REPORT

La vera storia del ransomware 2026

La prospettiva di 2.158 IT e Cybersecurity Manager situati in 17 paesi

SOPHOS

Introduzione

Il panorama dei ransomware si sta evolvendo rapidamente sulla scia dell'avvento dell'IA. I vantaggi sono evidenti per le organizzazioni che investono in modo continuativo nelle difese di cybersecurity, ma gli attacchi ransomware continuano comunque a costare milioni di dollari alle aziende.

Questa è la settima edizione del report annuale Sophos "La vera storia del ransomware", che offre nuove informazioni sugli attacchi ransomware dell'anno precedente. I risultati sono suddivisi in sezioni, che trattano i seguenti argomenti:

- Metodi di attacco e di difesa
- Crittografia e recupero dei dati
- Richieste e pagamenti del riscatto
- Impatto sulle aziende e sugli esseri umani

I dati raccontano una storia fatta di costi elevati, ma anche di reali progressi:

- I costi di riparazione dei danni di un attacco ransomware sono elevati, con una spesa tipica che si aggira ormai sugli 1,7 milioni di $.
- Oltre la metà degli attacchi ransomware (56%) è ancora in grado di crittografare i dati, con un tasso in aumento rispetto al 2025.
- Tuttavia, le richieste e i pagamenti del riscatto sono in calo; inoltre, le organizzazioni stanno migliorando nella gestione della negoziazione. Negli ultimi due anni, le richieste di riscatto mediane sono diminuite del 65% e i pagamenti sono scesi del 62%.
- Dopo tre anni al primo posto, le vulnerabilità soggette a exploit non sono più la causa principale degli attacchi ransomware (18%): i vettori di attacco più comuni sono ora gli attacchi basati su e-mail (phishing 24% o e-mail malevole 26%).

2.158

Numero di IT e Security Manager situati in 17 paesi le cui organizzazioni sono state colpite dal ransomware nell'ultimo anno, che hanno partecipato a un sondaggio globale vendor-agnostic su cui si basa la ricerca di quest'anno.

Informazioni sul sondaggio

Questo report si basa sui risultati di un sondaggio indipendente e vendor-agnostic commissionato da Sophos. Il sondaggio ha posto domande sulle esperienze delle organizzazioni in merito agli attacchi ransomware e alle intrusioni basate sull'identità, monitorando anno su anno i tassi di pagamento del riscatto, i costi di riparazione dei danni, i tempi di recupero dopo un attacco e molte altre metriche. Le risposte sono state raccolte tra gennaio a marzo 2026 e si basano sulle esperienze maturate dai partecipanti nei 12 mesi precedenti.

I partecipanti sono situati in 17 paesi, provengono da un'ampia varietà di settori pubblici e privati, e includono un campionamento a curva gaussiana di aziende con un numero di dipendenti compreso tra 100 e 5.000, mantenutosi proporzionalmente coerente nei sette anni di storia del sondaggio. Tutti i dati finanziari sono espressi in dollari U.S.A.

I risultati più importanti, in sintesi

- **La compromissione dell'identità è il principale meccanismo di distribuzione dei ransomware.**
  - E-mail malevole (26%) e phishing (24%) sono diventate le principali cause originarie degli attacchi ransomware.
  - Le vulnerabilità soggette a exploit, (la causa primaria negli ultimi tre anni), sono diminuite di 14 punti percentuali nell'ultimo anno, attestandosi al 18%.
  - Due terzi delle vittime di ransomware (67%) hanno confermato che l'incidente subito è stato anche il loro attacco basato sull'identità più significativo.
- **Le lacune in materia di protezione, sicurezza e risorse espongono le organizzazioni agli attacchi**
  - Le lacune di sicurezza (note o sconosciute) sono state la causa operativa primaria più citata per il secondo anno consecutivo (62%), seguite dalla mancanza di personale o competenze (58%) e dalla scarsa qualità o assenza di protezione (57%).
- **L'implementazione della sola autenticazione multifattoriale (MFA) non è sufficiente a fermare il ransomware**
  - La MFA è stata implementata, in qualche misura, nel 97% dei casi in cui le credenziali compromesse rappresentavano la causa originaria degli attacchi ransomware.
- **In oltre la metà degli incidenti, le organizzazioni non riescono a rilevare e bloccare gli attacchi ransomware in tempo**
  - Più della metà degli attacchi ransomware (56%) è riuscita a crittografare i dati, e nel 16% dei casi i dati sono stati sia crittografati che esfiltrati.
- **Quando i dati vengono crittografati, gli autori degli attacchi hanno circa il 50% di probabilità di ricevere il pagamento di un riscatto**
  - Il 48% delle organizzazioni i cui dati sono stati crittografati ha pagato il riscatto
  - La media su quattro anni registra ora un tasso di pagamento del riscatto del 50% a seguito della crittografia non autorizzata.
- **Le richieste di riscatto sono in calo, ma gli autori degli attacchi chiedono cifre più alte quando ottengono l'accesso a un sistema privilegiato: un problema difficile da risolvere per i team di difesa**
  - La richiesta di riscatto mediana è scesa a 698.000 $, confermando una tendenza pluriennale al ribasso, rispetto alla cifra mediana di 1,3 milioni di $ registrata nel report del 2025 e ai 2 milioni di $ del report del 2024.
  - Il 59% delle richieste di riscatto derivanti da attacchi che hanno avuto inizio per via di una vulnerabilità del firewall soggetta a exploit ammonta a 1 milione di $ o più, rispetto al 48% di tutte le richieste.
- **I pagamenti del riscatto sono in calo, e le vittime spesso riescono a negoziare un importo inferiore a quello richiesto inizialmente**
  - Il pagamento del riscatto mediano è ora di 769.000 $, un calo considerevole rispetto alla cifra di 1 milione di $ riportata lo scorso anno.
  - Poco meno della metà (48%) dei pagamenti è stata pari o superiore a 1 milione di $, in calo rispetto al 52% dell'anno precedente.
  - Quasi la metà (51%) delle organizzazioni che hanno pagato un riscatto ha versato una somma inferiore a quella richiesta, un dato che si avvicina a quello del report del 2025 (53%) e che supera del 7% quello del report del 2024 (44%).
- **Il costo necessario per rimediare ai danni di un attacco ransomware è aumentato**
  - Il costo medio necessario per rimediare ai danni di un attacco ransomware (escludendo l'eventuale riscatto pagato) è ora di 1.700.200 $, con un aumento dell'11% rispetto alla media di 1.525.716 $ del report del 2025.
- **La crittografia non autorizzata dei dati ha quasi sempre ripercussioni per i membri del team IT/di cybersecurity.**
  - Il 99% delle vittime del ransomware i cui dati sono stati crittografati ha affermato che l'attacco ha avuto ripercussioni sul proprio team IT/di cybersecurity.
  - L'impatto più comune è la maggiore ansia o stress per paura di attacchi futuri (41%), seguito dalle maggiori pressioni dal Senior Management (40%).
  - L'unico impatto a essere aumentato rispetto all'anno precedente è stata la maggiore stima da parte del Senior Management (36%, rispetto al 31% del report del 2025).

Metodi di attacco e di difesa

Cause all'origine degli attacchi

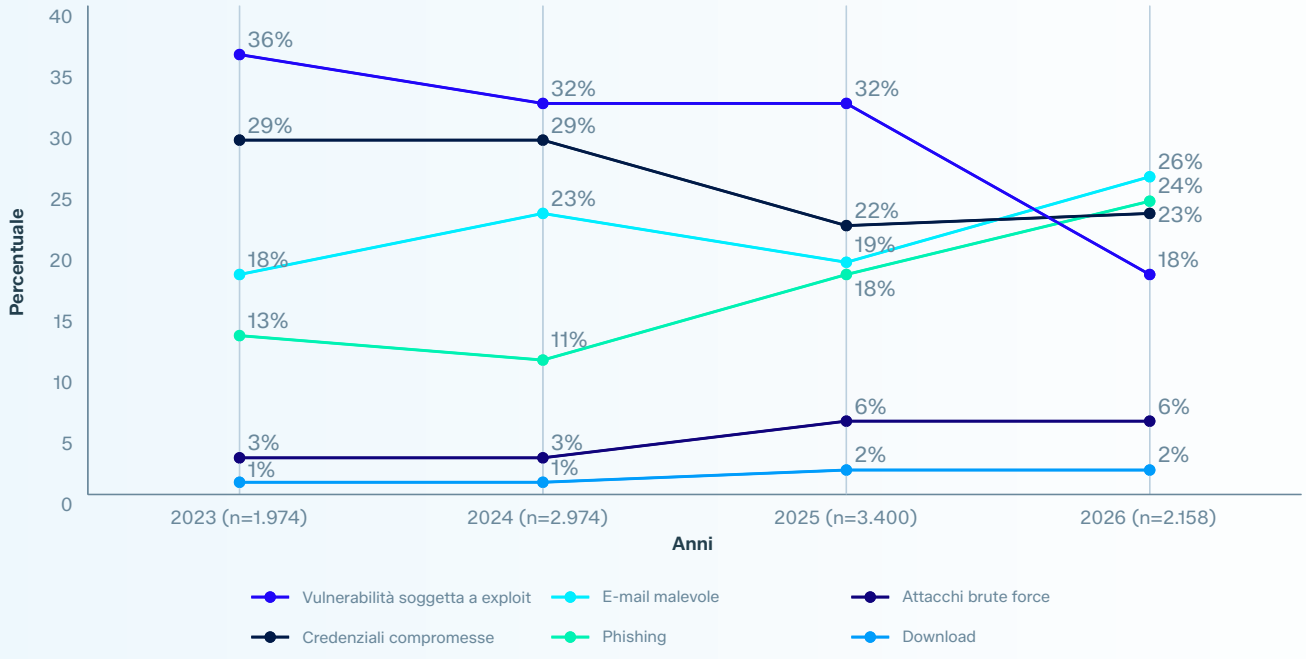
Le principali cause tecniche all'origine degli attacchi ransomware sono cambiate nel report di quest'anno. Le e-mail malevole (26%) e il phishing (24%) sono state le due principali cause originarie degli attacchi ransomware, rappresentando la metà di tutti gli incidenti. Ciò costituisce un cambiamento significativo rispetto agli anni precedenti, quando le vulnerabilità soggette a exploit dominavano costantemente le classifiche.

