SOPHOS

# LA VERA STORIA DEL RANSOMWARE 2025

I risultati di uno studio indipendente a cui hanno partecipato 3.400 IT e Cybersecurity Manager in 17 paesi, le cui organizzazioni sono state colpite dal ransomware l'anno scorso.

Whitepaper Sophos. Giugno 2025

# Introduzione

Ti diamo il benvenuto alla sesta edizione del report annuale di Sophos La Vera Storia del Ransomware, che rivela le dinamiche del malware nel 2025.

Il report di quest'anno offre una descrizione dettagliata di come si sono evolute le esperienze con il ransomware (tanto le cause, quanto le conseguenze) delle organizzazioni nel corso degli ultimi 12 mesi. Inoltre, offre una prospettiva più nitida di ambiti precedentemente inesplorati, inclusi i fattori operativi che hanno esposto le organizzazioni ai rischi di attacco, nonché l'impatto umano degli incidenti sul team IT/di cybersecurity.

Basandosi sulle esperienze reali vissute in prima persona da 3.400 IT e Cybersecurity Manager in 17 paesi, che lavorano per organizzazioni cadute vittima del ransomware l'anno scorso, questo report offre approfondimenti esclusivi su argomenti come:

- Perché le organizzazioni vengono colpite dal ransomware.
- Cosa succede ai dati.
- I riscatti: richieste e pagamenti.
- L'impatto commerciale del ransomware.
- L'impatto umano del ransomware.

## Una nota sul periodo di riferimento del report

Per facilitare il confronto delle statistiche dei nostri sondaggi annuali, i nostri report vengono nominati in base all'anno in cui viene condotto il sondaggio, in questo caso il 2025. Siamo consci del fatto che i partecipanti condividono le loro esperienze nel corso dell'anno precedente, per cui molti degli attacchi menzionati si sono verificati nel 2024.

## Informazioni sul sondaggio

Il report è basato sui risultati di un sondaggio indipendente e vendor-agnostic che valuta le esperienze delle organizzazioni con il ransomware. È stato condotto per conto di Sophos da specialisti di terze parti nel periodo tra gennaio e marzo 2025. A tutti i partecipanti, che lavorano in organizzazioni con un numero di dipendenti compreso tra 100 e 5.000, è stato chiesto di rispondere tenendo in considerazione le proprie esperienze nei 12 mesi precedenti.

Le organizzazioni prese in esame nel sondaggio sono situate in 17 paesi e operano in vari settori, per garantire che i risultati del sondaggio riflettano le diverse esperienze in settori pubblici e privati. Il report include confronti con i risultati dei nostri studi di ricerca precedenti, per un raffronto annuo. Tutti i dati finanziari sono espressi in dollari U.S.A.

# I risultati più salienti

## Perché le organizzazioni vengono colpite dal ransomware

- Per il terzo anno consecutivo, le vittime identificano le **vulnerabilità soggette a exploit** come la più comune causa originaria di un attacco, essendo state utilizzate nel 32% degli incidenti.
- Le organizzazioni sono state colpite dal ransomware per via di diversi fattori operativi, il più ricorrente dei quali è la **mancanza di competenze**, segnalata dal 40,2% delle vittime. Questo fattore viene seguito a stretta distanza dalla presenza di **lacune di sicurezza che l'organizzazione non sapeva esistessero**, un problema che ha contribuito al 40,1% degli attacchi. Al terzo posto si trova la **mancanza di personale/capacità**, che è risultata nel 39,4% degli attacchi.

## Cosa succede ai dati

- La **crittografia dei dati** come conseguenza degli attacchi è scesa al livello più basso in sei anni, in quanto è stata riscontrata nel 50% dei casi: una percentuale in calo rispetto al 70% del 2024.
- Il 28% delle organizzazioni che avevano subito la crittografia non autorizzata dei dati sono cadute vittima anche dell'**esfiltrazione dei dati**.
- Il 97% dei partecipanti al sondaggio i cui dati erano stati crittografati sono stati in grado di recuperarli.
- L'utilizzo di **backup** per ripristinare i dati crittografati ha toccato il punto più basso negli ultimi sei anni, essendo stato osservato nel 54% degli incidenti.
- Nel 49% dei casi, le vittime hanno **pagato il riscatto** per recuperare i dati sottratti. Sebbene si tratti di una leggera diminuzione rispetto al 56% dell'anno scorso, è pur sempre il secondo più alto tasso di pagamento del riscatto riscontrato negli ultimi sei anni.

## I riscatti: richieste e pagamenti

- La somma media (mediana) delle **richieste di riscatto** è calata di un terzo (34%) negli ultimi 12 mesi: nel 2025 ammonta infatti a 1.324.439 $, mentre nel 2024 era arrivata a 2 milioni di $.
- La cifra media (mediana) per il **pagamento del riscatto** ha registrato una diminuzione del 50% l'anno scorso, passando dai 2 milioni di $ del 2024 a 1 milione di $ nel 2025. La principale causa di questo calo è l'abbassamento del tasso dei pagamenti del riscatto di 5 o più milioni di $, che è scesa dal 31% dei pagamenti nel 2024 al 20% nel 2025.
- Eseguendo un confronto tra **le richieste e i pagamenti**, il pagamento finale è stato pari alla richiesta iniziale solo per il 29% degli intervistati. Nel 53% degli incidenti, le vittime hanno pagato meno della richiesta iniziale, mentre nel 18% dei casi hanno pagato di più.

## L'impatto commerciale del ransomware

- Escludendo le cifre pagate per il riscatto, l'anno scorso il **costo medio della riparazione dei danni** di un attacco ransomware è sceso del 44%, con 1,53 milioni di $, rispetto ai 2,73 milioni di $ del 2024.
- Analizzando il **tempo necessario per tornare alla normalità operativa**, le organizzazioni si riprendono dagli attacchi con maggiore rapidità, con il 53% degli intervistati che sostengono di aver ripreso le normali attività dopo una settimana, una statistica in aumento rispetto al 35% del 2024.

## L'impatto umano del ransomware

- Tutte le organizzazioni che avevano subito la crittografia non autorizzata dei dati confessano che ci sono state **ripercussioni dirette** sui loro team IT/di cybersecurity:
  - Il 41% dei team IT/di cybersecurity dichiarano di soffrire di **maggiore ansia o stress** per paura di attacchi futuri.
  - Un terzo (34%) sostiene che il team ha avuto **sensi di colpa** dovuti al fatto che l'attacco non era stato fermato in tempo.
  - Il 40% indica di sentire **maggiori pressioni** dal Senior Management, mentre il 31% nota **maggiore stima**.
  - Nel 31% dei team sono state osservate **assenze del personale** dovute a problemi di stress/salute mentale correlati all'attacco.
  - In un quarto di questi casi, c'è stato un **cambio di leadership** nel team, come conseguenza dell'attacco.

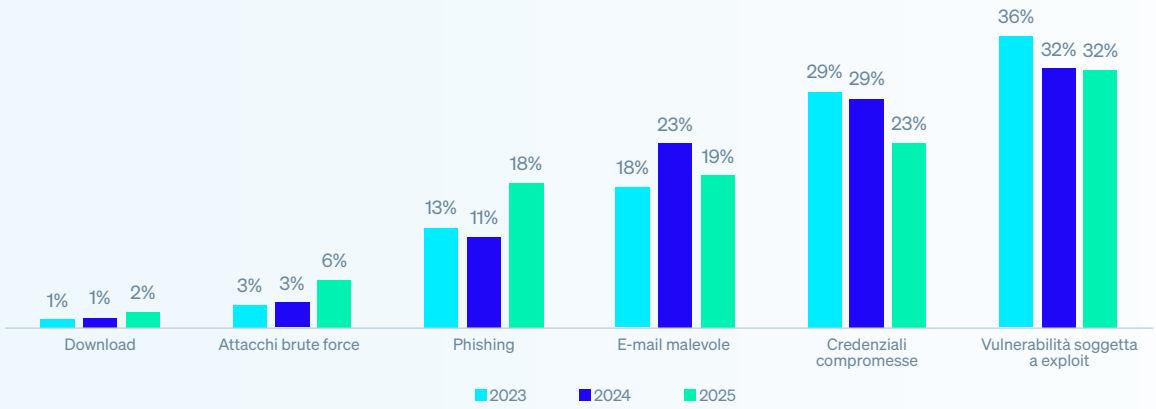
# Perché le organizzazioni vengono colpite dal ransomware

## Causa tecnica all'origine degli attacchi

Per il terzo anno consecutivo, le vittime identificano le **vulnerabilità soggette a exploit** come la più comune causa originaria degli incidenti di ransomware, essendo state utilizzate per l'infiltrazione nei sistemi delle organizzazioni nel 32% di tutti gli attacchi.

Le **credenziali compromesse** mantengono il secondo posto nella classifica dei più comuni vettori di attacco percepiti, sebbene la percentuale degli attacchi che utilizzano questo approccio sia scesa dal 29% del 2024 al 23% del 2025. Le e-mail rimangono uno dei vettori di attacco maggiormente sfruttati, con il 19% delle vittime che indica come causa originaria degli incidenti le **e-mail pericolose**, e con un ulteriore 18% che attribuisce invece la colpa al **phishing**: un balzo significativo rispetto all'11% dell'anno scorso.

**Grafico 1: Causa tecnica all'origine degli attacchi ransomware, 2023-2025**

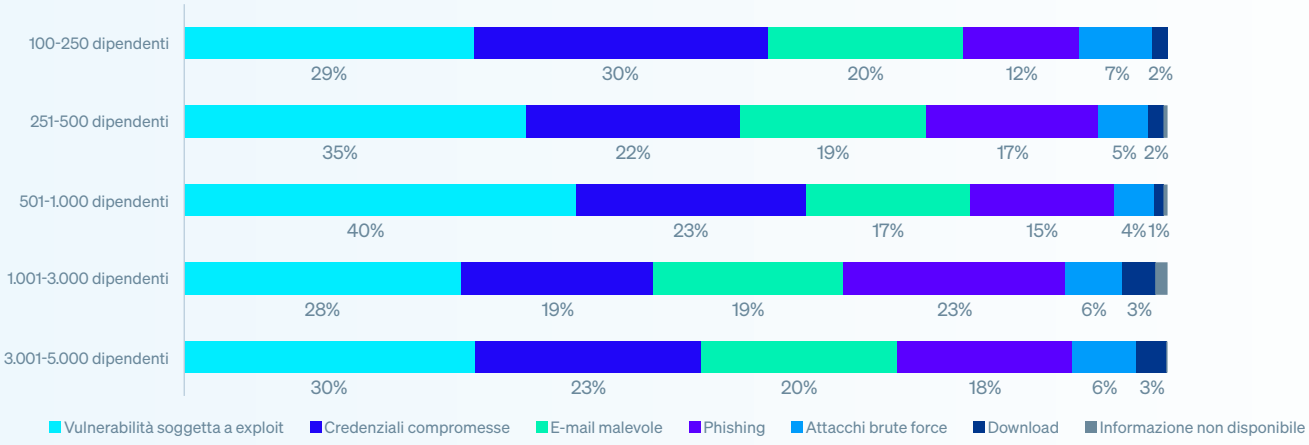



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. n=3.400 (2025), n=2.974 (2024), n=1.974 (2023).

Dal sondaggio emergono differenze nei vettori di attacco, correlate alle dimensioni dell'organizzazione:

- Le **credenziali compromesse** sono state la più comune causa all'origine degli attacchi nella fascia di organizzazioni con 100-250 dipendenti, dove sono state utilizzate nel 30% degli attacchi.
- Il 40% degli attacchi subiti dalle organizzazioni con 501-1.000 dipendenti ha avuto inizio con una **vulnerabilità soggetta a exploit**.
- Poco meno di un quarto (23%) degli attacchi nelle organizzazioni con 1.001-3.000 dipendenti è stato causato da un'**e-mail di phishing**.

**Grafico 2: Causa tecnica all'origine degli attacchi, con risultati suddivisi in base alle dimensioni dell'organizzazione**

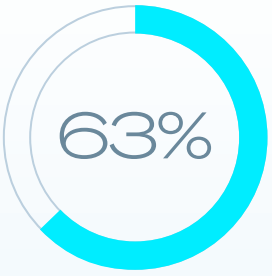



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. n=3.400

## Causa operativa all'origine degli incidenti

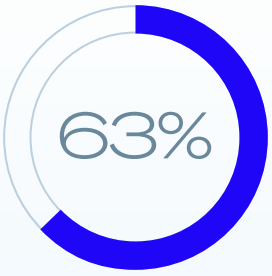
Il report di quest'anno esplora per la prima volta i fattori organizzativi che hanno esposto le aziende agli attacchi. Dai risultati emerge che di solito le vittime devono affrontare varie sfide operative, in quanto gli intervistati citano una media di 2,7 fattori che hanno contribuito a renderli un bersaglio per gli attacchi ransomware.

Complessivamente non esiste una singola causa originaria organizzativa che spicchi fra le altre: nella maggior parte dei casi si tratta di problemi di protezione, scarsa disponibilità di risorse e lacune di sicurezza, tutti equamente distribuiti.



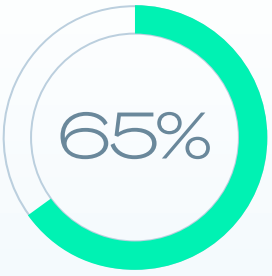

**Problemi di protezione**

(scarsa qualità o assenza di soluzioni di protezione)




**Scarsa disponibilità di risorse**

(mancanza di competenze o di personale/capacità)



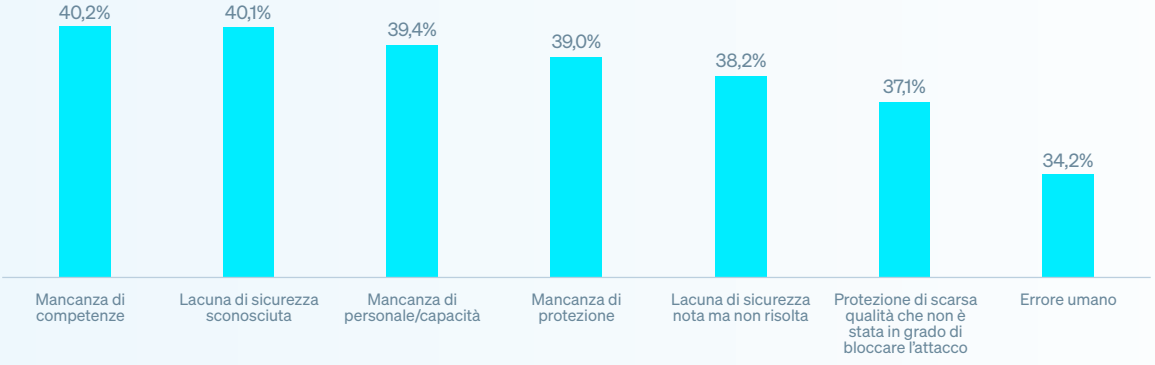

**Lacuna di sicurezza**

(nota o sconosciuta)

Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=3.400

La **mancanza di competenze** (ovvero l'assenza delle capacità o delle conoscenze necessarie per rilevare e bloccare l'attacco in tempo), è il principale motivo operativo fornito, in quanto è stata indicata dal 40,2% dei partecipanti allo studio di ricerca. Viene seguita a stretta distanza dalla presenza di **lacune di sicurezza che l'organizzazione non sapeva esistessero**, un fattore che ha contribuito al 40,1% degli attacchi. Al terzo posto si trova la **mancanza di personale/capacità** (ovvero non avere a disposizione un numero sufficiente di esperti di cybersecurity che monitorassero i sistemi al momento dell'attacco), che ha contribuito al 39,4% degli attacchi.

**Grafico 3: Causa operativa all'origine degli attacchi ransomware**

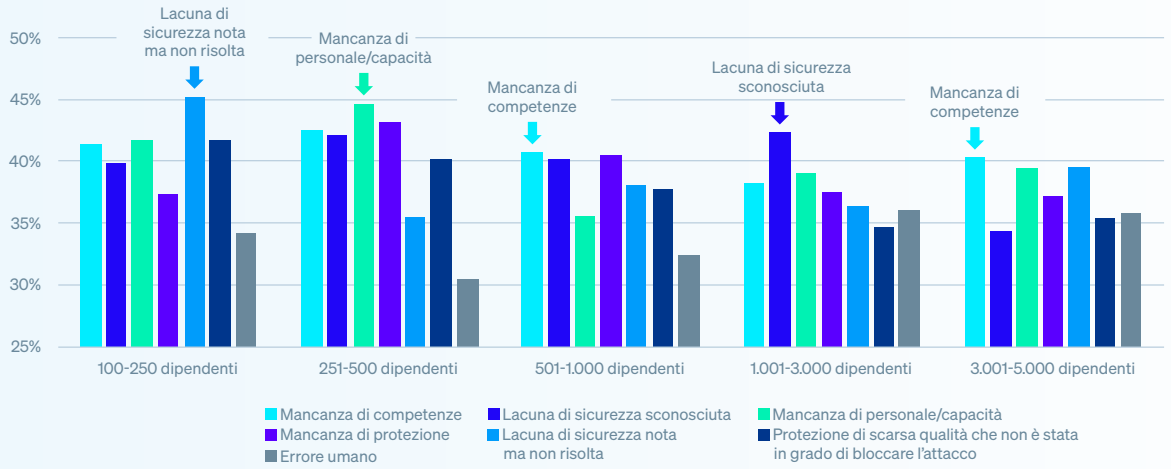



Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=3.400

## Causa operativa all'origine dell'attacco, in base alle dimensioni dell'azienda

Il più comune motivo organizzativo per cui le aziende vengono colpite dal ransomware varia a seconda delle dimensioni dell'organizzazione, in linea con le diverse sfide affrontate. Nelle cinque fasce utilizzate in questo report per rappresentare le dimensioni delle aziende in base al numero di dipendenti, tra i fattori che hanno contribuito agli attacchi sono emerse quattro sfide principali, come mostra il grafico seguente.

**Grafico 4: Causa operativa all'origine degli attacchi, con risultati suddivisi in base alle dimensioni dell'organizzazione**




Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=3.400. Risultati suddivisi in base alle dimensioni dell'organizzazione (numero di dipendenti)

## Causa operativa all'origine dell'attacco, in base al settore

Analogamente, la causa operativa all'origine dell'attacco varia anche a seconda del settore, il che riflette le diverse tipologie di sfide affrontate dalle aziende. È importante sottolineare che nessuno dei settori ha indicato l'"errore umano" come motivo principale per cui l'organizzazione ha subito l'attacco ransomware.

**Grafico 5: Principale causa operativa all'origine degli attacchi ransomware, in base al settore**

* Indica la presenza di più di una causa principale all'origine degli attacchi.

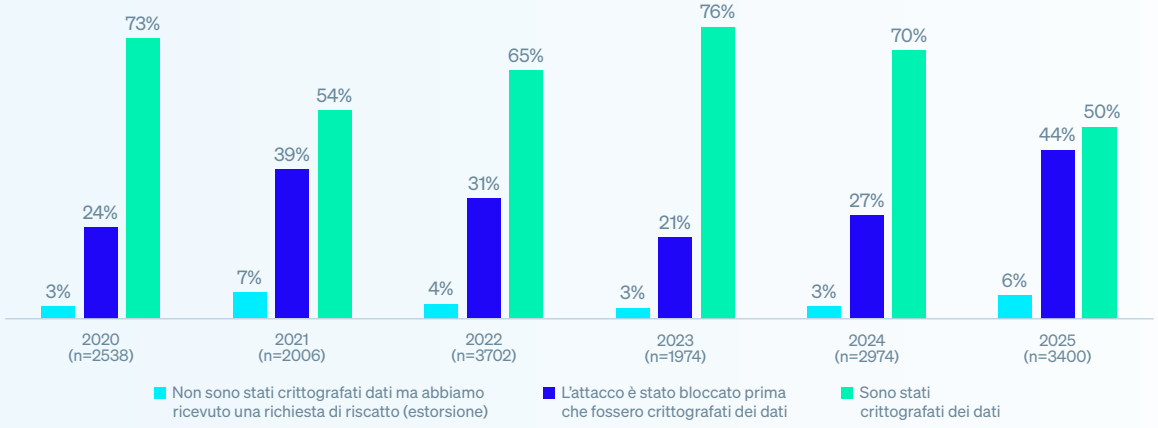
Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=3.400. Risultati suddivisi in base al settore

# Cosa succede ai dati

## Crittografia dei dati

Un dato incoraggiante è che il tasso di crittografia non autorizzata dei dati è stato il più basso tra quelli registrati nei sei anni di questo studio di ricerca, in quanto i dati sono stati crittografati nel 50% degli attacchi. Negli ultimi 12 mesi si è registrata una diminuzione significativa della percentuale di attacchi che hanno portato alla crittografia non autorizzata dei dati: dal 70% del sondaggio del 2024, sono infatti scesi al 50% nel 2025. Questa differenza suggerisce che le organizzazioni hanno una maggiore capacità di bloccare gli attacchi prima che venga distribuito il payload di crittografia.

**Grafico 6: Tasso di crittografia dei dati negli attacchi ransomware, 2020-2025**




Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico.

Le organizzazioni più grandi che hanno partecipato alla ricerca sono state quelle con la maggiore probabilità di subire la crittografia non autorizzata dei dati: il 65% degli attacchi contro organizzazioni con 3.001-5.000 dipendenti hanno infatti portato alla crittografia dei dati, il più alto tasso di crittografia segnalato in tutte le coorti dello studio. Questo indica che, rispetto alle piccole imprese, le organizzazioni più grandi hanno una capacità minore di rilevare e bloccare un attacco prima della crittografia, e/o che sono meno frequentemente in grado di bloccare le attività di crittografia non autorizzata e ripristinare i file allo stato pre-attacco.

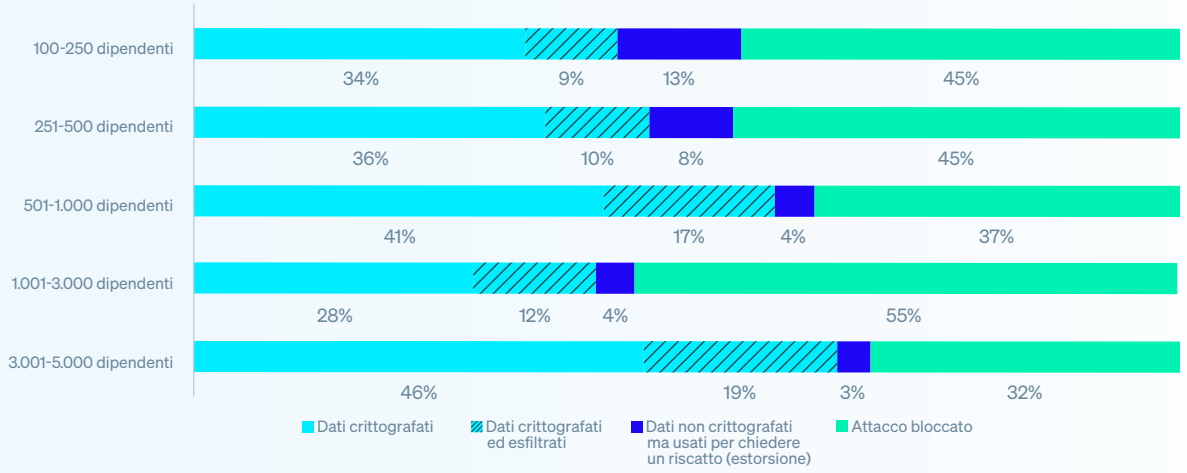
## Furto dei dati

I cybercriminali non si limitano solo a crittografare i dati, ma se ne appropriano anche illecitamente. Il 14% di tutte le organizzazioni attaccate dal ransomware e il 28% di quelle i cui dati erano stati crittografati sono anche cadute vittima del furto dei dati. Analizzando le statistiche in base alle dimensioni dell'azienda, si nota che le organizzazioni più piccole hanno quasi il 40% in meno di probabilità di subire il furto dei dati, rispetto a quelle più grandi.

- Il 22% delle organizzazioni con 100-500 dipendenti i cui dati erano stati crittografati ha subito anche il furto dei dati.
- Il 30% delle organizzazioni con 501-5.000 dipendenti i cui dati erano stati crittografati ha subito anche il furto dei dati.

Nonostante ci sia la possibilità che le organizzazioni più piccole abbiano una maggiore capacità di prevenire il furto dei dati rispetto a quelle più grandi, la differenza potrebbe essere dovuta al fatto che è molto più probabile che gli autori degli attacchi cerchino di esfiltrare dati dalle organizzazioni di grandi dimensioni, nonché alla possibilità che le aziende più piccole siano meno in grado di determinare se siano stati sottratti dati.

**Grafico 7: Tasso di crittografia dei dati negli attacchi ransomware, con risultati suddivisi in base alle dimensioni dell'organizzazione**




Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? n=3.400

## Attacchi di estorsione

Come indicato nel Grafico 6, l'anno scorso la percentuale di organizzazioni che non ha subito la crittografia dei dati ma ha comunque ricevuto una richiesta di riscatto (estorsione) è raddoppiata, salendo al 6% degli attacchi nel 2025, rispetto ad appena il 3% nel 2024. Rispetto a quelle più grandi, le organizzazioni di piccole dimensioni hanno una probabilità minore di ricevere richieste di riscatto senza che siano stati crittografati dati (attacco di estorsione):

- Il 13% delle organizzazioni con 100-250 dipendenti colpite dagli attacchi hanno subito un attacco di estorsione.
- Il 3% delle organizzazioni con 3.001-5.000 dipendenti colpite dagli attacchi hanno subito un attacco di estorsione.

Complessivamente, le organizzazioni con 1.001-3.000 dipendenti sono quelle maggiormente in grado di prevenire le ripercussioni di un attacco ransomware (ovvero sono riuscite a impedire che i dati venissero crittografati o esfiltrati, e ad evitare i tentativi di estorsione). È possibile che queste organizzazioni si trovino nel perfetto punto di equilibrio per cui hanno dimensioni abbastanza grandi per poter contare su strumenti e competenze di cybersecurity elevate, senza però presentare gli stessi livelli di complessità organizzativa delle grandi imprese.

## Recupero dei dati crittografati

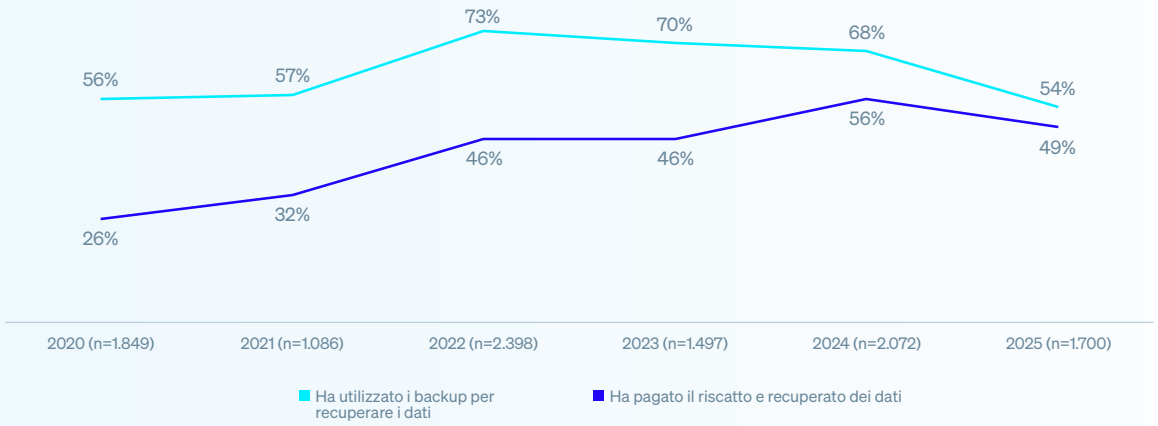
Il 97% delle organizzazioni che hanno partecipato al sondaggio, i cui dati erano stati crittografati sono state in grado di recuperarli.

A ripristinare i dati dai backup sono state poco più della metà (54%): è il terzo anno consecutivo che si osserva una diminuzione in questa statistica. Complessivamente, il recupero dei dati con i backup ha toccato il tasso più basso registrato in questi sei anni.

Poco meno della metà (49%) degli intervistati sostiene di aver pagato il riscatto e aver recuperato i dati in questo modo. Anche se si tratta di un leggero calo rispetto al 56% dell'anno scorso, è pur sempre il secondo più alto tasso di pagamento del riscatto riscontrato negli ultimi sei anni.

Il 29% dei partecipanti che hanno subito la crittografia non autorizzata dei dati sostengono di aver utilizzato "altri metodi" per riappropriarsi dei dati. Con molta probabilità, questi metodi includono l'utilizzo di chiavi di decrittografia che erano state rese pubbliche in passato.

**Grafico 8: Recupero dei dati tramite backup e tramite pagamento del riscatto, 2020-2025**




La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato i backup per recuperare i dati. Base di partecipanti indicata

# Riscatti

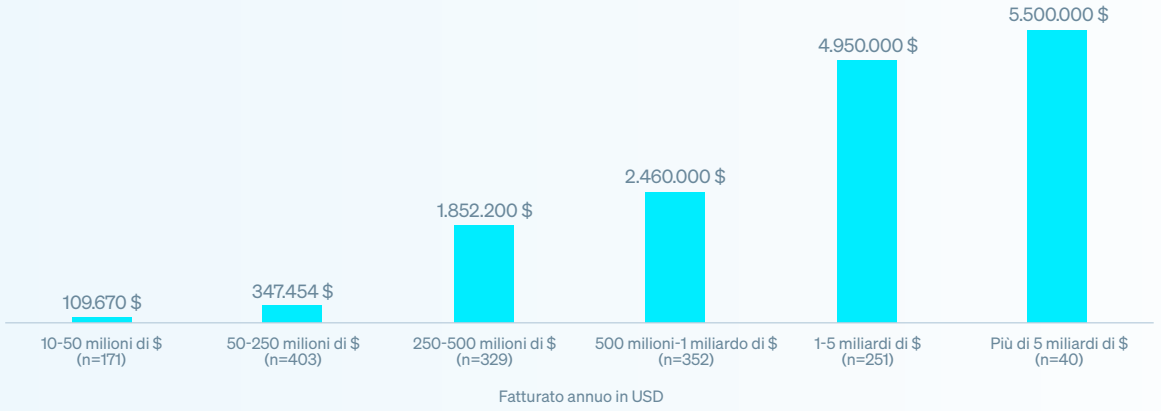
## Richieste di riscatto

La somma media (mediana) delle richieste di riscatto è diminuita di un terzo (34%) negli ultimi 12 mesi: quest'anno ammonta infatti a 1.324.439 $, mentre nel 2024 era arrivata a 2 milioni di $. Questo calo è dovuto principalmente a una diminuzione delle richieste di riscatto pari a 5 o più milioni di $, che è scesa dal 30% al 24%. Sebbene questa differenza sia sicuramente un buon segno, è importante tenere presente che il 57% delle richieste di riscatto ammonta a 1 o più milioni di $.

Le richieste di riscatto aumentano in maniera direttamente proporzionale al fatturato delle organizzazioni, il che suggerisce che i cybercriminali stabiliscono il "prezzo" del riscatto in base alla capacità di pagamento percepita della vittima:

- 109.670 $: cifra di riscatto media per le organizzazioni con un fatturato annuo di 10-50 milioni di $.
- 5.500.000 $: cifra di riscatto media per le organizzazioni con un fatturato annuo pari o superiore a 5 miliardi di $.

**Grafico 9: Richieste di riscatto, con risultati suddivisi in base al fatturato annuo**




A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? Base di partecipanti indicata nel grafico.

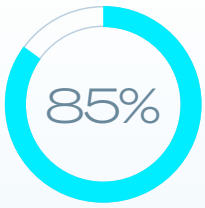
## Pagamento del riscatto

La cifra media (mediana) per il pagamento del riscatto è scesa del 50% l'anno scorso, passando da 2 milioni di $ nel 2024 a 1 milione di $ nel 2025. Proprio come nel caso delle richieste di riscatto, la principale causa di questo calo del pagamento del riscatto mediano è l'abbassamento del tasso dei pagamenti del riscatto di 5 o più milioni di $, che è scesa dal 31% nel 2024 al 20% nel 2025.

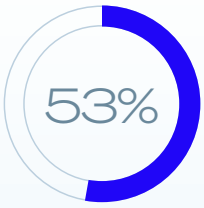
Anche se sia le richieste che i pagamenti di riscatto sono diminuiti l'anno scorso, è sicuramente un buon segno che i pagamenti abbiano registrato il calo più significativo. Detto questo, 1 milione di $ rimane pur sempre una somma molto alta, che può causare gravi conseguenze per la maggior parte delle organizzazioni.

## Confronto tra pagamenti effettivi e richieste di riscatto iniziali

826 delle organizzazioni che hanno pagato il riscatto hanno condiviso sia la richiesta iniziale dei cybercriminali, che la somma effettiva pagata. I risultati rivelano che queste vittime hanno pagato in media l'85% della richiesta di riscatto iniziale. Complessivamente, nel 53% dei casi hanno pagato meno della somma richiesta, nel 18% hanno pagato di più e nel 29% degli incidenti si sono attenute alla richiesta iniziale.

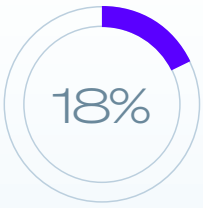



della somma di riscatto richiesta **è stata pagata**, in media




dei pagamenti sono stati **meno** della richiesta di riscatto iniziale

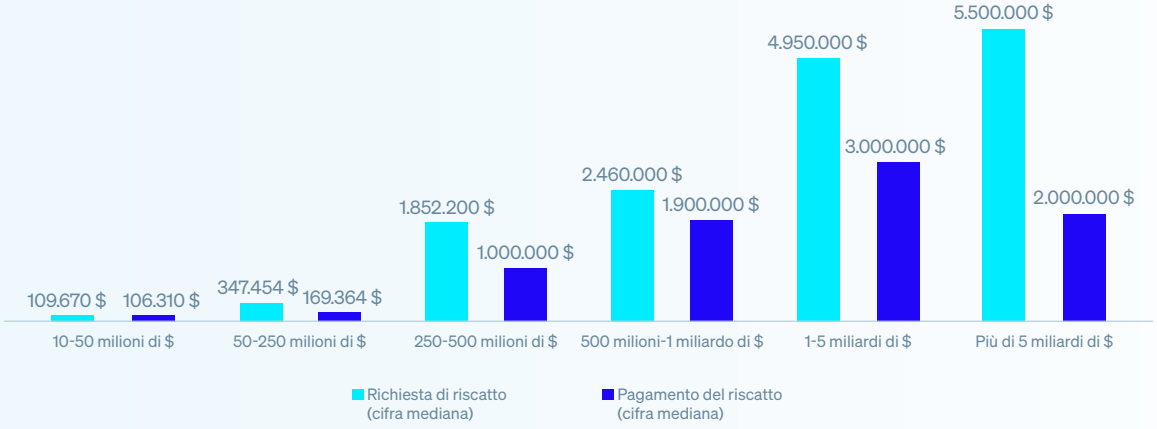
dei pagamenti sono stati **pari** alla richiesta di riscatto iniziale




dei pagamenti sono stati **più** della richiesta di riscatto iniziale

Suddividendo i dati in base al fatturato annuo, si osserva che tutte le coorti di fatturato hanno pagato in media meno della richiesta iniziale. Tuttavia, le organizzazioni più grandi (con fatturato annuo di 5 o più miliardi di $) hanno riscontrato il calo più significativo, in quanto la media del pagamento effettivo per queste aziende (2 milioni di $) rappresenta appena il 36% della richiesta di riscatto iniziale ricevuta (5,5 milioni di $), a parte alcuni valori aberranti. Le organizzazioni con 10-50 milioni di $ di fatturato annuo hanno invece registrato la diminuzione meno alta, con un pagamento mediano pari al 97% della richiesta mediana.

**Grafico 10: Confronto tra le richieste e i pagamenti di riscatto, con risultati suddivisi in base al fatturato annuo**




A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali? (n=1.552/836)

## Perché nella maggior parte dei casi c'è una differenza tra i pagamenti del riscatto e la somma richiesta inizialmente?

Quest'anno abbiamo esplorato per la prima volta i motivi per cui alcune organizzazioni pagano più della richiesta di riscatto iniziale e perché altre pagano meno, offrendo una nuova prospettiva su un ambito importante della gestione degli attacchi ransomware.

151 organizzazioni che **hanno pagato più** della richiesta iniziale hanno rivelato che:

- 50% degli intervistati: i cybercriminali erano convinti che potevamo permetterci di pagare di più.
- 48% degli intervistati: i cybercriminali hanno capito che eravamo un bersaglio di alto valore.
- 38% degli intervistati: i cybercriminali si sono infastiditi e hanno aumentato il riscatto.
- 38% degli intervistati: i nostri backup non hanno funzionato o presentavano difetti.
- 32% degli intervistati: non abbiamo pagato abbastanza rapidamente, quindi la somma è salita.

Tipicamente, le organizzazioni hanno indicato due fattori alla base della decisione di pagare di più, rivelando così le molteplici sfide che le vittime si trovano ad affrontare quando cercano di recuperare i propri dati.

445 organizzazioni che hanno **pagato meno** della cifra di riscatto richiesta inizialmente hanno condiviso come sono riuscite a ridurre la somma:

- 47% degli intervistati: abbiamo negoziato una cifra più bassa con i cybercriminali.
- 45% degli intervistati: i cybercriminali hanno ridotto la richiesta iniziale per via di pressioni esterne (ad es. da parte dei media o delle forze dell'ordine).
- 45% degli intervistati: i cybercriminali hanno diminuito la richiesta per convincerci a pagare.
- 43% degli intervistati: abbiamo pagato il riscatto velocemente, così abbiamo usufruito di uno sconto.
- 40% degli intervistati: una terza parte ha negoziato con i cybercriminali per ridurre la cifra iniziale.

Questa coorte ha anche fornito , in media, due fattori alla base dei pagamenti di una somma minore di riscatto rispetto a quella iniziale, evidenziando ulteriormente la natura complessa e poliedrica della situazione affrontata dalle vittime del ransomware.

# Le conseguenze commerciali del ransomware

## Costi di riparazione dei danni

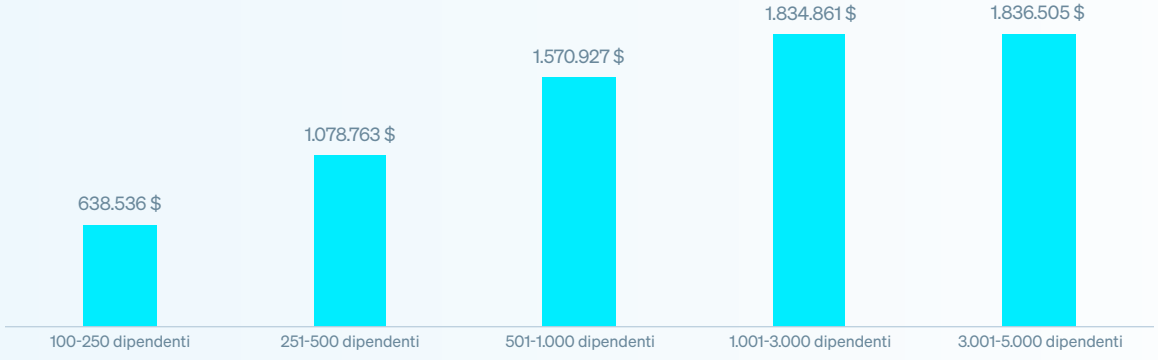
L'anno scorso il costo medio della riparazione dei danni di un attacco ransomware (escludendo eventuali somme di riscatto pagate) è sceso a 1,53 milioni di $, con un calo del 44% rispetto ai 2,73 milioni di $ del 2024. È anche poco più di 300.000 $ inferiore alla somma registrata nel 2023.

| 2023 | 2024 | 2025 |
|---|---|---|
| 1,82 Mio di $ | 2,83 Mio di $ | 1,53 Mio di $ |

Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.), escludendo eventuali pagamenti del riscatto? n=3.400 (2025), n=2.974 (2024), n=1.974 (2023)

I costi di riparazione dei danni aumentano parallelamente alle dimensioni dell'organizzazione della vittima, per poi fermarsi con le organizzazioni che hanno da 1.000 a 5.000 dipendenti. Le organizzazioni con 100-250 dipendenti segnalano un costo medio di riparazione dei danni di 638.536 $, mentre quelle con 1.000-5.000 dipendenti hanno dovuto sostenere costi pari a 1,83 milioni di $.

**Grafico 11: Costi di riparazione dei danni del ransomware, con risultati suddivisi in base alle dimensioni dell'azienda**

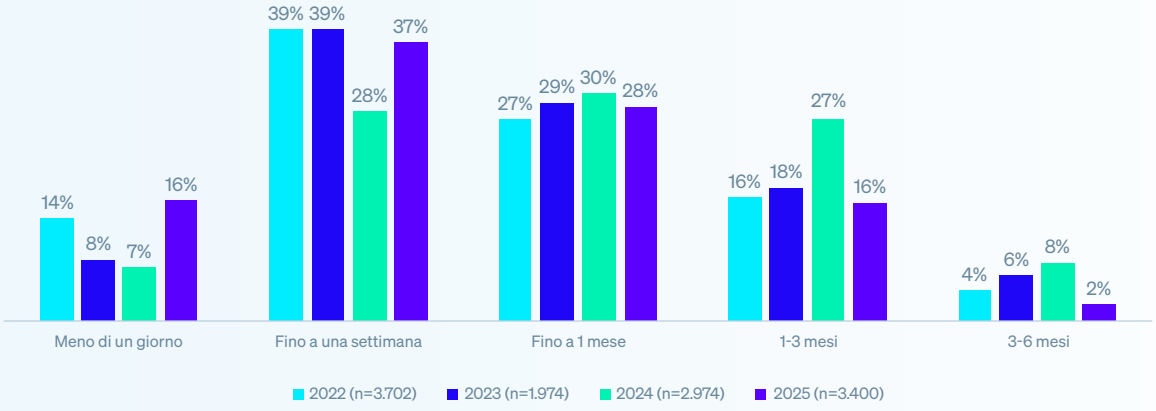



Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.), escludendo eventuali pagamenti del riscatto? n=3.400

## Tempi necessari per riprendere le normali attività

Dai dati emerge che le organizzazioni hanno accorciato i tempi necessari per riprendere le normali attività in seguito a un attacco, con il 16% degli intervistati che hanno impiegato un giorno: una statistica in aumento rispetto al 7% del 2024 e all'8% del 2023. Oltre la metà (53%) dei partecipanti ha ripreso le normali attività in meno di una settimana, un balzo significativo rispetto al 35% registrato nel 2024. Nel complesso, quasi tutte le vittime (97%) sono tornate completamente operative entro tre mesi dopo l'attacco. Questo miglioramento dei tempi di ripresa potrebbe indicare che l'anno scorso le organizzazioni hanno investito nel prepararsi agli incidenti informatici e alla riparazione dei danni.

**Grafico 12: Tempi necessari per tornare alla normalità operativa in seguito a un attacco ransomware, 2022-2025**



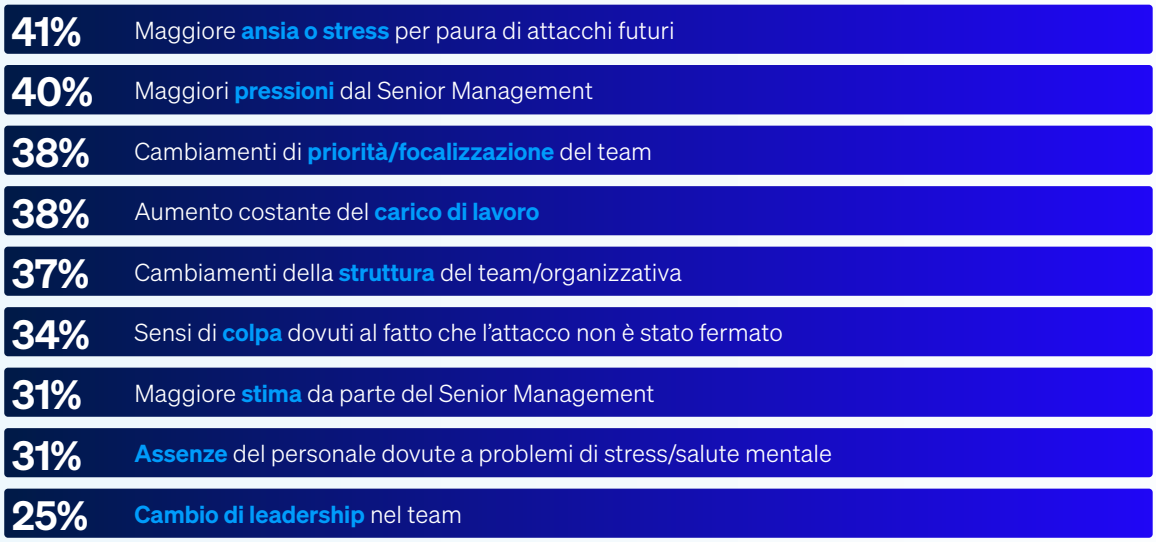

Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware?
Base di partecipanti indicata nel grafico

Non sorprende il fatto che, tipicamente, le organizzazioni che avevano subito la crittografia non autorizzata dei dati sono state più lente a riprendersi rispetto a quelle che erano riuscite a prevenirla: Nel 9% dei casi le aziende i cui dati erano stati crittografati sono tornate operative entro un giorno, mentre questa statistica sale al 24% per le organizzazioni che sono riuscite a impedire ai cybercriminali di crittografare i dati.

# Le conseguenze umane del ransomware

Il sondaggio indica chiaramente che subire la crittografia non autorizzata dei dati durante un attacco ransomware implica ripercussioni molto serie per i team IT/di cybersecurity, in quanto tutti gli intervistati sostengono che il proprio team ne ha risentito in qualche misura.

**Grafico 13: Le conseguenze della crittografia non autorizzata dei dati sui team IT/di cybersecurity**




Quali ripercussioni (se presenti) ha avuto l'attacco ransomware sui membri del tuo team IT/di cybersecurity? n=1.700

# Raccomandazioni

Sebbene nell'ultimo anno ci siano stati diversi cambiamenti nelle esperienze con il ransomware delle organizzazioni, questa minaccia continua a rappresentare un serio pericolo per tutte le aziende. Con cybercriminali che continuano a replicare ed evolvere i loro attacchi, è fondamentale che i team di sicurezza e le difese informatiche delle organizzazioni non restino indietro, per poter tener testa al ransomware e ad altre minacce. Utilizza gli approfondimenti di questo report per potenziare le tue difese, ottimizzare le tue attività di risposta alle minacce e limitare l'impatto del ransomware sia sulla tua azienda che sui dipendenti. Concentrati su questi quattro ambiti per tenerti un passo avanti rispetto agli attacchi:

- **Prevenzione**. La difesa più efficace contro il ransomware è quella che lo previene del tutto, perché impedisce ai cybercriminali di compromettere la tua organizzazione. Adotta misure adeguate per eliminare le cause tecniche e operative all'origine degli attacchi che sono state indicate in questo report.
- **Protezione**. Avere una solida base di sicurezza è un must. Gli endpoint (server inclusi) sono l'obiettivo iniziale primario per i cybercriminali del ransomware, per cui è importante assicurarsi che vengano difesi adeguatamente, con una protezione antiransomware dedicata, in grado di bloccare i tentativi di crittografia non autorizzata e ripristinare i file allo stato pre-attacco.
- **Rilevamento e risposta**. Prima viene bloccato un attacco, migliori saranno i risultati. Un sistema di rilevamento e risposta alle minacce attivo 24/7 è un livello di difesa a cui ormai non è possibile rinunciare. Se non hai le risorse o le competenze necessarie per implementarlo e gestirlo internamente, cerca di collaborare con un fornitore di servizi MDR (Managed Detection and Response).
- **Pianificazione e preparazione**. Poter contare su un piano strategico di incident response con cui hai già acquisito familiarità migliorerà notevolmente i risultati, qualora succedesse il peggio e la tua organizzazione dovesse subire un attacco grave. Assicurati di eseguire backup di alta qualità e svolgi esercitazioni regolari di ripristino dei dati per accelerare il ritorno alla normalità operativa nel caso in cui i tuoi sistemi dovessero essere colpiti.

Per esplorare come Sophos può aiutarti a ottimizzare le tue difese antiransomware, parla con un consulente o visita www.sophos.it

## Scopri di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione.

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

© Copyright 2025. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con Nº 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

2025-06-25 WP (DD)

SOPHOS