il 14% delle organizzazioni i cui sistemi sono stati violati non è riuscito a rilevare e bloccare** l'attacco all'identità più grave prima che causasse danni.
- **Il costo medio necessario per rimediare ai danni di una violazione dell'identità è stato pari a 1,64 milioni di dollari**, con un valore mediano di 750.000 dollari.
- **Il furto di dati (49%) e il ransomware (48%) sono state le conseguenze più comuni** degli attacchi di furto d'identità andati a segno.
- **Due terzi (67%) delle vittime del ransomware hanno riferito che l'attacco ransomware è stato anche il loro attacco all'identità più grave**, il che indica un chiaro nesso tra attacchi all'identità e ransomware.
- **La gestione inadeguata delle identità non umane (NHI) è stata citata nel 41% dei casi di violazione dell'identità**, risultando così la seconda causa più comune dopo l'errore umano (43%).
- **Le organizzazioni con una gestione inadeguata delle identità non umane hanno il 22% di probabilità in più di subire furti finanziari, il 24% di probabilità in più di cadere vittima di un tentativo di estorsione** e registrano costi di recovery complessivi che superano la media generale di quasi 150.000 dollari.
- **Solo 1 organizzazione su 3 (34%) effettua regolarmente la rotazione o il controllo degli account di servizio e delle identità non umane**, e appena l'11% lo fa continuamente. Questo crea lacune di sicurezza che vengono sfruttate dai cybercriminali.
- **Solo il 24% delle organizzazioni controlla continuamente se sono stati effettuati tentativi di accesso sospetti**, mentre più della metà lo fa ogni tre mesi o meno.
- **I fornitori che operano nel settore Fonti di energia, petrolio/gas e utenze (80%) e Governo centrale/federale (78%) hanno segnalato i più elevati tassi di violazione dei dati personali**, mentre IT, tecnologie e telecomunicazioni (63%) e Sanità (63%) hanno registrato quelli più bassi.
- **Le organizzazioni più piccole (100-250 dipendenti) hanno avuto il 72% di probabilità in meno di rilevare un attacco all'identità**, rispetto a quelle con 1.001-3.000 dipendenti (19% vs 11%).

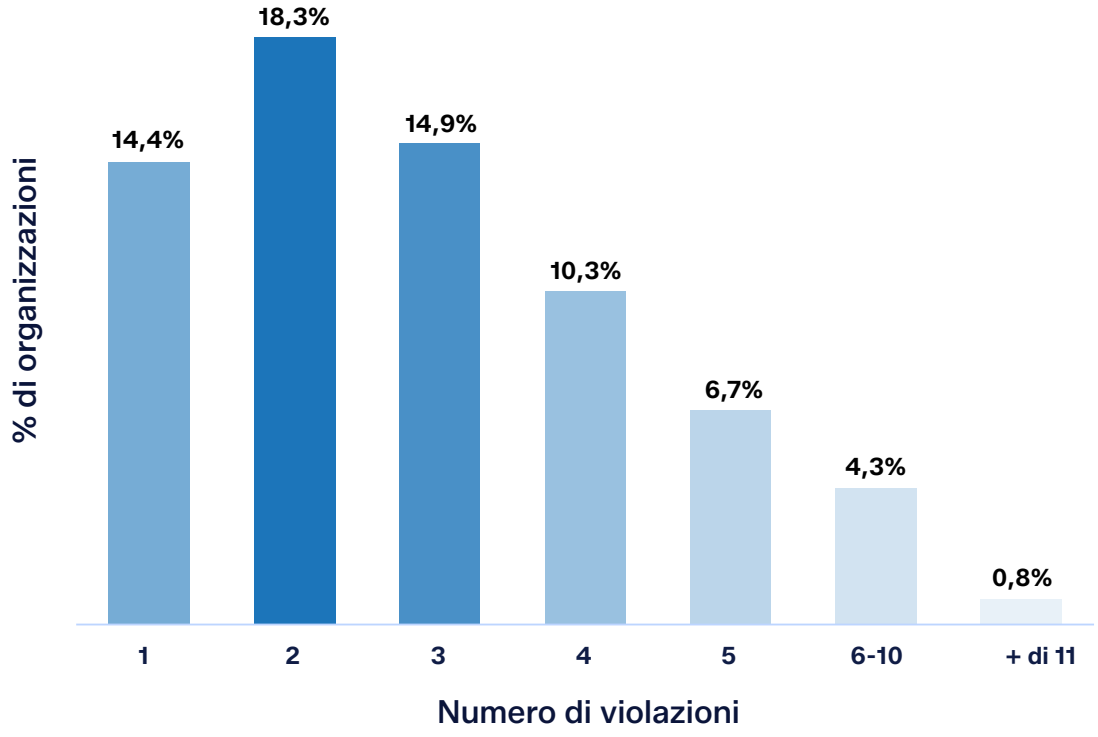
# Risultati dettagliati

## Frequenza degli attacchi all'identità

Il sondaggio rivela che le violazioni legate all'identità non sono casi isolati, bensì molto frequenti. Più di sette organizzazioni su dieci (70,9%) sono state vittime di almeno una violazione di sicurezza legata all'identità negli ultimi 12 mesi. Solo il 22,6% afferma con certezza di non aver subito alcuna violazione, mentre il 6,4% dei partecipanti ammette che potrebbero essersi verificati attacchi a loro sua insaputa.

Tra i casi di violazione, il numero medio di incidenti è stato pari a 3,1, il che indica che gli attacchi all'identità sono raramente eventi isolati. Il 5% degli intervistati ha dichiarato di aver subito sei o più violazioni nell'ultimo anno.

### Distribuzione della frequenza delle violazioni




*La tua organizzazione ha subito violazioni relative alla sicurezza dell'identità negli ultimi 12 mesi? Se sì, quante? n=5.000*

**67%**

Percentuale di tutti gli incidenti sui quali Sophos Incident Response e Sophos MDR hanno svolto indagini nel 2025, in cui erano coinvolti attacchi all'identità.

Approfondimenti di Sophos X-Ops

## Approfondimenti in base al paese

I tassi di violazione variano notevolmente da un'area geografica all'altra. La Svizzera (88,7%) ha registrato il tasso più alto, superando la media globale di 18 punti percentuali, seguita dal Messico (83,3%) e dall'Italia (80,0%). Germania (62,6%), Colombia (62,7%) e Giappone (64,7%) sono stati i paesi meno colpiti, sebbene anche i tassi più bassi siano oltre il 60%.

| Paese | Tasso di violazione | vs Percentuale globale (70,9%) |
|---|---|---|
| Svizzera | 88,7% | +17,8 p.p. |
| Messico | 83,3% | +12,4 p.p. |
| Italia | 80,0% | +9,1 p.p. |
| Australia | 79,7% | +8,8 p.p. |
| India | 76,8% | +5,9 p.p. |
| Sud Africa | 75,0% | +4,1 p.p. |
| Brasile | 74,0% | +3,1 p.p. |
| EAU | 73,3% | +2,4 p.p. |
| Singapore | 72,0% | +1,1 p.p. |
| Spagna | 70,0% | -0,9 p.p. |
| Cile | 66,7% | -4,2 p.p. |
| Stati Uniti | 66,1% | -4,8 p.p. |
| Francia | 66,0% | -4,9 p.p. |
| Regno Unito | 65,3% | -5,6 p.p. |
| Giappone | 64,7% | -6,2 p.p. |
| Colombia | 62,7% | -8,2 p.p. |
| Germania | 62,6% | -8,3 p.p. |

*La tua organizzazione ha subito violazioni relative alla sicurezza dell'identità negli ultimi 12 mesi? Se sì, quante? n=5.000.*

## Approfondimenti in base al settore

Analizzando le statistiche in base al settore, Fonti di energia, petrolio/gas e utenze (80,3%) e Governo centrale/federale (78,4%) hanno registrato i più elevati tassi di violazione dei dati. IT, tecnologie e telecomunicazioni (63,1%) e il settore Sanitario (63,4%) sono stati quelli meno colpiti, forse per via di una maggiore maturità di questi settori in termini di investimenti di sicurezza.

| Settore | Tasso di violazione |
|---|---|
| Fonti di energia, petrolio/gas e utenze | **80,3%** |
| Governo centrale/federale | 78,4% |
| Edilizia e immobili | 76,1% |
| Industria manifatturiera e produzione | 73,6% |
| Retail | 72,0% |
| Istruzione scolastica (scuole primarie e secondarie) | 71,1% |
| Servizi finanziari | 71,0% |
| Mass media, tempo libero e intrattenimento | 70,9% |
| Amministrazione locale/pubblica | 69,6% |
| Distribuzione e trasporto | 67,6% |
| Istruzione superiore | 65,9% |
| Servizi commerciali e professionali | 64,5% |
| Settore Sanitario | 63,4% |
| IT, tecnologie e telecomunicazioni | 63,1% |

*La tua organizzazione ha subito violazioni relative alla sicurezza dell'identità negli ultimi 12 mesi? Se sì, quante? n=5.000.*

## La conformità come indicatore

Le organizzazioni che hanno definito "Molto difficile" il rispetto dei requisiti di conformità hanno registrato un tasso di violazioni pari all'82,4%, ben 14 punti percentuali in più rispetto alle aziende che hanno definito tale adempimento come "Piuttosto difficile" o "Per niente difficile" (68,3%). Tutto ciò sembra suggerire che le difficoltà in termini di conformità siano un indicatore che segnala la presenza di vulnerabilità di sicurezza più ampie.

# Nozioni di base sulla sicurezza dell'identità

## I quattro tipi di identità che le organizzazioni devono gestire

Ogni azienda concede l'accesso a diversi tipi di identità. Ciascuna di esse comporta i propri rischi.

**Categoria 1 - Identità della forza lavoro**

Le persone all'interno dell'organizzazione che hanno bisogno di accedere a sistemi e dati per svolgere il proprio lavoro.

- Dipendenti
- Collaboratori esterni
- Amministratori IT e di sicurezza delle informazioni (persone il cui ruolo richiede accesso privilegiato al sistema)
- Dirigenti (persone il cui ruolo le rende particolarmente preziose per gli autori degli attacchi)

**Categoria 2 - Identità esterne**

Soggetti esterni all'organizzazione, ai quali viene concesso l'accesso, in modo temporaneo o permanente, per svolgere un ruolo o un'attività specifica e ben definita.

- Partner
- Fornitori
- Clienti

**Categoria 3 - Identità non umane (NHI)**

Software, sistemi e processi automatizzati ai quali è consentito eseguire attività senza un intervento umano.

- Account di servizio (ad es. backup pianificati)
- Chiavi API (ad es. integrazioni di app)
- Agenti IA (ad es. processi autonomi)
- Dispositivi IoT (ad es. sensori, fotocamere)

**Categoria 4 - Identità privilegiate (il livello di rischio più alto)**

Qualsiasi entità, umana o non umana, dotata di autorizzazioni avanzate che le concedono accesso profondo a sistemi e dati di natura sensibile.

- Super amministratori (ovvero persone con pieno controllo dei sistemi)
- Account root (ad es. accesso come amministratore cloud)
- Account condivisi (ad es. account di gruppo)
- Accesso di emergenza (ad es. account "break-glass")

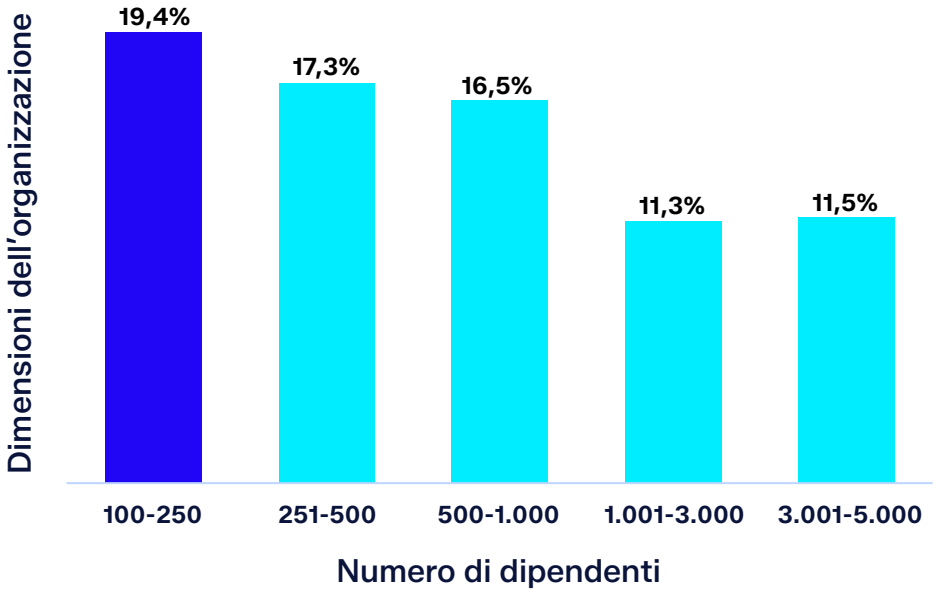
**Ogni identità è un potenziale punto di accesso**. Gestire chi e cosa ha accesso ai tuoi sistemi e garantire che questo accesso sia adeguato e monitorato sono le azioni più importanti che un'organizzazione può intraprendere per tutelare la propria sicurezza.

## Capacità di rilevare e bloccare gli attacchi all'identità

Dei 3.545 partecipanti al sondaggio che nel 2025 hanno subito una violazione legata all'identità, l'85,4% è riuscito a rilevare e bloccare l'attacco più grave prima che causasse danni. Sebbene questo dimostri che la maggior parte delle organizzazioni possiede una certa capacità di rilevamento, il 14,4% degli intervistati che non sono riusciti a bloccare l'attacco rappresenta un rischio estremo che non va sottovalutato. Inoltre, come rivelano i risultati successivi, le conseguenze subite da queste organizzazioni sono state molto gravi.

### Mancato rilevamento in base alle dimensioni dell'organizzazione

Le organizzazioni con meno dipendenti hanno mostrato una capacità nettamente inferiore di rilevare gli attacchi. Tra le aziende più piccole (100-250 dipendenti) oggetto del sondaggio, il 19,4% non è riuscito a bloccare l'attacco, una percentuale quasi doppia rispetto a quella delle organizzazioni con 1.001-3.000 dipendenti (11,3%). Questo divario mette in evidenza le difficoltà in termini di mancanza di risorse e capacità affrontate dalle aziende di dimensioni ridotte.




*Considerando l'attacco all'identità più grave subito negli ultimi 12 mesi, la tua organizzazione è stata in grado di bloccare l'attacco all'identità prima che causasse danni? Base: l'organizzazione ha subito una violazione di sicurezza legata all'identità. n=3.545.*

## Mancato rilevamento in base al paese

Il Brasile (21,6%) e la Svizzera (21,1%) hanno registrato i tassi più alti di mancato rilevamento, mentre il Regno Unito (7,1%) e il Messico (9,6%) hanno ottenuto i risultati migliori. In particolare, l'alto tasso di violazioni in Svizzera, unito all'elevata percentuale di casi di mancato rilevamento, contribuisce a incrementare la vulnerabilità di questo paese.

| Paese | Mancato rilevamento |
|---|---|
| **Brasile** | **21,6%** |
| Svizzera | 21,1% |
| Giappone | 19,6% |
| Spagna | 18,1% |
| Cile | 18,0% |
| Singapore | 17,6% |
| Germania | 17,4% |
| Francia | 14,6% |
| Italia | 14,6% |
| Australia | 13,8% |
| Colombia | 13,8% |
| Stati Uniti | 12,8% |
| EAU | 11,8% |
| India | 11,2% |
| Sud Africa | 10,7% |
| Messico | 9,8% |
| Regno Unito | 7,1% |

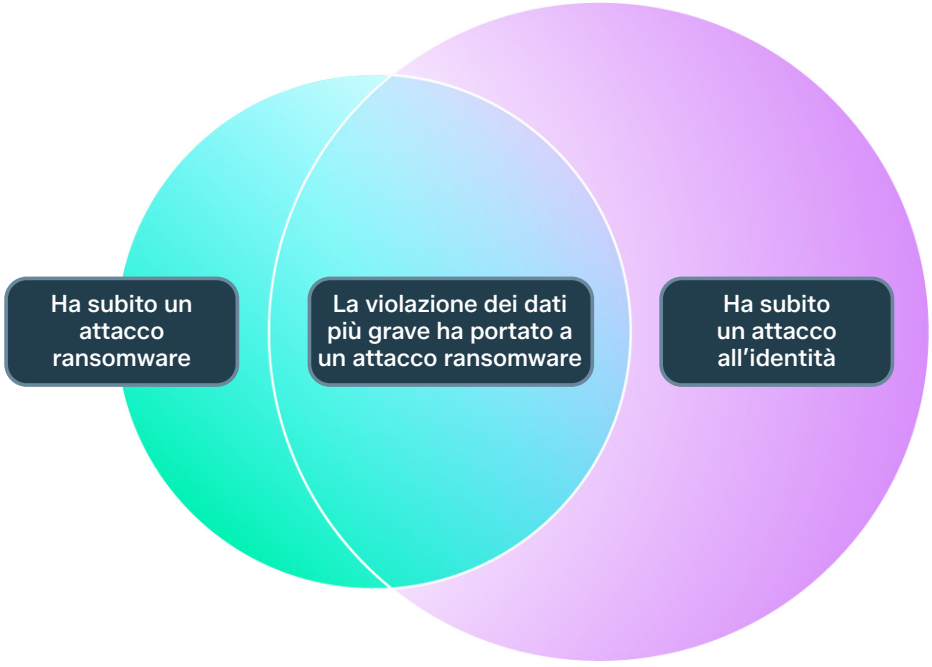
*Considerando l'attacco all'identità più grave subito negli ultimi 12 mesi, la tua organizzazione è stata in grado di bloccare l'attacco all'identità prima che causasse danni? Base: l'organizzazione ha subito una violazione di sicurezza legata all'identità. n=3.545.*

## Mancato rilevamento in base al settore

Il settore Mass media, tempo libero e intrattenimento (22,4%) ha registrato il più elevato tasso di mancato rilevamento, seguito dall'Industria manifatturiera (18,4%) e dai Servizi finanziari (17,9%). Il settore Sanitario (8,1%) ha ottenuto i risultati migliori in termini di rilevamento, il che potrebbe riflettere una maggiore pressione normativa a investire nel monitoraggio delle minacce.

## La correlazione tra identità e ransomware

Uno dei risultati più sorprendenti di questo sondaggio è il legame diretto tra attacchi all'identità e ransomware. Delle organizzazioni colpite dal ransomware nel 2025, due terzi (66,5%) hanno confermato che l'incidente causato dal ransomware era lo stesso evento del loro attacco all'identità più grave. Anche se non tutti gli attacchi hanno portato alla crittografia non autorizzata dei dati, questa statistica dimostra che la compromissione dell'identità è il principale meccanismo di diffusione del ransomware.




*La tua organizzazione è stata colpita dal ransomware l'anno scorso? (n=5,000). La tua organizzazione ha subito violazioni relative alla sicurezza dell'identità negli ultimi 12 mesi? Se sì, quante? (n=5.000) [Se la risposta è stata "Sì" a entrambe le domande] Quell'incidente di ransomware è stato anche l'attacco all'identità più grave subito dalla tua organizzazione?*

## La correlazione tra ransomware e identità, in base alle dimensioni dell'organizzazione

La correlazione tra identità e ransomware è stata più accentuata nelle organizzazioni con 1.001-3.000 dipendenti (71,6%) e meno presente in quelle con 100-250 dipendenti (62,4%). Questa variazione potrebbe riflettere le differenze in ambiti come la complessità dell'infrastruttura organizzativa, i livelli di visibilità o la capacità di mettere in relazione il vettore di attacco con il bersaglio dell'attacco nei vari segmenti.

| Dimensioni dell'organizzazione | Ransomware = Attacco all'identità |
|---|---|
| 100-250 o più dipendenti | 62,4% |
| 251-500 o più dipendenti | 68,2% |
| 501-1.000 o più dipendenti | 62,5% |
| 1.001-3.000 o più dipendenti | **71,6%** |
| 3.001-5.000 o più dipendenti | 64,6% |

*La tua organizzazione è stata colpita dal ransomware l'anno scorso? (n=5,000). La tua organizzazione ha subito violazioni relative alla sicurezza dell'identità negli ultimi 12 mesi? Se sì, quante? (n=5.000) [Se la risposta è stata "Sì" a entrambe le domande] Quell'incidente di ransomware è stato anche l'attacco all'identità più grave subito dalla tua organizzazione?*

## Approfondimenti in base al settore

Istruzione superiore (76,8%) e Distribuzione e trasporto (75,0%) hanno mostrato la correlazione più forte tra ransomware e identità, mentre Servizi finanziari (57,6%) e IT, tecnologie e telecomunicazioni (61,1%) hanno registrato valori più bassi (sebbene comunque ben al di sopra del 50%).

## Conseguenze delle violazioni dell'identità non rilevate

Per le 510 organizzazioni che non sono state in grado di bloccare il loro attacco all'identità più grave, l'impatto è stato grave e poliedrico, con vittime che hanno segnalato in media due conseguenze derivate dall'evento.

| Conseguenza | % di organizzazioni vittime di violazioni |
|---|---|
| **Furto di dati - Gli autori dell'attacco hanno rubato dati sensibili** | **48,8%** |
| Ransomware - Credenziali rubate utilizzate per facilitare l'esecuzione dell'attacco ransomware | 48,4% |
| Estorsione - I cybercriminali hanno chiesto dei soldi, minacciando le vittime | 43,9% |
| Sabotaggio - Gli autori dell'attacco hanno usato credenziali legittime per causare danni all'organizzazione | 30,0% |
| Furto finanziario - Pagamenti dirottati | 28,0% |
| Furto finanziario - Denaro rubato dai conti | 25,5% |
| **Riepilogo: Furto finanziario (in qualsiasi forma)** | **46,7%** |

*Quali sono state le conseguenze per la tua organizzazione di questa violazione dell'identità? Base: l'organizzazione non è riuscita a fermare la violazione di sicurezza. n=510.*

Quasi la metà delle aziende vittime della violazione dei dati ha subito un furto di dati (48,8%), mentre una percentuale pressoché identica è stata colpita da un attacco ransomware (48,4%). Quasi la metà (46,7%) degli intervistati ha subito una qualche forma di furto finanziario diretto (pagamenti dirottati, fondi sottratti o entrambi). Se considerati insieme ai casi di estorsione (43,9%), questi dati dimostrano che gli attacchi all'identità che non vengono rilevati portano quasi sempre a conseguenze estremamente gravi.

## Perché le organizzazioni sono cadute in trappola

Capire perché questi attacchi sono andati a segno è fondamentale per prevenirne di futuri. Il sondaggio ha messo in luce una combinazione di errori umani, procedurali e tecnici che ha portato le organizzazioni a cadere vittime di attacchi basati sull'identità. Dalle analisi è anche emerso che raramente esiste una sola causa: in media, gli intervistati hanno indicato due cause all'origine dell'incidente.

| Causa originaria | % di organizzazioni vittime di violazioni |
|---|---|
| **Errore umano - Un dipendente è stato indotto con l'inganno a fornire le proprie credenziali** | **42,7%** |
| Gestione inadeguata delle identità non umane (ad es. chiavi API memorizzate nel codice, credenziali statiche, account di servizio orfani che in passato collegavano applicazioni a sistemi, ecc.) | 40,6% |
| Gestione inadeguata delle identità umane per i dipendenti | 38,6% |
| Mancanza di visibilità sugli accessi e sulle autorizzazioni concesse ad applicazioni esterne | 35,7% |
| Gestione inadeguata delle identità umane per fornitori/collaboratori esterni | 31,4% |
| Mancanza di controllo sugli accessi e sulle autorizzazioni concesse ad applicazioni esterne | 30,8% |
| Un dipendente malintenzionato - Un dipendente ha volutamente facilitato l'attacco | 26,7% |
| **Riepilogo: Gestione inadeguata delle identità umane (in qualsiasi forma)** | **60,2%** |
| **Riepilogo: Problemi relativi all'accesso e alle autorizzazioni concesse ad applicazioni esterne (in qualsiasi forma)** | **56,1%** |

*Perché la tua organizzazione è stata vittima di un attacco legato all'identità? Seleziona tutte le risposte applicabili. Base: l'organizzazione non è riuscita a fermare la violazione di sicurezza. n=510.*

L'errore umano è stato il principale fattore individuale all'origine delle violazioni dell'identità, in quanto è stato segnalato dal 42,7% delle vittime. Al secondo posto si trova la gestione inadeguata delle identità non umane (40,6%), il che è particolarmente preoccupante perché include chiavi API memorizzate nel codice, credenziali statiche e account di servizio orfani, che sono più difficili da controllare e da monitorare.

In più un quarto (26,7%) degli attacchi è stata segnalata la presenza di attività malevole per mano di personale interno che ha volutamente facilitato l'attacco; questa statistica sottolinea l'importanza di mantenere controlli interni rigorosi e alti livelli di vigilanza.

Nel complesso, la gestione inadeguata delle identità umane (60,2%) è la causa più comune per cui le organizzazioni sono cadute vittime di attacchi basati sull'identità, mentre i problemi relativi agli accessi e alle autorizzazioni concesse ad applicazioni esterne hanno contribuito al 56,1% degli incidenti.

### 59,5%

La tecnologia MFA, ormai in uso da vari decenni, non era disponibile sul sistema preso di mira nel 59,5% dei casi che il team MDR ha analizzato per il Sophos Active Adversary Report 2025.

Approfondimenti di Sophos X-Ops

## Approfondimenti in base alle dimensioni delle organizzazioni

Le organizzazioni più grandi incontrano maggiori difficoltà rispetto a quelle più piccole in diversi ambiti legati alle vulnerabilità dell'identità; molto probabilmente questo è dovuto alle dimensioni più estese e alla maggiore complessità degli ambienti da monitorare e proteggere.

Più della metà (55,6%) delle aziende con 1.001-3.000 dipendenti ha indicato l'errore umano come causa principale dell'incidente, rispetto ad appena il 29,0% delle aziende con 251-500 dipendenti. Analogamente, il 68,6% delle organizzazioni con 3.001-5.000 dipendenti ha dichiarato che la gestione inadeguata delle identità umane ha contribuito a farle cadere vittime degli attacchi, mentre le aziende con 100-250 dipendenti che hanno fornito la stessa risposta sono state il 58,5%.

### Cosa sono le identità non umane

Un'identità non umana (NHI) è una credenziale digitale assegnata a un software, a un sistema o a un processo automatizzato per permettergli di accedere alle risorse senza alcun intervento umano. Per dimostrare la propria identità, le NHI non utilizzano password, bensì credenziali non umane, tra cui:

- Chiavi API che le collegano le applicazioni
- Account di servizio che eseguono backup
- Token OAuth per le integrazioni SaaS
- Agenti IA che accedono ai database

Le credenziali delle NHI possono essere rubate e utilizzate in modo illecito, proprio come avviene per i dati di accesso di utenti umani. La situazione è ancora più problematica quando le organizzazioni non controllano regolarmente le autorizzazioni delle NHI, che molto spesso sono estese e importanti.

Le NHI superano di gran lunga il numero di identità umane, e per alcune aziende il rapporto tra identità non umane e umane è di 100:1. L'IA agentica è una delle principali cause dell'aumento registrato negli ultimi anni di questo rapporto.

**96%**

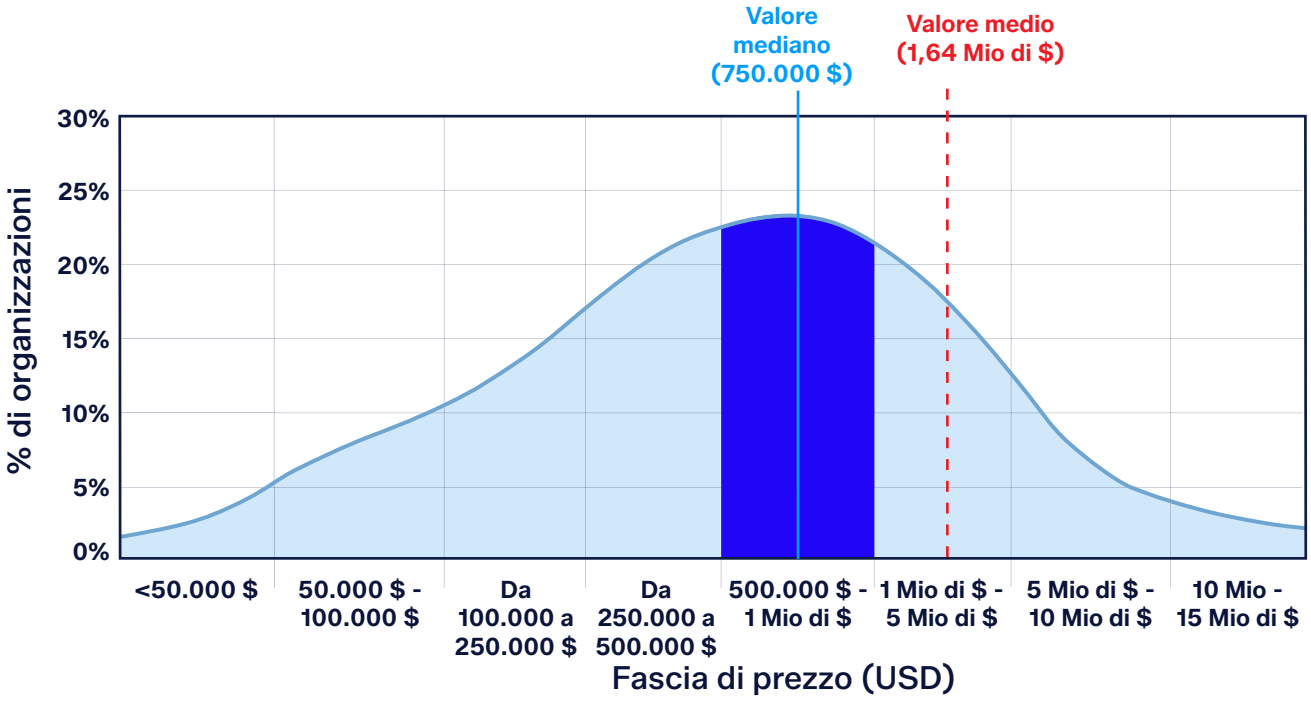
Percentuale di ambienti dei clienti Sophos ITDR in cui sono presenti applicazioni multitenant. Controllare o anche solo calcolare il numero delle NHI coinvolte in questi rapporti può essere molto difficile.

Approfondimenti di Sophos X-Ops

## L’impatto economico delle violazioni dell’identità

Le organizzazioni che hanno subito una violazione dei dati andata a segno hanno dovuto sostenere costi di riparazione notevoli. Il costo medio globale di recovery è stato pari a 1.637.363 dollari, con un valore mediano di 750.000 dollari. Il 73% delle organizzazioni colpite ha stimato costi pari o superiori a 250.000 dollari, mentre quasi un quarto (23,7%) rientra nella fascia compresa tra 500.000 e 1 milione di dollari.

### Ripartizione dei costi




*Quanto stimi che sia il costo complessivo sostenuto dalla tua organizzazione per rimediare ai danni della violazione dell’identità? Base: l’organizzazione non è riuscita a fermare la violazione di sicurezza. n=510.*

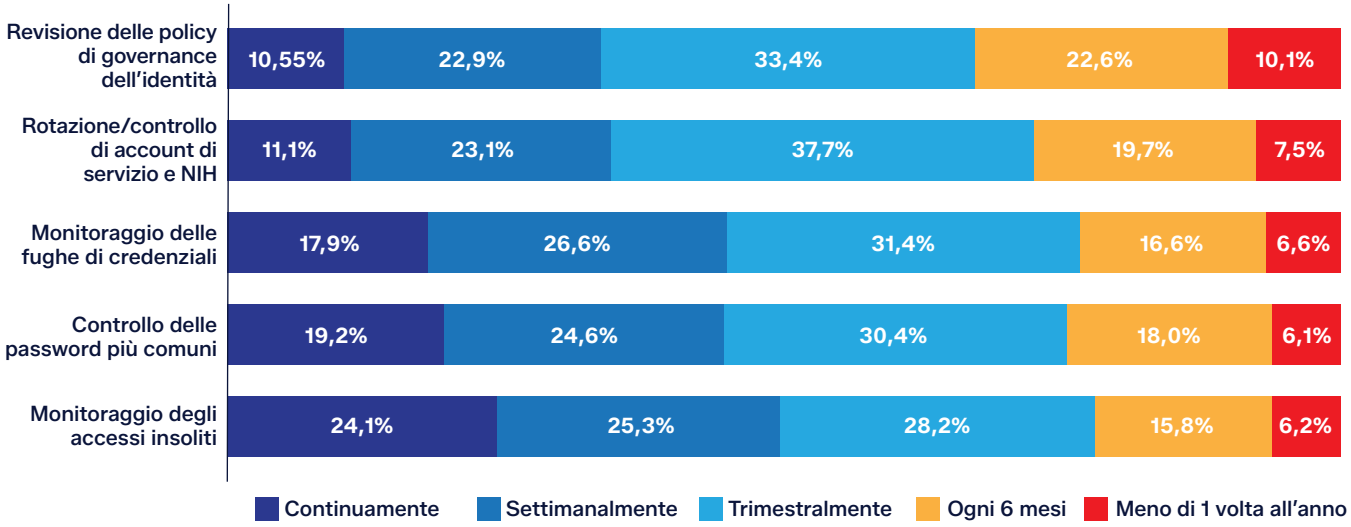
### Costo in base alle dimensioni dell’organizzazione

| Dimensioni dell’organizzazione | Costo medio | Costo mediano |
|---|---|---|
| 100-250 o più dipendenti | 1,125,562 $ | 375,000 $ |
| 251-500 o più dipendenti | 1,978,043 $ | 750,000 $ |
| 501-1.000 o più dipendenti | 1,009,205 $ | 375,000 $ |
| 1.001-3.000 o più dipendenti | 1,907,594 $ | 750,000 $ |
| 3.001-5.000 o più dipendenti | 2,452,929 $ | 750,000 $ |

*Quanto stimi che sia il costo complessivo sostenuto dalla tua organizzazione per rimediare ai danni della violazione dell’identità? Base: l’organizzazione non è riuscita a fermare la violazione di sicurezza. n=510.*

## Igiene della sicurezza dell'identità

Il sondaggio ha esaminato cinque attività fondamentali di gestione delle identità, insieme alla frequenza con cui vengono svolte dalle organizzazioni. I risultati mostrano divari significativi tra le best practice e la realtà, con differenze che aumentano il rischio di esposizione agli attacchi mirati all'identità.




*Con quale frequenza la tua organizzazione svolge le seguenti attività di gestione dell'identità? n=5.000*

Il monitoraggio dei tentativi di accesso insoliti è l'attività più comunemente svolta in tempo reale (24,1% in modo continuativo), eppure anche in questo caso oltre la metà (50,6%) delle organizzazioni effettua controlli non più di una volta ogni tre mesi. Per quanto riguarda la rotazione o il controllo delle identità non umane (un'attività fondamentale, visto che rappresenta la seconda causa principale delle violazioni), solo il 34,3% lo effettua ogni settimana o più sovente.

La revisione delle policy di governance dell'identità è l'attività svolta con minore frequenza su base continuativa (10,5%); un terzo delle organizzazioni (33,3%) le rivede non più di una volta ogni tre mesi, mentre il 22,6% le verifica solo ogni sei mesi. Visto che le minacce alla sicurezza dell'identità si evolvono rapidamente, eseguire revisioni annuali, semestrali o anche trimestrali significa esporsi a lacune pericolose.

## IA agentica: un fattore che aggrava il problema delle NHI

L'IA agentica ha complicato in modo esponenziale il problema della gestione delle NHI: un numero maggiore di identità, create più rapidamente, con un accesso più ampio e meno controllo umano. Le principali sfide relative alle NHI includono quanto segue:

- **Gli agenti IA moltiplicano automaticamente le NHI**
  Ogni agente IA ha bisogno di una propria identità e di un suo set di credenziali. Fondamentalmente, gli agenti possono creare in modo autonomo nuovi agenti per portare a termine attività secondarie, e ognuno di questi agenti genera ulteriori credenziali senza alcuna supervisione o intervento umano.
- **Gli agenti IA richiedono un accesso ampio e persistente**
  Per svolgere il loro lavoro, gli agenti IA devono interagire con diversi sistemi: calendari, database, CRM, file system e API. A differenza degli account di utenti umani, questi diritti di accesso scadono raramente e vengono controllati solo di rado.
- **Gli agenti IA sono più difficili da monitorare rispetto alle NHI tradizionali**
  Un account di servizio di backup esegue la stessa attività ogni notte alla stessa ora, il che ne facilita il monitoraggio. Gli agenti IA, invece, prendono decisioni in perfetta autonomia, agiscono in modo imprevedibile e sono attivi 24/7, e queste caratteristiche rendendo molto difficile capire quando qualcosa va storto.
- **Agenti IA di terze parti e rischi sconosciuti ereditati**
  Gli studi di ricerca indicano che, quando utilizzano funzionalità di agenti IA di terze parti, le organizzazioni ereditano tutte le credenziali e le autorizzazioni di accesso di tali agenti, pur avendo una visibilità limitata sul livello di sicurezza applicato durante la loro creazione o sugli elementi ai quali possono accedere.
- **Le regole di sicurezza non sono state pensate per gli agenti IA**
  Nella maggior parte dei casi, i framework di sicurezza dell'identità sono stati progettati per utenti umani e account macchina elementari. Non tengono conto degli agenti in grado di creare, delegare e revocare autonomamente le proprie credenziali durante il flusso di lavoro, creando così una lacuna significativa in termini di governance.

**L'IA agentica è uno dei motivi principali per cui la sicurezza delle NHI è diventata una priorità assoluta per i CISO.**

## Le conseguenze di una gestione inadeguata delle identità non umane

Come già indicato, la gestione inadeguata delle identità non umane (NHI) è stata la causa principale nel 40,6% degli attacchi andati a segno. Analizzando più a fondo i risultati, le statistiche rivelano che la compromissione delle NHI aggrava drasticamente le conseguenze finanziarie della violazione dei dati.

In particolare, le organizzazioni con una gestione inadeguata delle NHI sono molto più esposte al rischio di furti finanziari (in cui gli autori degli attacchi dirottano i pagamenti da conti legittimi), con una percentuale 27,9% più alta rispetto alla media, e al rischio di estorsione (in cui i cybercriminali chiedono soldi, minacciando le vittime), con un tasso che supera del 24,4% la media generale. Le uniche categorie nelle quali le organizzazioni con una gestione inadeguata delle NHI hanno ottenuto risultati leggermente superiori alla media sono state il furto di dati e il ransomware, anche se le differenze sono minime.

| Conseguenza | % di tutte le organizzazioni vittime di violazioni | % di organizzazioni vittime di violazioni con una gestione inadeguata delle identità non umane | Variazione percentuale con una gestione inadeguata delle identità non umane |
|---|---|---|---|
| Furto di dati - Gli autori dell'attacco hanno rubato dati sensibili | 48,8% | 47,8% | -2,1% |
| Ransomware - Credenziali rubate utilizzate per facilitare l'esecuzione dell'attacco ransomware | 48,4% | 46,4% | -4,1% |
| **Estorsione - I cybercriminali hanno chiesto dei soldi, minacciando le vittime** | 43,9% | **54,6%** | **+24,4%** |
| Sabotaggio - Gli autori dell'attacco hanno usato credenziali legittime per causare danni all'organizzazione | 30,0% | 33,8% | +12,7% |
| **Furto finanziario - Pagamenti dirottati** | 28,0% | **35,8%** | **+27,9%** |
| Furto finanziario - Denaro rubato dai conti | 25,5% | 29,9% | +15,7 |
| **Riepilogo: Furto finanziario (in qualsiasi forma)** | **46,7%** | **57,0%** | **+22%** |

*Quali sono state le conseguenze per la tua organizzazione di questa violazione dell'identità? Base: l'organizzazione non è riuscita a fermare la violazione di sicurezza. n=510 (tutte le violazioni), n=207 (violazioni che coinvolgevano le NHI)*

Considerando il crescente impatto finanziario delle NHI, non sorprende affatto che le organizzazioni con una gestione inadeguata delle NHI dichiarino costi complessivi di recovery da una violazione dell'identità notevolmente più alti, con una cifra che di solito supera di quasi 150.000 dollari la media totale.

### Costo medio necessario per rimediare ai danni delle violazioni dell'identità


Esiste una correlazione evidente tra una scarsa igiene delle NHI e la probabilità di subire una violazione dei dati correlata alle NHI. Mentre un terzo (34%) di tutte le organizzazioni effettua la rotazione o il controllo degli account di servizio e delle NHI continuamente o settimanalmente, questa percentuale scende a un quarto (24%) tra le aziende la cui violazione è stata causata dalla compromissione delle NHI.

## Conclusione

I risultati di questo sondaggio indicano che nessuno può abbassare la guardia. Nell'ultimo anno, le violazioni relative all'identità hanno colpito più di 7 organizzazioni su 10, con una media di oltre tre incidenti per ogni azienda coinvolta. Questo non è un rischio teorico o un problema limitato a determinati settori o aree geografiche. Si tratta di una minaccia universale e dilagante che colpisce le organizzazioni di qualsiasi dimensione, settore e regione. I dati dimostrano che gli attacchi all'identità sono la porta d'ingresso attraverso la quale il ransomware, il furto di dati e le estorsioni si infiltrano in un'organizzazione: il 67% delle vittime del ransomware ha ricondotto l'incidente direttamente a una violazione dei dati personali.

Quando gli attacchi all'identità vanno a segno, le conseguenze sono gravi e si ripercuotono su più fronti. Quasi la metà delle organizzazioni vittime della violazioni dei dati ha subito furti di dati o attacchi ransomware, e il costo medio di riparazione dei danni, pari a 1,64 milioni di dollari, rende ogni singolo incidente un evento finanziario di notevole entità.

Le cause originarie indicano carenze sistemiche: errore umano (42,7%), gestione inadeguata delle identità non umane (40,6%) e visibilità insufficiente sulle autorizzazioni delle applicazioni di terze parti (35,7%) sono tutti aspetti risolvibili, ma solo con investimenti continui e una vigilanza costante. Il fatto che le organizzazioni più piccole abbiano, rispetto alle imprese più grandi, quasi il doppio delle probabilità di non riuscire a rilevare gli attacchi mette in luce un divario di risorse di cybersecurity che la comunità di sicurezza non può ignorare.

Forse il fattore più preoccupante è il panorama generale dell'igiene della sicurezza dell'identità. Solo un quarto delle organizzazioni monitora continuamente gli accessi per individuare attività insolite, e meno di un'azienda su tre ruota regolarmente le credenziali non umane, ovvero i punti deboli maggiormente sfruttati dai cybercriminali.

Le organizzazioni devono rendersi conto che la sicurezza dell'identità non è un progetto singolo e isolato, ma una vera e propria disciplina operativa continua. Le aziende che la considereranno come tale si troveranno in una posizione decisamente migliore per difendersi dalle minacce che hanno caratterizzato il 2025 e che continueranno a intensificarsi nel 2026 e oltre.

# Raccomandazioni

Come è emerso dal sondaggio, poter contare su una sicurezza dell'identità di alta qualità è fondamentale per una strategia efficace di mitigazione del rischio informatico. Per ridurre l'esposizione agli attacchi legati all'identità, le organizzazioni devono cercare di implementare una difesa a più livelli sia per le identità umane che per quelle non umane. Inizia con gli step essenziali e procedi poi con quelli consigliati, nel contesto di un programma di miglioramento continuo.

## Step essenziali

### Identità umane

- Implementa l'autenticazione multifattoriale (MFA) per tutti gli account utente.
- Imposta credenziali diverse per le operazioni con privilegi e per quelle senza privilegi.
- Implementa il blocco degli account e la protezione contro gli attacchi brute force.
- Centralizza la gestione delle identità con il Single Sign-On (SSO).
- Assicurati che i tuoi programmi di formazione e sensibilizzazione degli utenti includano le nuove tecniche di phishing e furto delle credenziali.

### Identità non umane

- Compila periodicamente un inventario e classifica tutte le identità non umane.
- Utilizza credenziali temporanee, invece di segreti di lunga durata.

### Identità umane e non umane

- Applica il principio dell'assegnazione di meno privilegi possibili
- Proteggi e gestisci correttamente le credenziali.
- Disattiva o elimina immediatamente le identità non attive.
- Implementa una procedura formale di offboarding che preveda il controllo e la revoca degli accessi alle risorse aziendali.
- Registra nei log e monitora tutte le attività di autenticazione, e conserva i log per almeno 30 giorni.

## Step consigliati

### Identità umane

- Implementa accesso condizionale e policy basate sul rischio.
- Implementa le chiavi di accesso (hardware o software) come metodo di autenticazione principale.
- Applica la federazione delle identità utilizzando protocolli di identità ampiamente riconosciuti, come il Security Assertion Markup Language (SAML) o il più recente OpenID Connect (OIDC).

### Identità non umane

- Usa la federazione delle identità dei workload, invece di segreti statici.
- Adotta una piattaforma di gestione dei segreti per le NHI su larga scala.
- Abilita la scansione dei segreti sulle piattaforme supportate (GitHub, GitLab).

### Identità umane e non umane

- Distribuisci una soluzione di Privileged Access Management (PAM).
- Adotta un modello di sicurezza Zero Trust.
- Conduci revisioni periodiche degli accessi ed effettua la ricertificazione dei diritti.
- Implementa funzionalità di Identity Threat Detection and Response (ITDR).
- Segmenta l'accesso alla rete in base all'identità e al ruolo.
- Definisci uno o più playbook di incident response per l'identità e conduci esercitazioni per testarne l'efficacia. I playbook devono indicare come gestire attacchi all'identità simili a quelli descritti in questo report.

# Scopri di Più

## Leggi la nostra Guida alle best practice per la sicurezza dell'identità

### *Metodologia*

*Questo sondaggio è stato condotto da Vanson Bourne per conto di Sophos nel primo trimestre del 2026. Sono stati intervistati 5.000 decision maker in ambito IT e Cybersecurity, situati in 17 paesi: Stati Uniti, Brasile, Cile, Colombia, Messico, Regno Unito, Francia, Germania, Italia, Spagna, Svizzera, Australia, India, Giappone, Singapore, Sudafrica ed Emirati Arabi Uniti. I partecipanti fanno parte di organizzazioni con un numero di dipendenti compreso tra 100 e 5.000, che operano in 15 settori.*

SOPHOS

Per parlare delle tue esigenze in materia di sicurezza dell'identità e per scoprire come Sophos può aiutarti, visita il nostro sito web o parla con un nostro consulente.

**Vendite per l'Italia**
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it


2026-05-08 IT (TA) CRE-5312