Le segnalazioni di vulnerabilità soggette a exploit sono diminuite dal 32% nel report del 2025 al 18% nel report del 2026. Tuttavia, data la velocità e la portata delle capacità di individuazione delle vulnerabilità dell'IA di frontiera, nel corso del prossimo anno le organizzazioni dovrebbero mantenere alta la guardia sulla possibilità di un aumento degli attacchi ransomware la cui causa originaria è una vulnerabilità soggetta a exploit.

Le credenziali compromesse sono rimaste la terza causa originaria più comune, al 23%, in linea con gli anni precedenti.

Il 79% degli attacchi ha avuto inizio con un approccio basato sull'identità, volto a ottenere credenziali per scopi illeciti o a sfruttare credenziali già acquisite. Ciò evidenzia perché la sicurezza dell'identità sia un tassello cruciale nel contesto di un profilo di sicurezza olistico.

Causa tecnica all'origine degli attacchi ransomware (2023-2026)



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

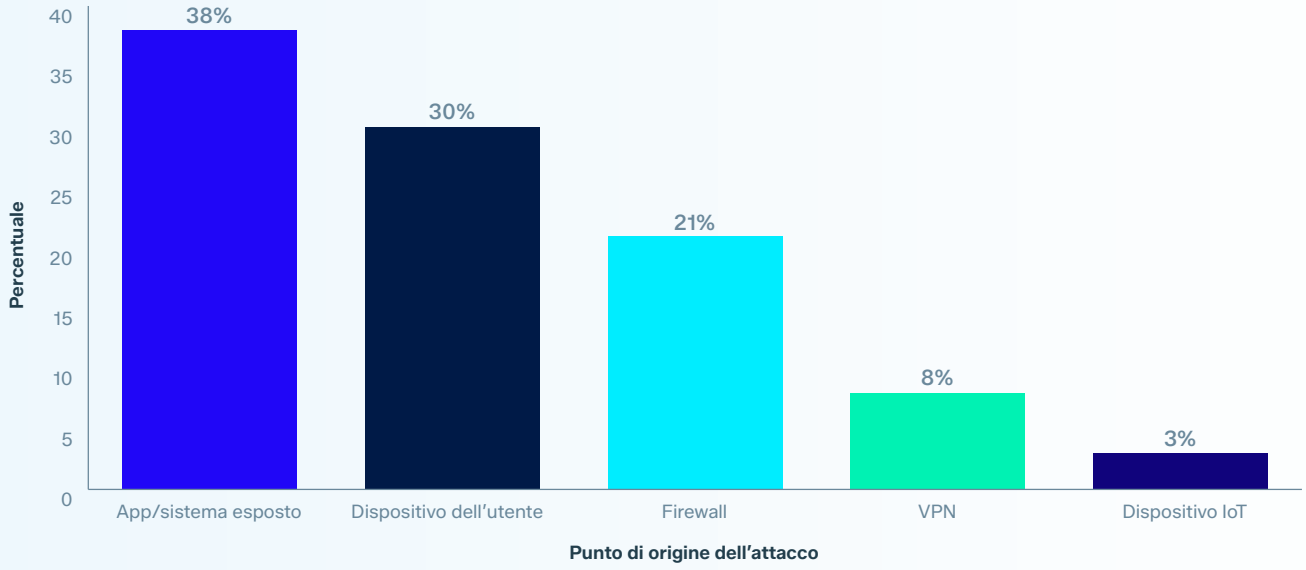
NUOVA RICERCA

Dove iniziano gli attacchi

Quest'anno, per la prima volta, riveliamo il punto esatto in cui si è verificata la causa originaria all'interno dell'ambiente dell'organizzazione. Comprendere le origini degli attacchi è fondamentale per orientare le strategie di riduzione del rischio. Negli incidenti ransomware causati da una vulnerabilità soggetta a exploit, credenziali compromesse o un attacco brute force, **le applicazioni e sistemi esposti sono stati il punto di ingresso dell'attacco più comune in assoluto (38%)**, seguiti dai dispositivi degli utenti (30%) e dai firewall (21%).

La rilevanza delle applicazioni esposte si allinea con il contesto più ampio del passaggio ad ambienti cloud e SaaS, dove i sistemi connessi a Internet rappresentano una superficie di attacco estesa e in continua espansione.

Punto di origine degli attacchi ransomware



Hai indicato che la causa originaria era una vulnerabilità soggetta a exploit, credenziali compromesse o un attacco brute force: in quale punto del tuo ambiente aziendale si è verificata? n=1.022

Analizzando più a fondo i dati, emerge quanto sia diffuso l'uso di credenziali compromesse in app e sistemi esposti, firewall, VPN e dispositivi IoT.

Le più comuni cause primarie per ciascun punto di origine

Causa originaria	In un'applicazione o sistema esposto	Nel nostro firewall	Nella nostra VPN	In un dispositivo IoT
Credenziali compromesse	59%	41%	44%	48%
Una vulnerabilità soggetta a exploit	31%	33%	41%	36%
Attacchi brute force	10%	26%	15%	16%

Hai indicato che la causa originaria era una vulnerabilità soggetta a exploit, credenziali compromesse o un attacco brute force: in quale punto del tuo ambiente aziendale si è verificata? Selezione di risposte. n=711

Gli attacchi basati su credenziali compromesse sono risultati particolarmente frequenti nelle applicazioni e nei sistemi esposti (59%), evidenziando l'importanza di proteggere le risorse accessibili dall'esterno e i controlli sulla gestione delle identità.

Ricalibrando la base di confronto sui medesimi dati, sono emersi i bersagli più colpiti dalle credenziali compromesse e dagli attacchi brute force.

Dove iniziano gli attacchi ransomware

Punto di origine dell'attacco	% Totale	% Credenziali compromesse	% Attacco brute force
In un'applicazione o sistema esposto	38%	46%	30%
Nel dispositivo di un utente (con o senza connessione alla rete, ad es. laptop, desktop)	30%	27%	13%
Nel nostro firewall	21%	18%	44%
Nella nostra VPN	8%	7%	9%
In un dispositivo IoT	3%	3%	4%

Hai indicato che la causa originaria erano credenziali compromesse o un attacco brute force: in quale punto del tuo ambiente aziendale si è verificata? Selezione di risposte. n=628

Tipologie di attacco diverse hanno preso di mira punti di origine differenti.

- Gli attacchi basati su credenziali compromesse si sono concentrati su applicazioni e sistemi esposti (46%), seguiti dai dispositivi degli utenti.
- Gli attacchi brute force hanno colpito principalmente i firewall (44%), evidenziando l'importanza delle policy di limitazione della velocità e di blocco degli account nei dispositivi posizionati sul perimetro di rete.

NUOVA RICERCA

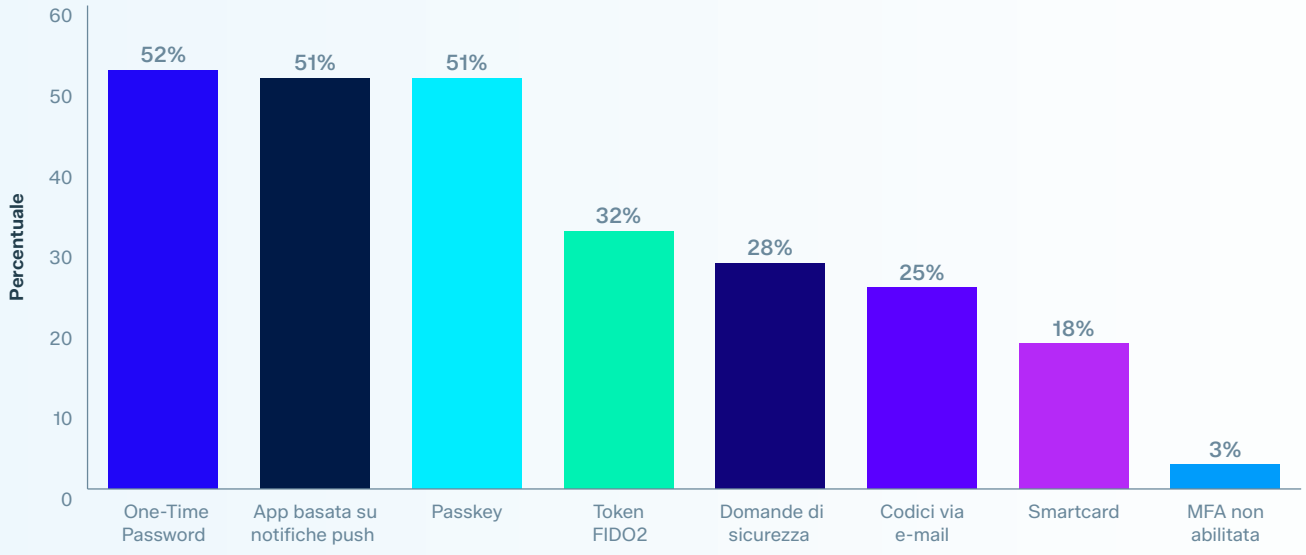
Il ruolo dell'autenticazione multifattoriale (MFA)

Quest'anno il report offre nuovi approfondimenti sul ruolo dell'autenticazione multifattoriale (MFA) negli attacchi ransomware.

Tra le organizzazioni in cui le credenziali compromesse sono state la causa principale dell'attacco ransomware, **il 97% aveva l'autenticazione multifattoriale abilitata in qualche misura al momento dell'incidente**. Le One-Time Password (52%), le applicazioni basate su notifiche push (51%) e le passkey (51%) sono stati i metodi più diffusi, con gli intervistati che hanno indicato di usare, in media, 2,5 metodi MFA.

L'elevata percentuale di vittime di ransomware che avevano implementato la MFA al momento dell'attacco indica che questa potrebbe non essere stata applicata integralmente su tutti i sistemi pertinenti, creando lacune che gli aggressori hanno potuto sfruttare. Ciò suggerisce inoltre che, sebbene la MFA rimanga un elemento essenziale delle strategie di cyber difesa efficaci, da sola non è sufficiente a prevenire gli attacchi basati sulle credenziali, poiché le tecniche di elusione continuano a evolversi.

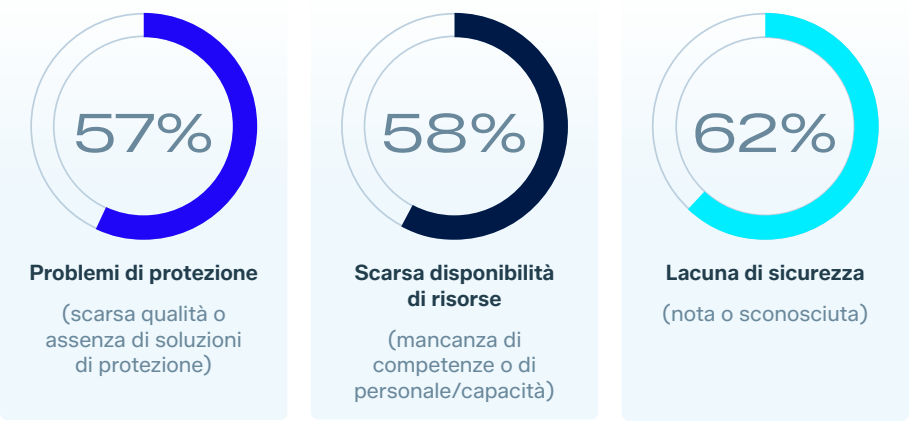
Metodi MFA abilitati al momento dell'attacco



Quale tipo di autenticazione multifattoriale era attiva al momento dell'attacco, se presente? Base: l'attacco si è verificato a causa di credenziali compromesse. n=503

Cosa ha reso vulnerabili le organizzazioni

Per il secondo anno consecutivo, non è emerso un singolo fattore organizzativo dominante che abbia esposto le organizzazioni agli attacchi; gli intervistati hanno segnalato un'ampia gamma di sfide, dalla scarsa qualità o assenza di protezione alla mancanza di personale/competenze, fino alle lacune nei sistemi di sicurezza.



Le lacune di sicurezza sono state la categoria più citata tra le cause operative primarie per il secondo anno consecutivo, con il 62%, seguite dalla mancanza di personale o competenze (58%) e dalla scarsa qualità o assenza di protezione (57%).

Un dato incoraggiante è che tutti i fattori individuali (tranne uno) hanno mostrato un calo anno su anno; **l'errore umano (35%) è stato l'unico fattore operativo in aumento negli ultimi 12 mesi**.

Come nel 2025, le vittime del ransomware hanno riportato molteplici sfide organizzative, con **una media di 2,5 fattori citati**, in calo rispetto ai 2,7 registrati precedentemente.

35%

L'errore umano: l'unica costante. L'unica causa operativa all'origine degli attacchi che non è diminuita rispetto al report del 2025.

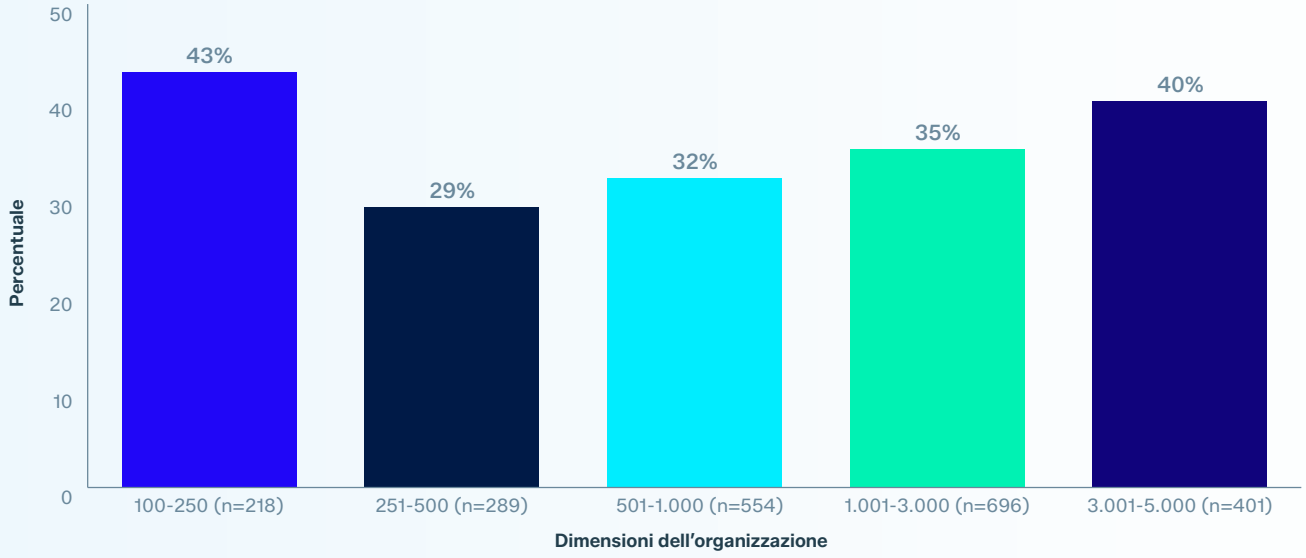
Le 7 principali cause originarie operative degli attacchi ransomware

Classifica	2025	%	Classifica	2026	%
1	Mancanza di competenze	40,2%	1	Mancanza di protezione	36,4%
2	Lacuna di sicurezza sconosciuta	40,1%	2	Lacuna di sicurezza sconosciuta	36,3%
3	Mancanza di personale/capacità	39,4%	3	Lacuna di sicurezza nota	36,0%
4	Mancanza di protezione	39,0%	4	Mancanza di personale/capacità	35,3%
5	Lacuna di sicurezza nota	38,2%	5	Errore umano	35,3%
6	Protezione di scarsa qualità	37,1%	6	Mancanza di competenze	35,1%
7	Errore umano	34,2%	7	Protezione di scarsa qualità	32,6%

Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=3.400 (2025), n=2.158 (2026)

Come prevedibile, la mancanza di personale/capacità è stata citata frequentemente dalle organizzazioni di piccole dimensioni, con un organico compreso tra 100 e 250 dipendenti. Tuttavia, quattro imprese su 10 con un numero di dipendenti pari a 3.001-5.000 segnalano problemi di capacità con una frequenza inferiore di appena il 3% rispetto alle organizzazioni con 100-250

La mancanza di personale/capacità ha contribuito a rendere le aziende vittime del ransomware



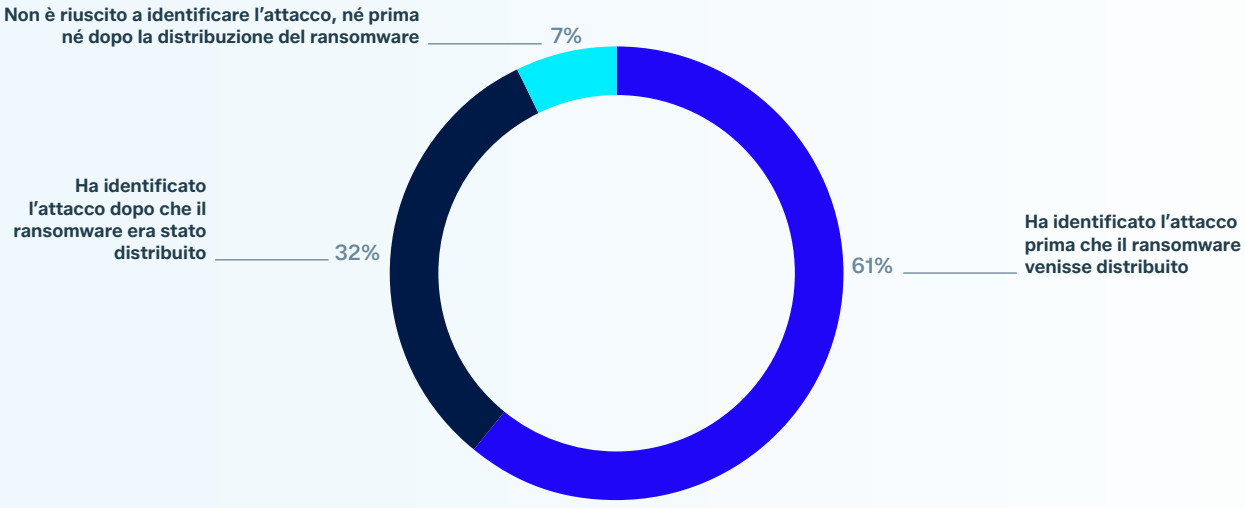
Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? Non avevamo un numero sufficiente di esperti di cybersecurity che monitoravano i nostri sistemi al momento dell'attacco. Base di partecipanti indicata nella tabella.

NUOVA RICERCA

Il ruolo dei firewall nelle difese antiransomware

Il 61% delle vittime ha riferito che il proprio firewall ha rilevato l'attacco ransomware prima della detonazione del payload, e il 32% ha affermato che il firewall lo ha identificato dopo che il ransomware era già stato distribuito. Solo il 7% ha indicato che il proprio firewall non ha rilevato affatto l'attacco.

Quale ruolo ha svolto il tuo firewall nell'identificazione dell'attacco?



Quale ruolo ha svolto il tuo firewall nell'identificazione dell'attacco? n=2.158

Il 7% delle vittime il cui firewall non ha rilevato l'attacco ha subito le conseguenze peggiori in termini di crittografia non autorizzata, con il 71% dei dati crittografati, rispetto al 50% nei casi in cui il firewall ha rilevato l'attacco prima della distribuzione del ransomware. Il rilevamento avvenuto dopo la distribuzione del ransomware, solitamente un'identificazione a posteriori dei segnali successivamente associati all'attacco ransomware, è risultato correlato a un tasso crittografia del 65%.

I risultati dimostrano chiaramente che i firewall svolgono un ruolo chiave nel rilevamento degli attacchi ransomware, poiché i dati di telemetria provenienti da questi dispositivi forniscono preziosi segnali precoci di attività cybercriminale. Se utilizzata in combinazione con approfondimenti provenienti dall'intero ambiente di sicurezza (ad esempio dalla protezione endpoint o dalle soluzioni di sicurezza e-mail tramite uno strumento XDR o un servizio MDR), la telemetria del firewall può aiutare i team di sicurezza a intercettare e bloccare gli attacchi ransomware prima che i dati vengano crittografati.

Impatto dell'identificazione degli attacchi assistita dal firewall sul tasso di crittografia non autorizzata

	Ha identificato l'attacco prima che il ransomware venisse distribuito	Ha identificato l'attacco dopo che il ransomware era stato distribuito	Non è riuscito a identificare l'attacco, né prima né dopo la distribuzione del ransomware
I cybercriminali sono riusciti a crittografare i dati	50%	65%	71%
I criminali informatici non sono riusciti a crittografare i dati	50%	35%	29%

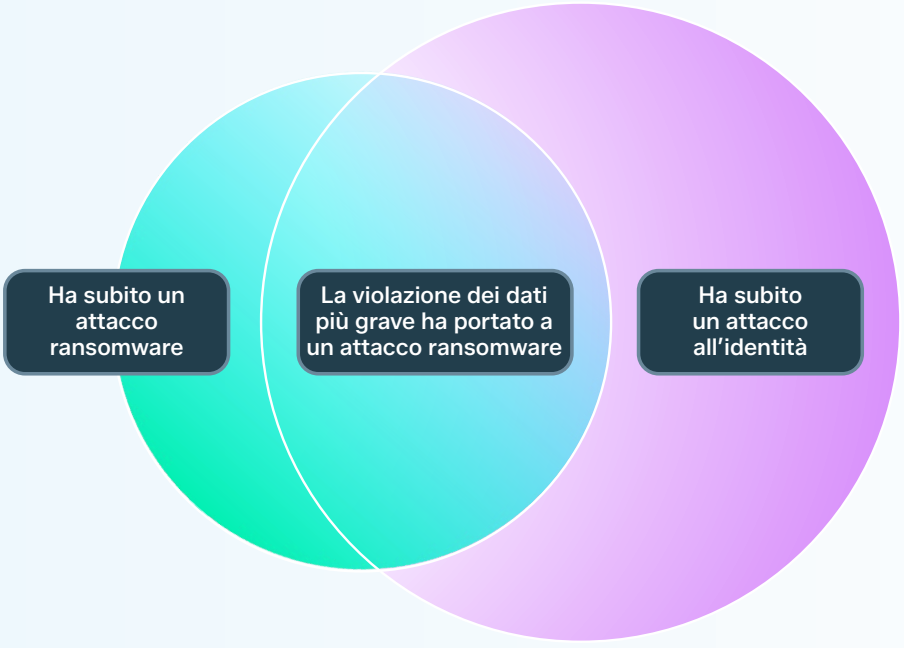
Quale ruolo ha svolto il tuo firewall nell'identificazione dell'attacco? Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? n=2.158

I firewall occupano una posizione fortemente privilegiata nell'infrastruttura aziendale; di conseguenza, la loro compromissione espone l'azienda a impatti decisamente più significativi rispetto ad altri ambiti dell'ambiente IT. Se gli autori degli attacchi riescono a sfruttare una vulnerabilità del firewall, spesso ottengono un accesso esteso all'intera azienda. La differenza nelle richieste di riscatto per questi scenari ne è la riprova: **le richieste di riscatto di 1 milione di $ o più, derivanti da attacchi che hanno avuto inizio per via di una vulnerabilità del firewall soggetta a exploit sono pari al 59%**, rispetto al 48% di tutti gli attacchi.

NUOVA RICERCA

Il legame tra identità e ransomware

Uno dei risultati più sorprendenti della ricerca di quest'anno è la conferma del legame diretto tra attacchi all'identità e ransomware. Delle organizzazioni colpite dal ransomware nel l'anno scorso, due terzi (67%) 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, questo risultato dimostra che la compromissione dell'identità è un meccanismo dominante di diffusione del ransomware.



Suddivisione dei dati: 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? 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?

Crittografia e recupero dei dati

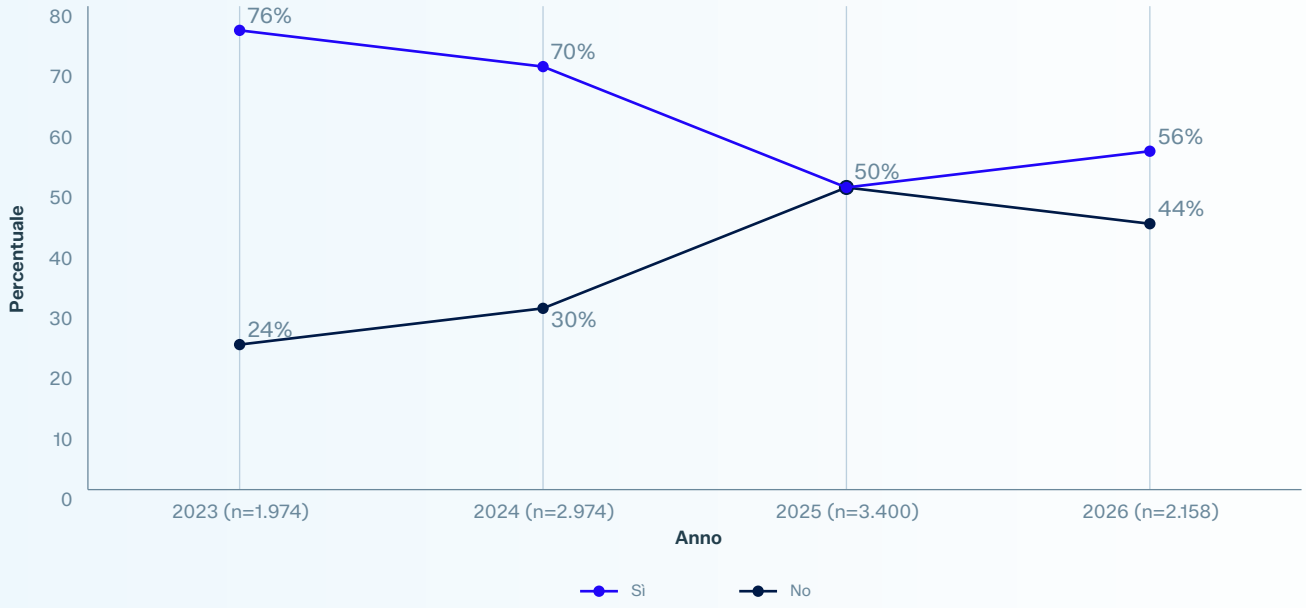
Tasso di crittografia dei dati

Oltre la metà (56%) degli attacchi ransomware è riuscita a crittografare i dati. Questa percentuale include il 40% dei casi in cui i dati sono stati solo crittografati e il 16% dei casi in cui i dati sono stati sia crittografati che esfiltrati. Il 41% degli attacchi è stato bloccato prima della crittografia, mentre il 2% ha coinvolto attacchi di tipo estorsivo senza crittografia.

+6%

Aumento del tasso di crittografia del ransomware rispetto al report dell'anno scorso.

Sono stati crittografati dati durante l'attacco? (Sintesi: Sì/No)

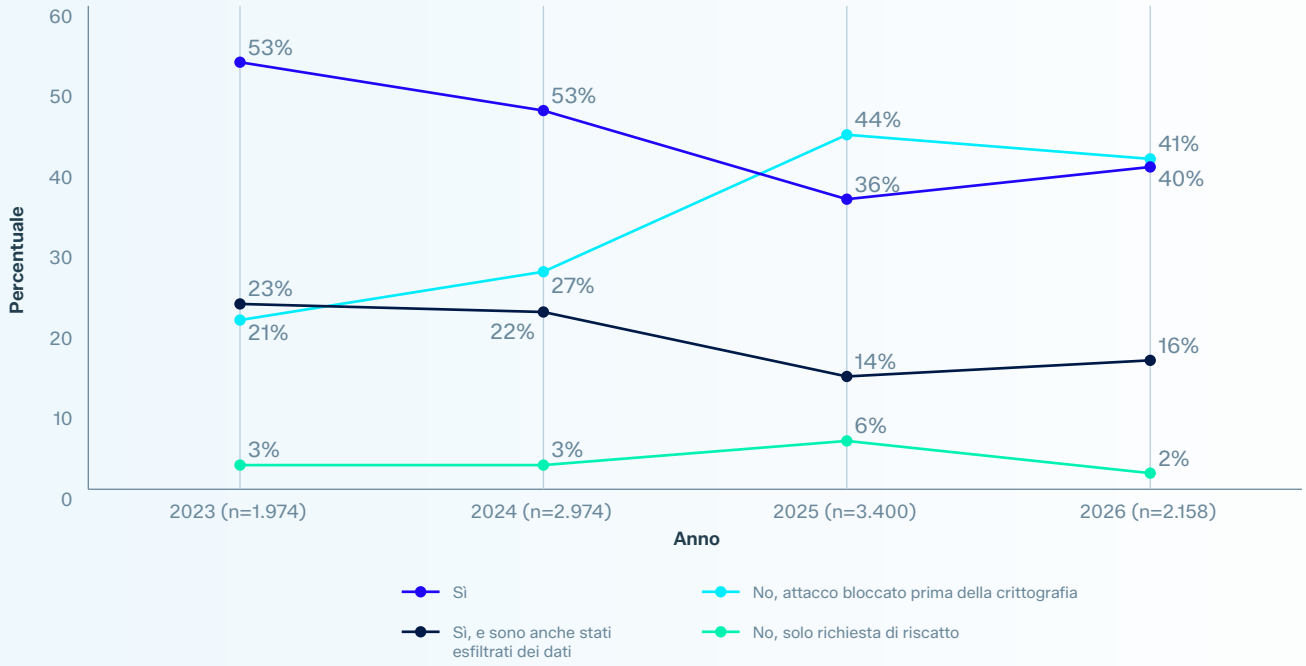


Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Risposte in sintesi: Sì/No. Base di partecipanti indicata nel grafico.

Sebbene il tasso crittografia rimanga ben al di sotto del picco del 76% registrato nel report del 2023, ha mostrato un lieve aumento rispetto al minimo del 50% del report del 2025. Questa inversione di tendenza merita attenzione: dopo due anni di declino nel successo della crittografia, sembra che gli autori degli attacchi stiano recuperando terreno.

Il 16% degli attacchi che includono sia la crittografia non autorizzata che il furto di dati è un dato particolarmente preoccupante, poiché questi attacchi a doppio impatto offrono ai cybercriminali più punti di leva per l'estorsione.

Sono stati crittografati dati durante l'attacco?

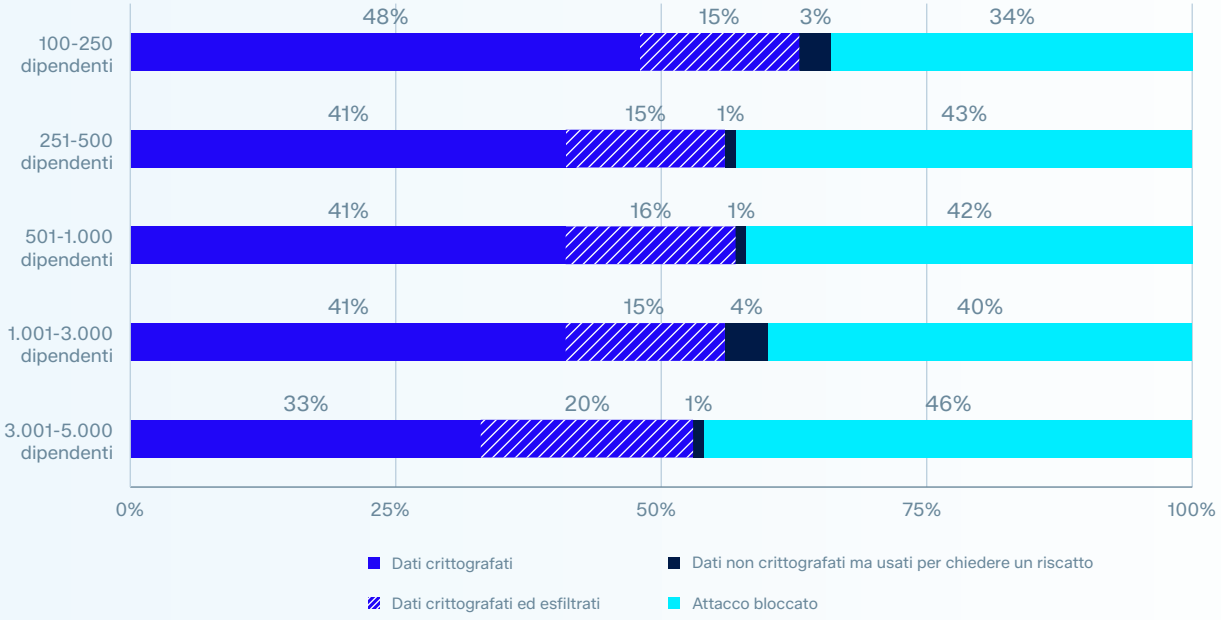


Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? (Elenco completo delle opzioni di risposta)
Base: organizzazioni colpite da ransomware. Base di partecipanti indicata nella tabella.

I risultati della crittografia variavano in base alle dimensioni dell'organizzazione: quelle **più grandi tra quelle interpellate (3.001-5.000 dipendenti) hanno registrato la maggiore probabilità di bloccare gli attacchi prima della crittografia o dell'estorsione (46%),** rispetto ad appena il 34% per le aziende più piccole (100-250 dipendenti).

Tuttavia, quando gli attacchi riuscivano a crittografare i dati nelle organizzazioni più grandi, le vittime avevano maggiori probabilità di subire anche il furto di dati, con un tasso di "dati crittografati ed esfiltrati" che raggiungeva il 20% per la fascia di aziende di dimensioni più grandi, rispetto al 15% per la maggior parte delle altre. L'esfiltrazione dei dati, unita all'utilizzo di ransomware, offre agli autori degli attacchi una seconda opportunità per monetizzare l'attacco.

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=2.158

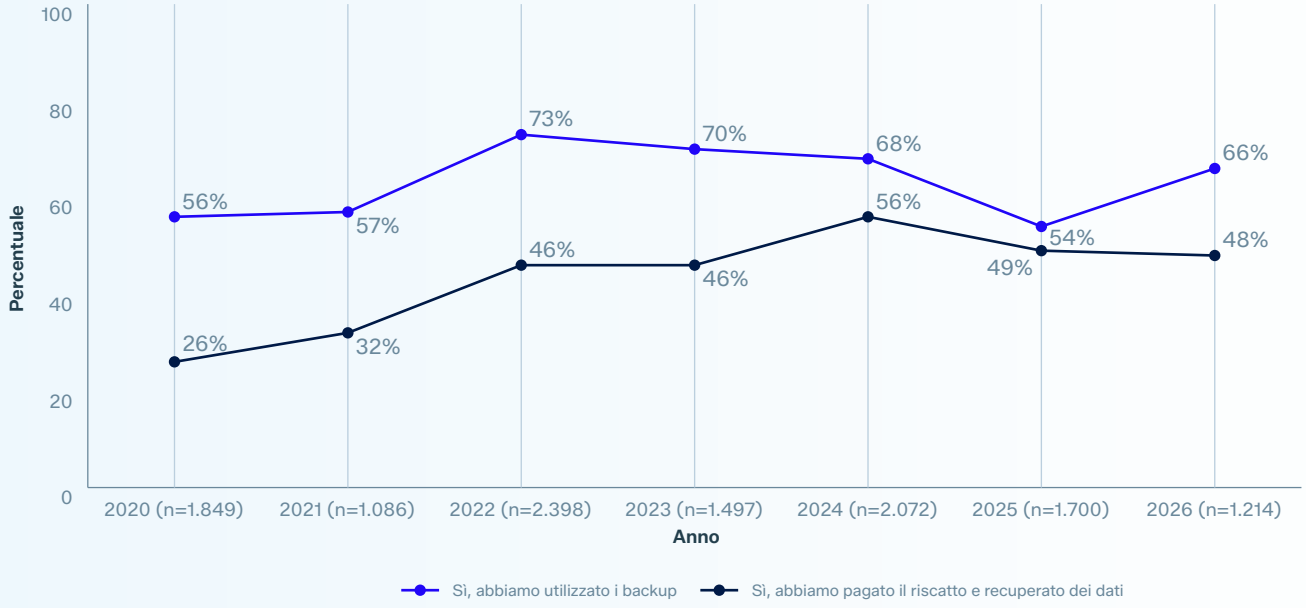
Come le organizzazioni hanno recuperato i dati crittografati

Il ripristino basato sui backup è balzato al 66% degli attacchi in cui i dati sono stati crittografati, in aumento rispetto al 54% registrato nel report del 2025.. Questa netta ripresa suggerisce che le organizzazioni hanno rinnovato i loro investimenti nelle infrastrutture di backup, dopo un calo di utilizzo nel 2025, e che stanno aumentando la propria resilienza contro le richieste di riscatto.

+12%

Aumento dell'utilizzo dei backup per recuperare i dati crittografati dal ransomware dal 2025 al 2026.

In che modo la tua organizzazione ha recuperato i dati dopo gli attacchi ransomware?



In che modo la tua organizzazione ha recuperato i dati? Base: organizzazioni che avevano subito la crittografia non autorizzata dei dati. Base di partecipanti indicata nella tabella. Erano consentite risposte multiple, pertanto la somma delle percentuali potrebbe superare il 100%.

La percentuale di organizzazioni che hanno pagato il riscatto per recuperare i dati è scesa al 48%, il tasso più basso degli ultimi 3 anni. Solo il 2% delle organizzazioni ha riferito di non aver recuperato alcun dato, il che indica che, quando i dati vengono crittografati, il recupero tramite un mezzo disponibile è pressoché universale.

Richieste e pagamenti del riscatto

698.000 $

Richiesta di riscatto mediana nell'ultimo anno.

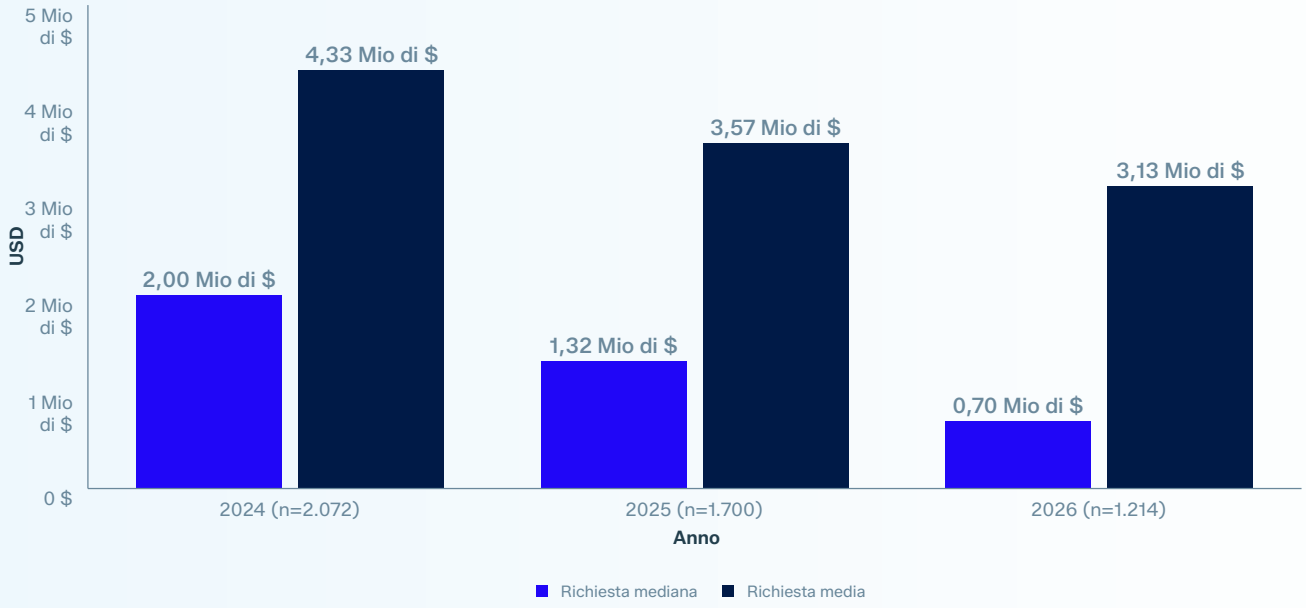
Richieste di riscatto

Nel report di quest'anno, la richiesta di riscatto mediana è scesa a 698.000 $, proseguendo una tendenza al ribasso pluriennale. Ciò rappresenta un calo del 65% negli ultimi due anni. Anche la richiesta media di riscatto è diminuita in questo periodo, attestandosi a 3.126.372 $, con una riduzione del 28% rispetto al report del 2024.

Il crescente divario tra le richieste medie e mediane segnala una distribuzione fortemente asimmetrica: un piccolo numero di richieste molto elevate gonfia la media, mentre l'organizzazione tipica si trova ad affrontare una richiesta di poco inferiore a 700.000 $.

Nota: i valori anomali dei riscatti pari o superiori a 40 milioni di $ sono stati rimossi da questi dati.

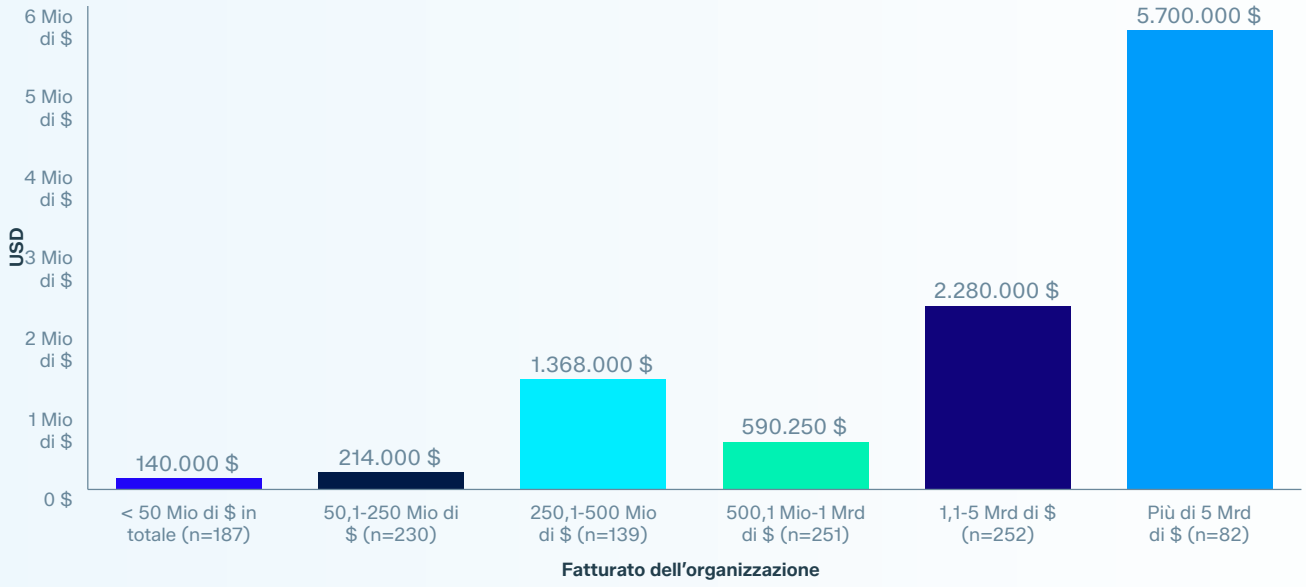
Richieste di riscatto medie e mediane



A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? Base: organizzazioni che avevano subito la crittografia non autorizzata dei dati. Base di partecipanti indicata nella tabella. Sono escluse le richieste con valori anomali, pari o superiori a 40 milioni di $.

Le richieste di riscatto aumentano vertiginosamente in proporzione al fatturato dell'organizzazione. Le organizzazioni con un fatturato inferiore a 50 milioni di $ hanno dovuto affrontare richieste di pagamento mediane di circa 140.000 $, mentre quelle con un fatturato superiore a 5 miliardi di $ si sono trovate di fronte a richieste di pagamento mediane di 5,7 milioni di $. Questo modello suggerisce fortemente che gli autori degli attacchi conducano attività di ricognizione per calibrare le richieste in base alla presunta capacità di pagamento della vittima.

Richiesta di riscatto mediana



A quanto ammonta la somma di riscatto? Base: organizzazioni che avevano subito la crittografia non autorizzata dei dati. Base di partecipanti indicata nella tabella. Sono escluse le richieste con valori anomali, pari o superiori a 40 milioni di $.

Pagamento del riscatto

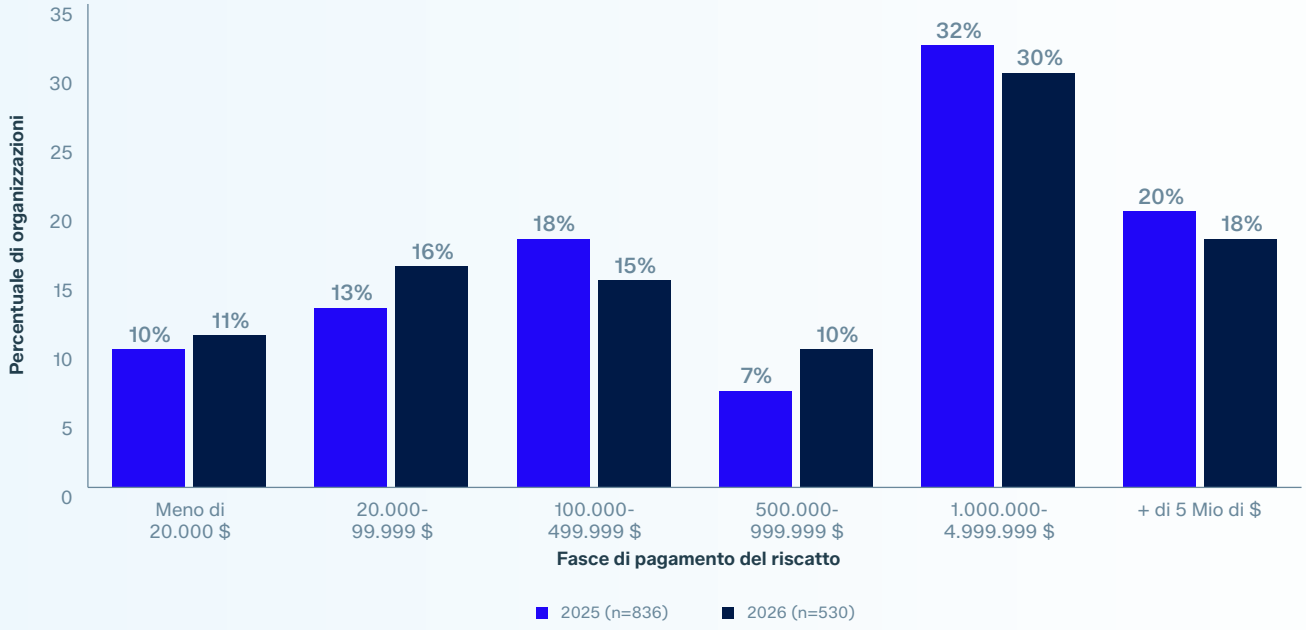
530 organizzazioni che hanno pagato il riscatto ne hanno comunicato l'importo, rivelando che il pagamento del riscatto mediano è ora pari a 769.000 $, un calo notevole rispetto al dato di 1 milione di $ riportato lo scorso anno. Poco meno della metà (48%) dei pagamenti è stata pari o superiore a 1 milione di $, in calo rispetto al 52% dell'anno precedente.

Analizzando l'intera distribuzione dei pagamenti, emerge un chiaro spostamento verso la fascia media. Le due fasce più elevate (1-5 Mio di $ e + di 5 Mio di $) hanno entrambe registrato un calo rispetto al report dell'anno scorso, mentre le fasce 20.000-99.999 $ e 500.000-999.999 $ sono entrambe aumentate, suggerendo che autori degli attacchi e vittime stanno trovando sempre più spesso un punto di incontro nella fascia di pagamento medio-bassa.

769.000 $

Pagamento del riscatto mediano nell'ultimo anno.

Fasce di pagamento del riscatto

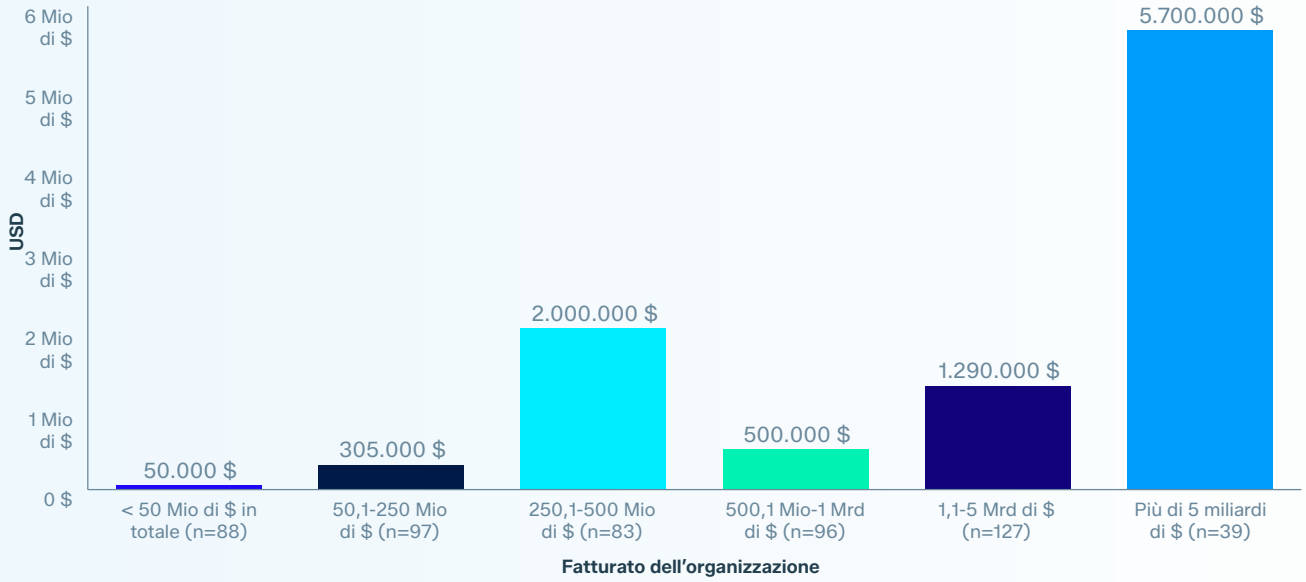


A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base di partecipanti indicata nella tabella.

Suddividendo i pagamenti del riscatto in base al fatturato dell'organizzazione, emerge un picco nella fascia 250,1-500 Mio di $, con le vittime che hanno versato un importo mediano di 2 milioni di $. Si tratta di una cifra superiore a quella di qualsiasi altro segmento, ad eccezione di quello più grande (fatturato annuo superiore a 5 miliardi di $), e quattro volte superiore a quella delle organizzazioni con un fatturato di 500,1 Mio-1 Mrd di $.

I dati relativi alle richieste di riscatto mostrano un picco simile nella fascia di fatturato 250,1-500 Mio di $, con richieste mediane di 1,37 milioni di $, rispetto ai 590.000 $ della fascia superiore; ciò suggerisce che questo segmento è particolarmente esposto agli impatti del ransomware.

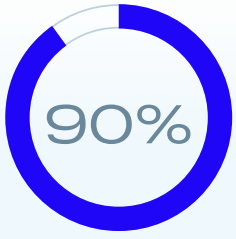
Pagamento del riscatto mediano



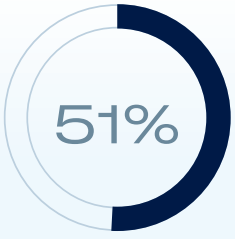
A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base: organizzazioni che hanno pagato il riscatto. Base di partecipanti indicata nella tabella.

Pagamenti effettivi vs richieste iniziali

507 organizzazioni hanno condiviso sia la richiesta di riscatto che il pagamento effettuato, rivelando l'efficacia delle trattative condotte dalle aziende con gli autori degli attacchi. **Il pagamento mediano è stato pari al 90% della richiesta (media: 85%)**, con poco più della metà (51%) che ha pagato meno della richiesta iniziale, il 30% che ha pagato la richiesta effettiva e il 18% che ha pagato di più. Queste statistiche sono molto vicine a quelle dell'anno scorso, il che dimostra che il rapporto tra richieste e pagamenti effettivi si è mantenuto relativamente stabile.

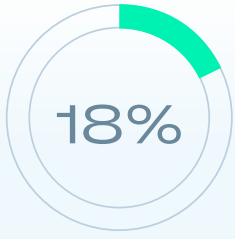


La percentuale **mediana** del riscatto pagato



Pagamenti **inferiori** alla richiesta di riscatto iniziale

Pagamenti **pari** alla richiesta di riscatto iniziale



Pagamenti **superiori** alla richiesta di riscatto iniziale

A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base: organizzazioni che hanno condiviso sia la richiesta di riscatto che il pagamento. n=507

Come già accennato, le richieste di riscatto mediane tendono ad aumentare quando l'organizzazione presa di mira ha un fatturato più elevato, ma le diverse fasce di fatturato presentano livelli di successo diversi nel negoziare al ribasso i pagamenti finali.

Le organizzazioni di medie dimensioni (con un fatturato compreso tra 50 e 250 milioni di $) sono quelle che ottengono i risultati peggiori nel ridurre i pagamenti del riscatto, con il 25% che paga più di quanto richiesto inizialmente. Le imprese più grandi (con un fatturato superiore a 5 miliardi di $) sono le più efficaci nel negoziare riscatti più bassi: solo l'11% paga più della richiesta iniziale e il 57% paga meno, la percentuale più alta tra tutti i gruppi analizzati.

Le organizzazioni con un fatturato più elevato (oltre 500 milioni di $) hanno avuto un maggior successo nel pagare un riscatto inferiore a quello richiesto; questo indica che, quando i riscatti sono più alti, i cybercriminali si dimostrano più disposti a concedere sconti per somme complessive maggiori. Anche le organizzazioni con un fatturato inferiore a 50 milioni di $ hanno ottenuto un modesto successo nella riduzione dei pagamenti del riscatto.

Percentuale di riscatto pagata (mediana), in base al fatturato dell'organizzazione

Fatturato	Percentuale del riscatto pagato (mediana)
< 50 Mio di $	95%
50,1-250 milioni di $	100%
250,1-500 milioni di $	100%
500.1 milioni-1 miliardo di $	83%
1,1-5 miliardi di $	83%
5 miliardi di $ o più	83%

A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? A quanto ammonta la somma di riscatto pagata ai cybercriminali?
Base: organizzazioni che hanno condiviso sia la richiesta di riscatto che il pagamento. n=507

Pagamenti del riscatto in base al settore

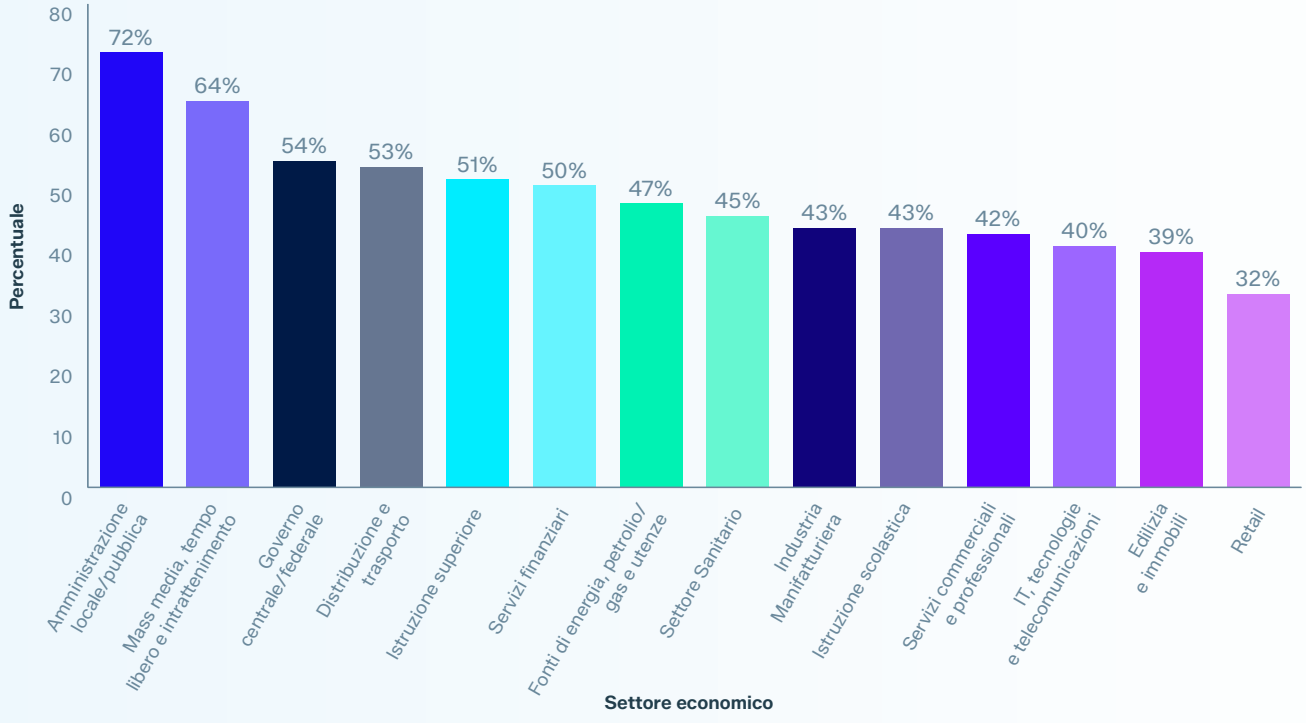
La propensione a pagare il riscatto varia a seconda del settore. **Amministrazione locale/pubblica (72%) e Mass media, tempo libero e intrattenimento (64%) sono stati i settori più propensi a pagare il riscatto**, riportando un tasso più che doppio rispetto al Retail (32%).

Le organizzazioni che operano nell'ambito della pubblica amministrazione e dei media si trovano spesso a dover affrontare forti pressioni per ripristinare rapidamente servizi rivolti ai cittadini o critici in termini di tempo, mentre le organizzazioni del retail potrebbero essere più propense ad attendere per "superare la tempesta".

Retail

È stato il settore con la minore percentuale di pagamenti agli autori degli attacchi ransomware (32%).

Percentuale di organizzazioni che hanno pagato il riscatto, in base al settore



In che modo la tua organizzazione ha recuperato i dati? Abbiamo pagato il riscatto. Base: organizzazioni che avevano subito la crittografia non autorizzata dei dati. n=1.214

Impatto sulle aziende e sugli esseri umani

Costi di riparazione dei danni del ransomware

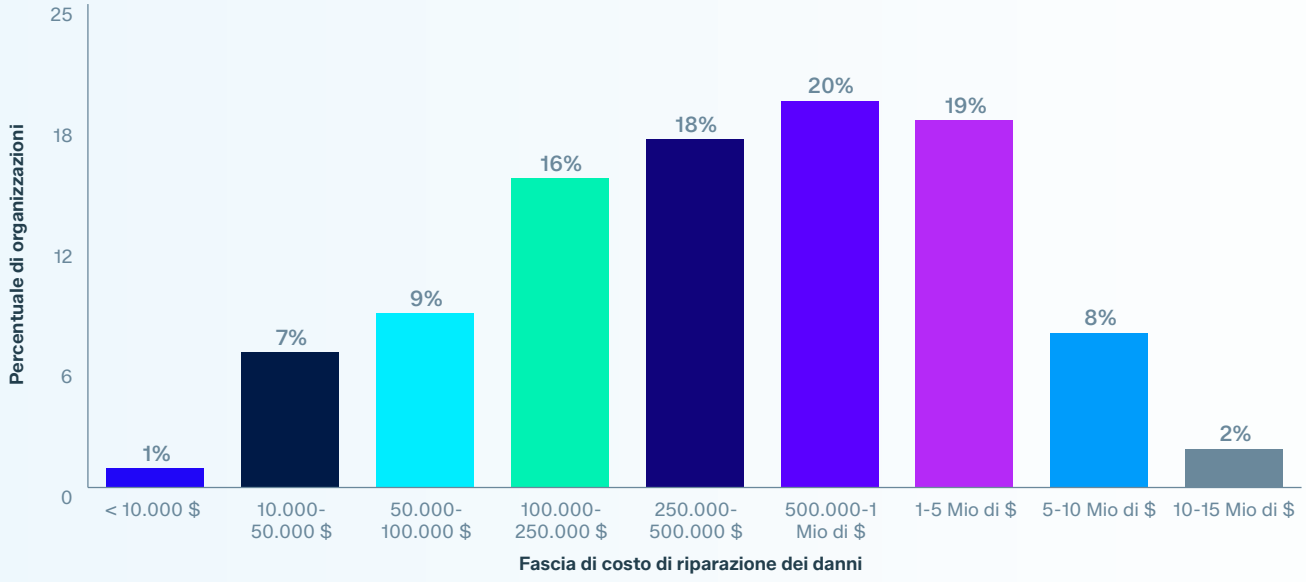
Nell'ultimo anno, il costo medio necessario per rimediare ai danni di un attacco ransomware, escluso un eventuale riscatto pagato, è stato pari a 1.700.200 $. Si tratta di un aumento dell'11% rispetto alla media di 1.525.716 $ osservata nel report del 2025, ma rimane inferiore del 38% al picco di 2.730.684 $ registrato nel report del 2024. Il costo mediano si attesta a 375.000 $, e resta invariato rispetto al report dello scorso anno.

2024	2025	2026
2,73 milioni di $	1,53 milioni di $	1,70 milioni 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=2.158 (2026), n=3.400 (2025), 2.974 (2024)

I costi di riparazione dei danni variano notevolmente: il 20% delle organizzazioni ha sostenuto spese comprese tra 500.000 e 1 milione di $, mentre il 19% ha speso tra 1 e 5 milioni di $.

I costi di riparazione dei danni degli attacchi ransomware



Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave? n=2.158

Tempi necessari per riprendere le normali attività

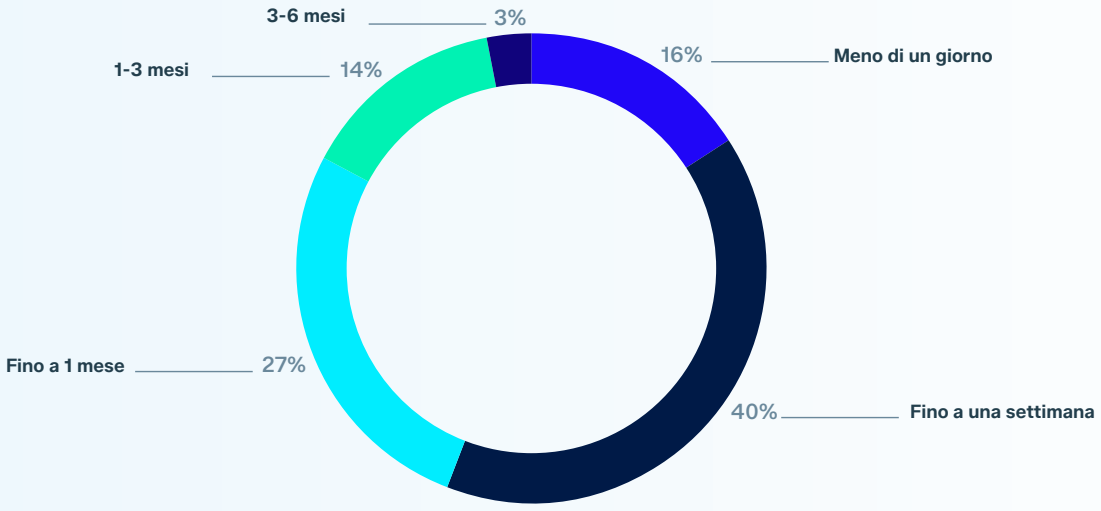
Oltre la metà delle organizzazioni (55%) ha ripreso le normali attività entro una settimana dall'attacco ransomware (il 16% in meno di un giorno) e l'83% entro un mese. Solo il 3% ha impiegato più di tre mesi.

Il tasso di ripresa delle normali attività entro una settimana, pari al 55%, è aumentato del 3% rispetto all'anno precedente. Il numero medio di settimane necessarie per riprendere le normali attività è rimasto fermo a tre (report del 2026 e del 2025), in calo rispetto alle cinque settimane emerse dal report del 2024.

55%

Percentuale di organizzazioni che ha ripreso le normali attività entro una settimana dall'attacco ransomware.

Quanto tempo è stato necessario per riprendere le normali attività operative



Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware? n=2.158

L'impatto umano del ransomware

Praticamente tutte le organizzazioni che hanno subito la crittografia non autorizzata dei dati (99%) hanno riportato ripercussioni durature sui propri team IT e di cybersecurity. Gli impatti più citati sono stati la maggiore ansia o stress per paura di attacchi futuri (41%) e le maggiori pressioni dal Senior Management (40%). Per oltre una vittima su cinque (21%), il team di leadership è stato sostituito come conseguenza diretta dell'attacco.

L'unico impatto ad aumentare su base annua è stata la maggiore stima da parte del Senior Management., che è salita dal 31% al 36%. Tutte le altre ripercussioni misurate sono diminuite, compresi i cambiamenti di priorità dei team (in calo di sette punti), gli aumenti costanti del carico di lavoro (in calo di sette punti) e le modifiche della struttura dei team (in calo di cinque punti).

21%

Percentuale di team di leadership di IT/ cybersecurity che sono stati sostituiti a causa dell'attacco ransomware.

Gli effetti del ransomware sui team IT/di cybersecurity

Ripercussioni	2026	Variazione dal 2025
Maggiore ansia o stress per paura di attacchi futuri	41%	-
Maggiori pressioni dal Senior Management	40%	-
Maggiore stima da parte del Senior Management	36%	↑ 5 punti percentuali
Cambiamenti della struttura del team/organizzativa	32%	↓ 5 punti percentuali
Cambiamenti di priorità/focalizzazione del team	32%	↓ 6 punti percentuali
Sensi di colpa dovuti al fatto che l'attacco non è stato fermato	31%	↓ 3 punti percentuali
Aumento costante del carico di lavoro	31%	↓ 7 punti percentuali
Assenze del personale dovute a problemi di stress/salute mentale	29%	↓ 2 punti percentuali
Cambio di leadership nel team	21%	↓ 4 punti percentuali

Quali ripercussioni ha avuto l'attacco ransomware sui membri del tuo team IT/di cybersecurity? Base: organizzazioni che avevano subito la crittografia non autorizzata dei dati. n=1.214 (2026), n=1.700 (2025)

L'aumento della stima da parte del Senior Management potrebbe di per sé rappresentare un fattore determinante per le tendenze operative positive osservate in altri punti di questo report, poiché una maggiore attenzione da parte della leadership può tradursi in una migliore assegnazione delle risorse e in un maggiore supporto organizzativo per i programmi di cybersecurity.

Raccomandazioni

Rafforzare la sicurezza dell'identità come difesa contro i ransomware. Due terzi delle vittime del ransomware hanno confermato che l'incidente è coinciso con il loro attacco all'identità più significativo, sottolineando lo stretto legame tra compromissione dell'identità e ransomware. Le organizzazioni devono dare priorità all'Identity Threat Detection and Response (ITDR), imporre l'autenticazione multifattoriale a tutti i punti di accesso ed eseguire regolarmente audit delle credenziali delle identità sia umane che non umane. Come dimostrano i risultati del sondaggio (il 97% delle organizzazioni aveva attivato la MFA in qualche misura al momento dell'attacco), la MFA da sola non è sufficiente a fermare gli attacchi e deve essere abilitata in modo completo ed esaustivo.

Rafforzare la protezione degli endpoint per i modelli di IA di frontiera. L'IA di frontiera sta accelerando l'individuazione e lo sfruttamento delle vulnerabilità. Avere difese potenti per gli endpoint, che siano in grado di bloccare automaticamente gli attacchi basati sugli exploit, è essenziale.

Avvalersi del supporto di uno specialista o di MDR. La mancanza di capacità, competenze ed esperienza è un problema ricorrente sia per le PMI che per le grandi imprese. Dover affrontare minacce potenziate dall'IA accentuerà ancora di più queste criticità, poiché i professionisti della sicurezza cercheranno di tenere il passo con una tecnologia IA in rapida evoluzione. A meno che tu non sia in grado di formare internamente un team dedicato alle Security Operations, valuta la possibilità di collaborare con uno specialista esterno per coprire i punti scoperti, rivolgendoti direttamente a un fornitore di servizi MDR che sia operativo 24/7, oppure a un provider di servizi gestiti. I vendor in grado di risolvere un maggior numero di incidenti end-to-end con l'IA e l'automazione rappresenteranno anche un moltiplicatore di forze che potrà contribuire a colmare le lacune in termini di competenze e capacità.

Dare priorità alla sicurezza delle e-mail. Poiché in questo report phishing ed e-mail malevole rappresentano ormai la metà di tutte le cause originarie dei ransomware, le organizzazioni devono implementare filtri e-mail avanzati, applicare protocolli DMARC/DKIM/SPF e investire in corsi di formazione periodici di consapevolezza sul phishing. Il passaggio ad attacchi basati sulle e-mail dimostra che la sola applicazione delle patch per le vulnerabilità tecniche non è sufficiente.

Investire nell'infrastruttura di backup e ripristino. Le organizzazioni che hanno mantenuto sistemi di backup solidi hanno recuperato i dati crittografati a tassi quasi record nell'ultimo anno. I backup devono essere testati regolarmente, conservati off-line o in formati immutabili e integrati in un piano di incident response documentato, che possa essere eseguito anche sotto pressione.

Mantenere programmi di gestione dell'esposizione. Il calo di 14 punti percentuali delle vulnerabilità soggette a exploit come causa originaria è incoraggiante, ma questi attacchi rimangono un vettore importante ed è probabile che aumentino man mano che i modelli di IA di frontiera individuano più rapidamente nuove vulnerabilità. Le organizzazioni devono mantenere ritmi di applicazione delle patch serrati e concentrarsi su misure di mitigazione quali l'implementazione di segmentazione, Zero Trust Network Access e MFA/autenticazione continua.

Ridurre l'esposizione tramite il firewall e sfruttare la telemetria del firewall per rilevare tempestivamente gli attacchi. Assicurati che il tuo firewall riceva aggiornamenti rapidi (idealmente automatizzati) e riduci al minimo i servizi esposti a Internet, come gli accessi amministrativi e i portali utente. Collega i firewall a soluzioni XDR e MDR per abilitare la telemetria dei firewall e rilevare così gli attacchi ransomware prima che i payload vengano distribuiti.

Supportare i team di cybersecurity nelle fasi successive all'incidente. Considerando che il 99% dei team colpiti dichiarano di aver subito ripercussioni, il costo umano del ransomware è pressoché universale. