SOPHOS

LA VERA STORIA DEL RANSOMWARE PER LE GRANDI IMPRESE 2025

I risultati di uno studio indipendente a cui hanno partecipato 1.733 IT e Cybersecurity Manager di grandi imprese che sono state colpite dal ransomware l'anno scorso.

Whitepaper Sophos. 2025 dicembre

Introduzione

Ti diamo il benvenuto alla prima edizione del report annuale di Sophos “La vera storia del ransomware per le grandi imprese”, che rivela le dinamiche del malware nel 2025 per le imprese di grandi dimensioni (oltre 1.000 dipendenti).

Il report di quest’anno mostra l’evoluzione delle esperienze con il ransomware (tanto le cause, quanto le conseguenze) delle grandi imprese nel corso degli ultimi 12 mesi. Inoltre, offre una nuova prospettiva sui fattori operativi che hanno esposto le grandi imprese agli attacchi, nonché l’impatto umano degli incidenti sui team IT/di cybersecurity.

Basandosi sulle esperienze reali vissute in prima persona da 1.733 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 grandi imprese vengono colpite dal ransomware.
- Cosa succede ai dati.
- I riscatti: richieste e pagamenti.
- L’impatto commerciale del ransomware.
- L’impatto umano del ransomware.

Informazioni sul sondaggio

Il report è basato sui risultati di una ricerca indipendente e vendor-agnostic svolta per conto di Sophos, che valuta le esperienze delle organizzazioni con il ransomware. Un’azienda indipendente specializzata ha condotto il sondaggio tra gennaio e marzo 2025. A tutti i partecipanti che lavorano in grandi imprese con un numero di dipendenti compreso tra 1.000 e 5.000 è stato chiesto di rispondere tenendo in considerazione le proprie esperienze nei 12 mesi precedenti.

I 1.733 intervistati in questi tipi di aziende che hanno contribuito al report provengono da 17 paesi e 14 settori, per garantire che i risultati del sondaggio riflettano una selezione ampia e diversificata di esperienze. Il report include comparazioni con i dati raccolti nell’ambito dei nostri studi di ricerca precedenti, per un raffronto annuo. Tutti i dati finanziari sono espressi in dollari U.S.A.

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 consapevoli del fatto che i partecipanti condividono le loro esperienze nel corso dell’anno precedente, per cui molti degli attacchi menzionati, nonché il rispettivo impatto, si riferiscono al 2024.

I risultati salienti

Perché le grandi imprese vengono colpite dal ransomware

- Gli **exploit delle vulnerabilità** sono stati la più comune causa tecnica all'origine degli attacchi, essendo stati utilizzati nel 29% degli incidenti. Il **phishing** e le **credenziali compromesse** seguono a distanza ravvicinata a pari merito, avendo svolto un ruolo fondamentale nel 21% degli incidenti.
- Le organizzazioni di grandi dimensioni sono state colpite dal ransomware per via di diversi fattori operativi, il più ricorrente dei quali sono le **lacune di sicurezza sconosciute**, segnalate dal 40% delle vittime. Seguono a breve distanza la **mancanza di personale/capacità** e la **mancanza di competenze**, che hanno contribuito al 39% degli attacchi.

Cosa succede ai dati

- La crittografia dei dati come conseguenza degli attacchi nelle grandi imprese è scesa al livello più basso in cinque anni, in quanto è stata **riscontrata nel 49% dei casi**: una percentuale in calo rispetto al picco del 64% nel 2022.
- Il 30% delle organizzazioni di grandi dimensioni che avevano subito la crittografia non autorizzata dei dati sono cadute vittima anche dell'esfiltrazione dei dati.
- Il 96% delle grandi imprese che hanno partecipato al sondaggio, i cui dati erano stati crittografati, è stato in grado di recuperarli.
- L'utilizzo di backup da parte di queste organizzazioni per ripristinare i dati crittografati ha toccato il punto più basso negli ultimi sei anni, essendo stato osservato nel 53% degli incidenti.
- Il **48% delle vittime nella grandi imprese ha pagato il riscatto** per riavere i propri dati: uno dei più bassi tassi registrati nel sondaggio di quest'anno.

Riscatti: le richieste e i pagamenti

- La somma media (mediana) delle **richieste di riscatto** nei confronti delle grandi imprese è diminuita del 56% negli ultimi 12 mesi, arrivando a **1,20 milioni di $** nel 2025, in contrasto con i 2,75 milioni di $ del 2024. La principale causa di questo ribasso è una diminuzione del 24% nel tasso delle richieste del riscatto pari a 5 o più milioni di $, che è passato dal 38% delle richieste nel 2024 al 29% nel 2025. Tuttavia, è importante tenere presente che c'è stato un incremento del 17% nelle richieste con somme comprese tra 1 e 5 milioni di $.
- Anche la somma media (mediana) **pagata per il riscatto** dalle grandi imprese è diminuita, raggiungendo **1 milione di $** nel 2025, rispetto agli 1,26 milioni di $ del 2024. Il calo è in gran parte dovuto a una diminuzione del 37% osservata nel tasso di pagamenti del riscatto pari o superiori a 5 milioni di $. Occorre tuttavia sottolineare che è stato riscontrato un aumento in quasi tutte le fasce di pagamento sotto i 5 milioni di $.
- La **percentuale delle richieste di riscatto che sono state pagate** dalle aziende di grandi dimensioni nel 2025 è infatti scesa all'86%, rispetto al 95% del 2024.
- Analizzando attentamente **le richieste rispetto ai pagamenti**, il pagamento finale è stato pari alla richiesta iniziale in quasi un terzo (31%) degli intervistati nelle grandi imprese. Nel 51% degli incidenti, le vittime hanno pagato meno della richiesta iniziale, mentre nell'18% dei casi hanno pagato di più.

L'impatto commerciale del ransomware

- L'anno scorso il **costo per il recovery in seguito all'attacco ransomware nelle grandi imprese** è sceso del 41%, con **1,84 milioni di $**, in calo rispetto ai 3,12 milioni di $ del 2024.
- Analizzando il **tempo necessario per tornare alla normalità operativa**, viene rilevato che queste organizzazioni si riprendono dagli attacchi con maggiore rapidità, con la metà esatta degli intervistati che sostiene di aver ripreso le normali attività dopo una settimana nel 2025, una statistica in aumento rispetto al 36% del 2024.

L'impatto umano del ransomware

Tutte le grandi imprese che avevano subito la crittografia non autorizzata dei dati confessano che ci sono state ripercussioni dirette sui loro team IT/di cybersecurity:

- Il 40% dei team IT/di cybersecurity ha subito **maggiori pressioni** dal Senior Management, mentre il 31% ha notato un **maggiore riconoscimento del proprio ruolo**.
- Il 39% ha registrato un **aumento costante del carico di lavoro** e **maggiore ansia o stress** per paura di attacchi futuri.
- Il 37% indica di aver riscontrato un **cambiamento di priorità/focalizzazione del team**.
- Più di un terzo (35%) degli intervistati dichiara sia di aver provato **sensi di colpa** dovuti al fatto che l'attacco non è stato fermato, sia di aver notato **cambiamenti della struttura del team/organizzativa**, come conseguenze dell'incidente.
- Nel 31% dei team sono state osservate **assenze del personale** dovute a problemi di stress/salute mentale correlati all'attacco.
- In più di un quarto di questi casi (27%), c'è stato un **cambio di leadership** nel team come conseguenza dell'attacco.

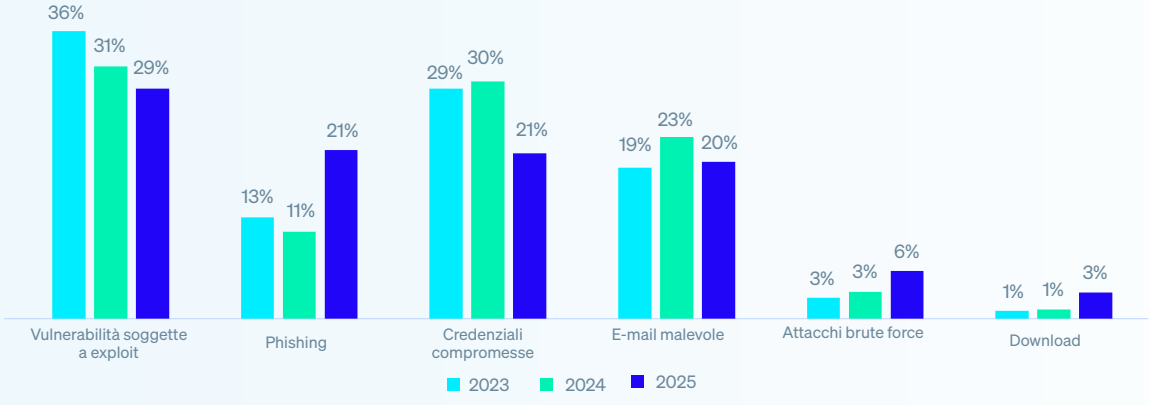
Perché le grandi imprese vengono colpite dal ransomware

Causa tecnica all'origine degli attacchi nelle grandi imprese

Per il terzo anno consecutivo, le vittime nelle organizzazioni di grandi dimensioni identificano nelle **vulnerabilità soggette a exploit** la principale causa originaria degli attacchi ransomware, essendo state sfruttate nel 29% degli incidenti. Le **e-mail di phishing** si trovano al secondo posto, in aumento rispetto all'11% del 2024 e al 21% del 2025.

Gli **attacchi che sfruttano le credenziali** continuano a costituire un rischio significativo, sebbene le segnalazioni di questo vettore di attacco siano in netto declino, essendo passate dal 30% del 2024 al 21% del 2025. Invece, per le **piccole e medie imprese** (PMI), ovvero quelle con 100-250 dipendenti, sono gli attacchi che sfruttano le credenziali a rappresentare la principale root cause degli incidenti di ransomware, in quanto risultano coinvolti in quasi un terzo (30%) dei casi.

Grafico 1: Causa tecnica all'origine degli attacchi ransomware nelle grandi imprese, 2023-2025

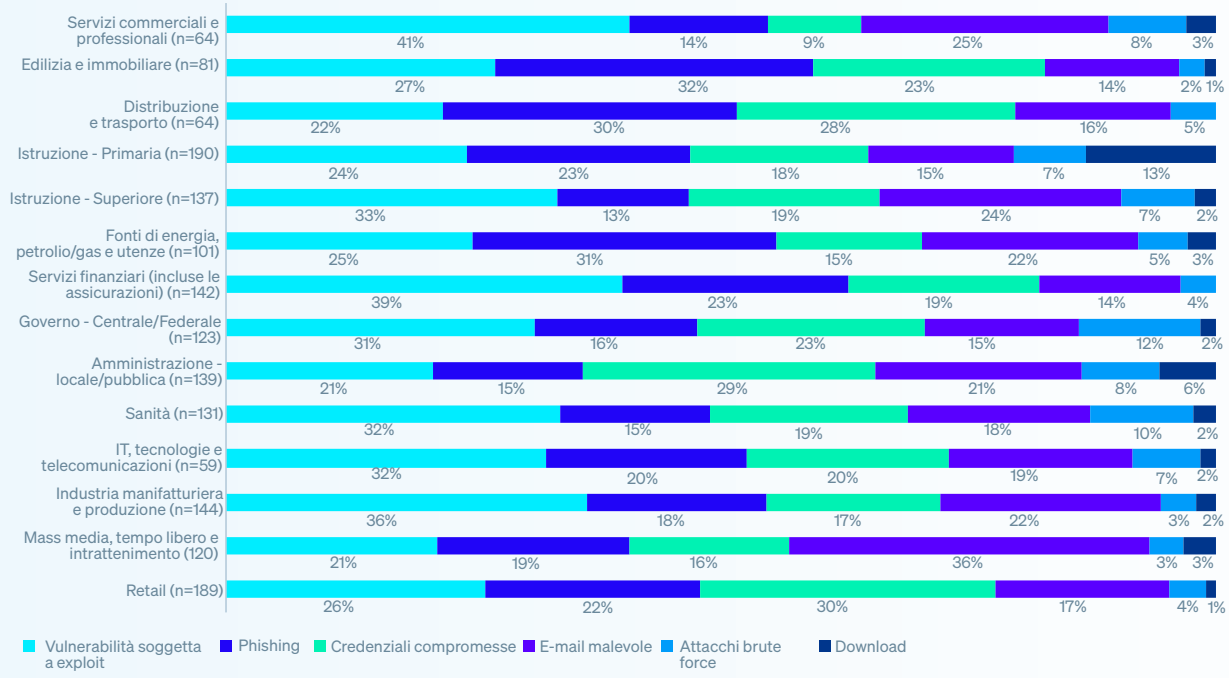


Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. n=1.733 (2025), n=1.409 (2024), n=1.045 (2023).

La ricerca rivela che, sebbene la causa originaria vari in base al settore, le vulnerabilità soggette a exploit sono uno dei principali vettori di attacco per le grandi imprese nella maggior parte dei settori. Eccezioni significative:

- Il **phishing** è stata la più comune causa originaria sia nel settore dell'**edilizia e immobiliare** (32%), che in quello di **distribuzione e trasporto** (30%), nonché per i fornitori di **fonti di energia, petrolio/gas e utenze** (31%).
- Le **credenziali compromesse** si trovano al primo posto nella classifica dei più comuni vettori di attacco percepiti per le grandi imprese che operano nel **retail**, in quanto costituiscono quasi un terzo degli incidenti (30%).

Grafico 2: Causa tecnica all'origine degli attacchi ransomware, con risultati suddivisi in base al settore

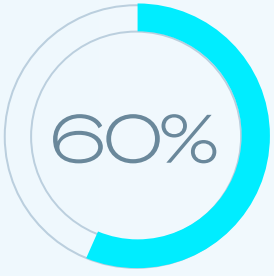


Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. Base di partecipanti indicata nel grafico.

Causa originaria degli incidenti inerente a fattori organizzativi nelle grandi imprese

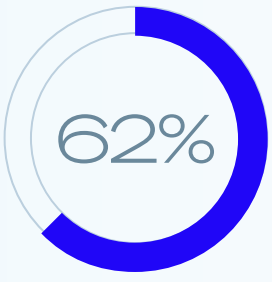
Insieme alle cause originarie degli incidenti, è utile anche comprendere i fattori organizzativi che hanno esposto le grandi imprese al rischio di attacco. Dai risultati emerge che di solito le vittime in queste aziende si trovano ad affrontare varie sfide organizzative, in quanto gli intervistati citano una media di tre fattori che hanno contribuito a renderli un bersaglio per gli attacchi ransomware.

Complessivamente, le cause originarie inerenti a fattori organizzativi sono suddivise in maniera piuttosto equa tra le seguenti categorie: problemi di protezione, difficoltà in termini di risorse e lacune di sicurezza. Tuttavia, le grandi imprese hanno una probabilità leggermente maggiore di segnalare una lacuna di sicurezza (nota o sconosciuta) come fattore principale.



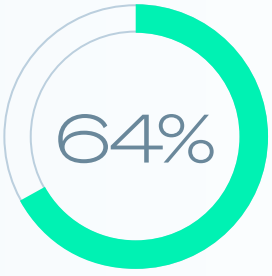
SCARSA QUALITÀ/ASSENZA DI SOLUZIONI DI PROTEZIONE

Mancanza di protezione o soluzioni di protezione di scarsa qualità, che non sono state in grado di bloccare l'attacco



MANCANZA DI PERSONALE/ COMPETENZE

Mancanza delle competenze umane (capacità o conoscenze) necessarie per rilevare e bloccare l'attacco in tempo



LACUNA DI SICUREZZA (NOTA/ SCONOSCIUTA)

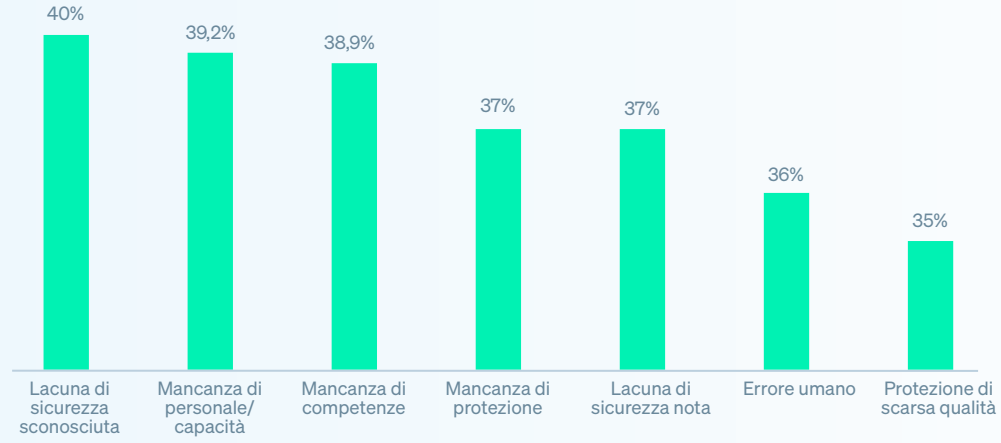
Vulnerabilità nota o sconosciuta nelle proprie difese

Perché ritieni che la tua organizzazione sia stata vittima dell'attacco ransomware? n=1.733. Risposte consolidate.

Le **lacune di sicurezza sconosciute** (ovvero una o più vulnerabilità nelle difese, di cui gli intervistati non erano a conoscenza) sono il singolo motivo principale indicato, in quanto sono state citate dal 40% delle aziende di grandi dimensioni. Seguono a distanza ravvicinata la **mancanza di personale/capacità** (ovvero una quantità insufficiente di esperti di cybersecurity che monitoravano i sistemi al momento dell'attacco) e la **mancanza di competenze** (ovvero la scarsa disponibilità delle capacità o delle conoscenze necessarie per rilevare e bloccare l'attacco in tempo), che hanno contribuito al 39% degli attacchi subiti da queste organizzazioni.

È degno di nota il fatto che anche per le **PMI** la mancanza di **personale/capacità** rappresenta un fattore molto comune, con il 42% dei partecipanti al sondaggio che lo menziona come uno dei motivi principali per cui le loro organizzazioni sono cadute vittima di un attacco. Questa statistica evidenzia quanto sia ancora diffuso il problema della disponibilità limitata di risorse, indipendentemente dalle dimensioni di un'organizzazione.

Grafico 3: Causa operativa all'origine degli attacchi ransomware nelle grandi imprese



Perché ritieni che la tua organizzazione sia statavittima dell'attacco ransomware? n=1.733.

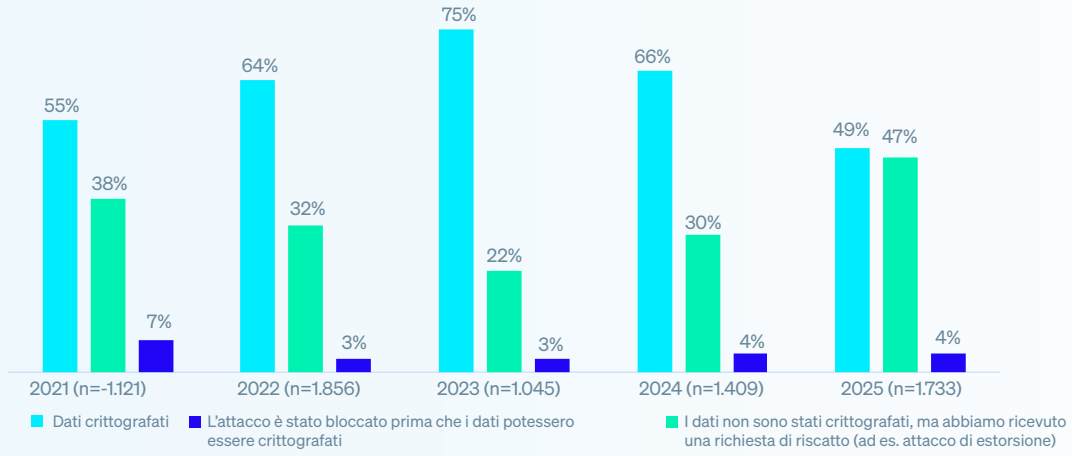
Cosa succede ai dati

La crittografia dei dati nelle grandi imprese

Un dato incoraggiante è che il tasso di crittografia non autorizzata dei dati nelle grandi imprese è stato il più basso tra quelli registrati nei cinque anni del nostro sondaggio, in quanto le informazioni sono state crittografate in poco meno della metà (49%) degli attacchi, in calo rispetto al 66% registrato nel 2024.

Allo stesso tempo, il tasso di attacchi ransomware bloccati prima della crittografia dei dati è più che raddoppiato negli ultimi due anni, salendo dal 22% del 2023 al 47% del 2025. Questo suggerisce che le grandi imprese stanno diventando più abili a rilevare e fermare gli attacchi prima che causino gravi danni.

Grafico 4: Tasso di crittografia dei dati negli attacchi ransomware subiti dalle grandi imprese, 2021-2025

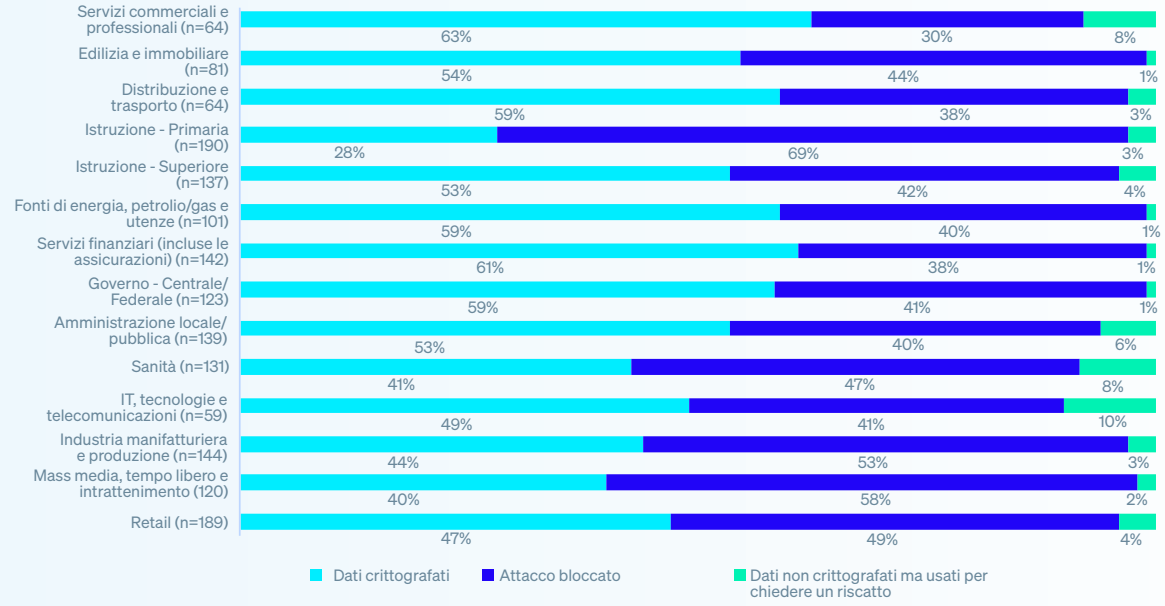


Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico.

Tassi di crittografia dei dati, in base al settore

Le grandi imprese nel settore dei **servizi commerciali e professionali** sono quelle con maggiore probabilità di subire la crittografia dei dati (63%), il che indica che hanno un minor tasso di successo nel rilevamento e nel blocco delle attività di crittografia non autorizzata e/o nel ripristino dei file allo stato pre-attacco. Gli intervistati che operano nel settore dell'**istruzione primaria** hanno invece registrato il più basso tasso di crittografia dei dati, con appena il 28%.

Grafico 5: Tassi di crittografia dei dati nelle grandi imprese, in base al settore



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

Furto dei dati

I cybercriminali non si limitano solo a crittografare i dati, ma se ne appropriano anche illecitamente. Il 15% di tutte le grandi imprese che sono state attaccate dal ransomware e il 30% di quelle i cui dati erano stati crittografati sono anche cadute vittima del furto dei dati. Analizzando le statistiche in base al settore, si osserva che:

- In cima alla classifica, il 52% delle aziende di grandi dimensioni nel settore **mass media, tempo libero e intrattenimento** ha subito sia la crittografia che il furto dei dati.
- In netto contrasto, solo l'11% delle grandi imprese che operano nel settore dell'**edilizia e immobiliare** ha dovuto affrontare sia il furto che la crittografia non autorizzata dei dati.

Attacchi a scopo di estorsione

Come mostra il Grafico 4, la percentuale di grandi imprese che sono riuscite a evitare la crittografia dei dati ma che hanno ricevuto una richiesta di riscatto è rimasta stabile al 4% rispetto all'anno scorso. Analizzando questa statistica in base al settore, le organizzazioni che operano nell'ambito di **IT, tecnologie e telecomunicazioni** sono state quelle maggiormente esposte a questi tipi di attacco (10%), mentre le imprese nel settore dell'**edilizia e immobiliare, i fornitori di fonti di energia, petrolio/gas e utenze, i servizi finanziari, e le organizzazioni appartenenti alla categoria governo centrale/federale** sono state quelle meno colpite, con appena l'1%.

Complessivamente, le imprese che operano nell'**istruzione primaria** sono quelle che si sono dimostrate maggiormente abili nel 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). Questo suggerisce che gli istituti scolastici primari dimostrano una sorprendente capacità di rilevamento e intervento, nonostante le limitazioni di budget.

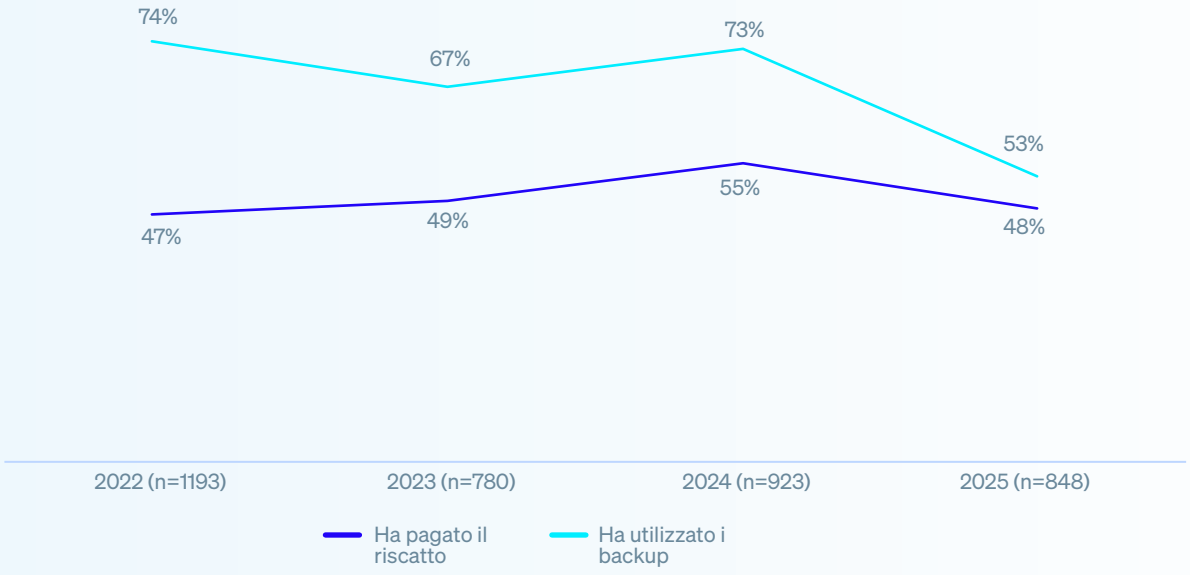
Recupero dei dati crittografati nelle organizzazioni di grandi dimensioni

Il 96% delle grandi imprese i cui dati erano stati crittografati sono riuscite a recuperarli.

Nel 2025, il 48% delle aziende di grandi dimensioni **ha pagato il riscatto per recuperare i dati**: in calo rispetto al 55% del 2024. Allo stesso tempo, l'**utilizzo di backup** ha subito un netto declino, scendendo al livello più basso osservato in quattro anni (53%, in calo rispetto al 73% del 2024). Complessivamente, questi risultati indicano una maggiore resistenza alle richieste di riscatto, pur in presenza di potenziali punti deboli e scarsa resilienza dei backup.

Inoltre, la riduzione del divario tra le grandi imprese che hanno pagato il riscatto per recuperare i dati e quelle che hanno invece eseguito il ripristino dai backup suggerisce una maggiore tendenza ad affidarsi a metodi di recupero multipli o alternativi. A dimostrazione di ciò, abbiamo constatato che quasi un terzo (30%) delle aziende di grandi dimensioni che avevano subito la crittografia dei dati ha dichiarato di aver **utilizzato altri metodi per recuperare le informazioni**. I metodi alternativi potevano includere il recupero dei dati da sistemi non colpiti, oppure da copie shadow, grazie alle funzionalità di ripristino allo stato pre-attacco offerte dalla protezione endpoint.

Grafico 6: Recupero dei dati crittografati nelle grandi imprese, 2021- 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 nel grafico.

Riscatti

Richieste di riscatto nelle grandi imprese

La somma media (mediana) delle richieste di riscatto nei confronti delle organizzazioni di grandi dimensioni è scesa del 56% negli ultimi 12 mesi, arrivando a 1,20 milioni di $ nel 2025, in calo rispetto ai 2,75 milioni di $ del 2024. La diminuzione delle richieste di pagamento del riscatto tra le grandi imprese è dovuta principalmente a una riduzione del 24% delle richieste di riscatto pari o superiori a 5 milioni di $ negli ultimi 12 mesi. Ciononostante, è importante tenere presente che è stato riscontrato un incremento del 17% nelle richieste con somme comprese tra 1 e 5 milioni di $ (che costituiscono il 27% di tutte le richieste di riscatto): in aumento rispetto al 23% del 2024.

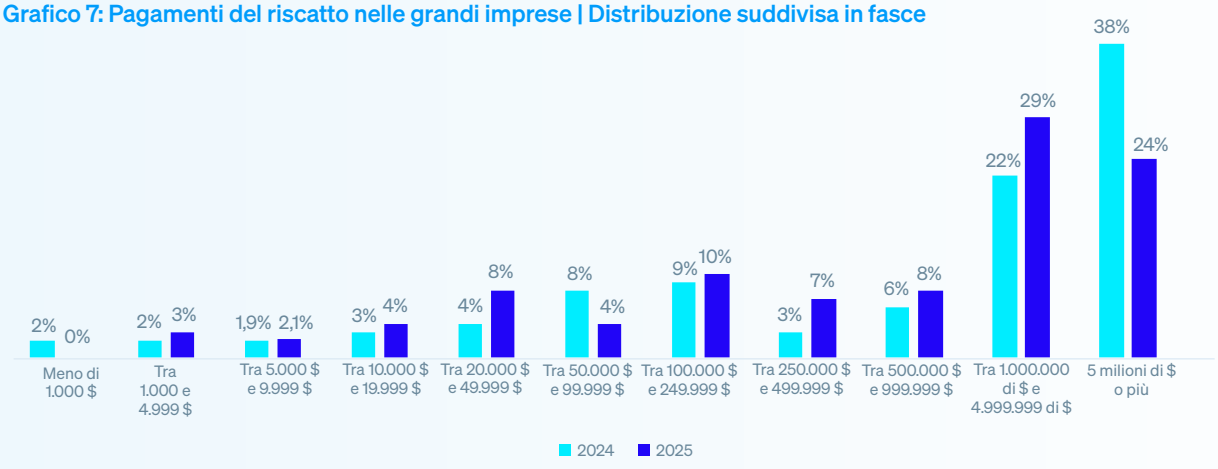
Pagamenti del riscatto nelle grandi imprese

In linea con questa tendenza, anche la somma media (mediana) pagata per il riscatto da queste aziende è scesa, passando da 1,26 milioni di $ nel 2024 ad appena 1 milione di $ nel 2025. Questo è dovuto in gran parte alla diminuzione del 37% dei pagamenti del riscatto pari a 5 o più milioni di $ nel corso degli ultimi 12 mesi. Tuttavia, effettuando un confronto con i dati dell'anno scorso, dal report sono emersi aumenti in quasi tutte le fasce di pagamento sotto i 5 milioni di $.

Queste tendenze suggeriscono che gli autori degli attacchi si stanno allontanando dalle richieste di riscatto più elevate per prendere di mira le grandi imprese puntando su importi di fascia media che, pur potendo causare gravi conseguenze, hanno maggiori probabilità di essere pagati.

Un simile modello è stato osservato anche per le **PMI**, sebbene la diminuzione delle richieste e dei pagamenti del riscatto sia stata ancora più pronunciata. Le richieste e i pagamenti mediani dei riscatti hanno subito un netto calo, in quanto nel 2025 sono scesi rispettivamente a 126.000 $ e 200.000 $, rispetto ai 2 milioni di $ del 2024. Queste statistiche confermano ulteriormente la tendenza più generale degli autori degli attacchi a ricalibrare le aspettative, favorendo somme più accessibili per le organizzazioni di tutte le dimensioni.

Grafico 7: Pagamenti del riscatto nelle grandi imprese | Distribuzione suddivisa in fasce

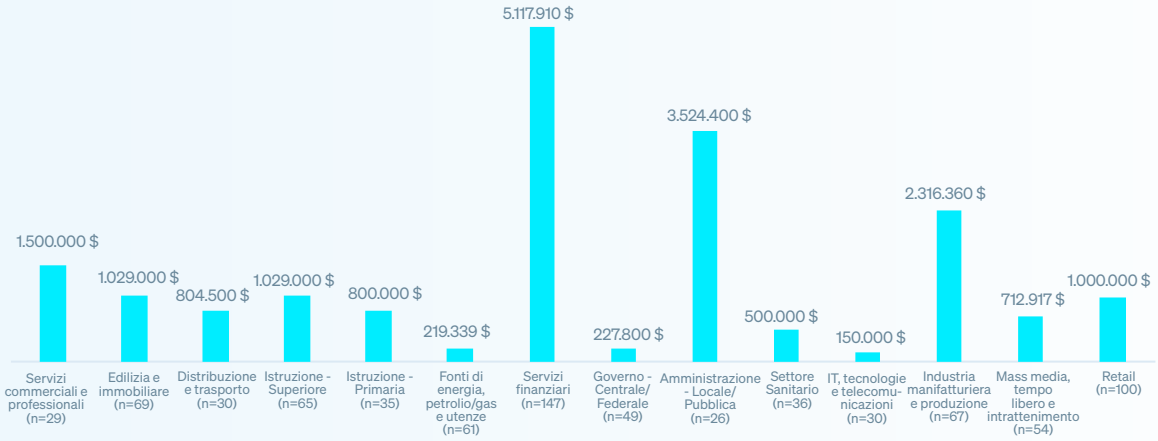


A quanto ammonta la somma di riscatto pagata ai cybercriminali? n=414 (2025), 470 (2024)

Pagamento del riscatto, in base al settore

I pagamenti del riscatto variano notevolmente in base al settore; a pagare la cifra media (mediana) più elevata sono le grandi imprese che operano nell'ambito dei servizi finanziari, con 5,1 milioni di $. Questo potrebbe essere dovuto agli elevati rischi operativi e alla bassa tolleranza alle interruzioni dei servizi di questo settore, che inducono i cybercriminali a considerare richieste più elevate.

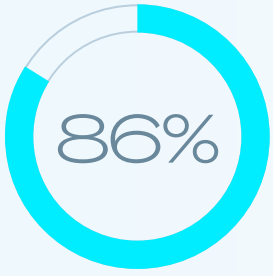
Grafico 8: Pagamento del riscatto, in base al settore



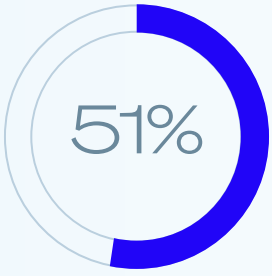
A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base di partecipanti indicata nel grafico. Nota: laddove il campione di riferimento sia inferiore a 30, i risultati sono da considerarsi puramente indicativi.

Confronto tra pagamenti effettivi e richieste di riscatto iniziali nelle grandi imprese

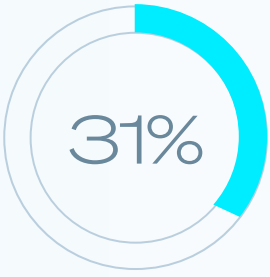
414 delle grandi imprese che hanno pagato il riscatto hanno condiviso sia informazioni relative alla richiesta iniziale dei cybercriminali, che dati sulla somma effettiva pagata. I risultati rivelano che queste vittime hanno pagato in media l'86% della somma richiesta originariamente per il riscatto: un calo incoraggiante rispetto al 95% registrato nel 2024. Complessivamente, nel 51% dei casi hanno pagato meno della somma richiesta, nel 18% hanno pagato di più e in quasi un terzo (31%) degli incidenti si sono attenute alla richiesta iniziale.



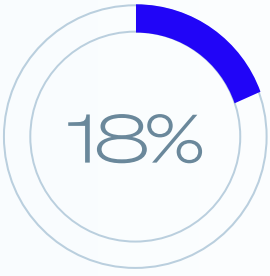
della somma di riscatto richiesta **è stata pagata**, in media



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

I motivi per cui nella maggior parte degli attacchi alle grandi imprese si registra una differenza tra la somma di riscatto pagata e quella richiesta inizialmente

Il sondaggio ha anche analizzato i motivi per cui alcune organizzazioni di grandi dimensioni 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.

72 imprese che **hanno pagato più** della richiesta iniziale hanno rivelato che:

- 61% degli intervistati: i cybercriminali erano convinti che potevamo permetterci di pagare di più.
- 49% degli intervistati: i cybercriminali hanno capito che eravamo un bersaglio di alto valore.
- 42% degli intervistati: i nostri backup non hanno funzionato o presentavano difetti.
- 39% degli intervistati: i cybercriminali si sono infastiditi e hanno aumentato il riscatto.
- 31% degli intervistati: non abbiamo pagato abbastanza rapidamente, quindi la somma è salita.

Tipicamente, le grandi imprese 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.

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

- 49% degli intervistati: abbiamo negoziato una cifra più bassa con i cybercriminali.
- 46% degli intervistati: abbiamo pagato il riscatto velocemente, così abbiamo usufruito di uno sconto.
- 45% degli intervistati: i cybercriminali hanno diminuito la richiesta per convincerci a pagare.
- 43% 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).
- 38% 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 nelle grandi imprese

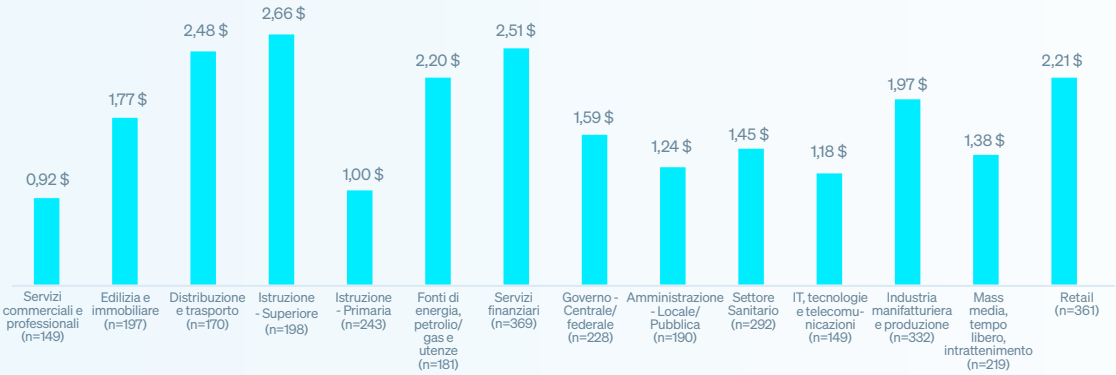
Il costo medio di recovery da un attacco ransomware per le imprese di grandi dimensioni (escludendo eventuali pagamenti del riscatto) ha toccato la cifra più bassa in tre anni, scendendo del 41% negli ultimi 12 mesi, con 1,84 milioni di $, in calo rispetto ai 3,12 milioni di $ del 2024. Si tratta inoltre di 330.000 $ in meno rispetto ai 2,17 milioni di $ registrati nel 2023.

2023	2024	2025
2,17 Mio di $	3,12 Mio di $	1,84 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=1.733 (2025), 1.409 (2024), 1.045 (2023)

Osservando la ripartizione in base al settore, i costi necessari per riprendere le normali attività operative variano in maniera notevole. Le grandi imprese che operano nell'**istruzione primaria** hanno segnalato il più alto costo medio di riparazione dei danni degli incidenti, con 2,66 milioni di $. All'altro estremo, le aziende di grandi dimensioni che si occupano di **servizi commerciali e professionali** hanno registrato il minore costo medio, con 0,92 milioni di $. Con molta probabilità, questa disparità riflette in parte il diverso grado di ricostruzione dell'infrastruttura IT necessario per riprendere le normali attività operative in seguito a un attacco, in quanto solitamente nell'istruzione vengono utilizzate soluzioni meno recenti rispetto a quelle implementate dai fornitori di servizi nel settore privato.

Grafico 9: Costi di recovery dai danni del ransomware, con risultati suddivisi in base al settore (in milioni di USD)

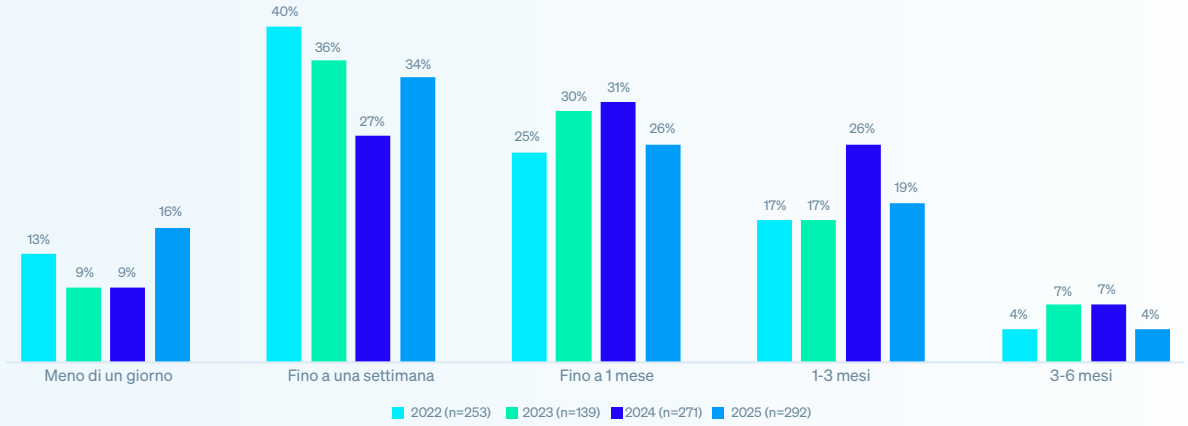


Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.),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

Tempi di recovery nelle grandi imprese

Dai dati emerge che nel 2025 le grandi imprese sono riuscite a riprendere più rapidamente le normali attività operative in seguito a un attacco ransomware. Il recovery ha richiesto meno di una settimana nella metà dei casi, in aumento rispetto al 36% registrato nel 2024. Allo stesso tempo, la percentuale di intervistati in grado di riprendere le normali attività è diminuita, passando dal 26% del 2024 al 19%. Complessivamente, nel 95% dei casi le grandi imprese che hanno subito un attacco sono tornate alla normalità operativa entro tre mesi, il che evidenzia una maggiore resilienza e capacità di recupero in questo settore.

Grafico 10: Tempi necessari per tornare alla normalità operativa in seguito a un attacco ransomware nelle grandi imprese, 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.

Le conseguenze a livello umano del ransomware

Il sondaggio mostra 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 che lavorano in grandi imprese sostengono che il proprio team ne ha risentito in qualche misura.

Grafico 13: Le conseguenze della crittografia 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=848.

Raccomandazioni

Sebbene negli ultimi 12 mesi le grandi imprese abbiano riscontrato diversi cambiamenti nelle proprie esperienze con questa minaccia, il ransomware continua a rappresentare un serio pericolo. Con cybercriminali che continuano a 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 altri rischi. Sfrutta 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, chiedi un supporto ad 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 scoprire come Sophos può aiutarti a ottimizzare le tue difese anti-ransomware, 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 sue 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.

2025-12-08 WP (MP)

SOPHOS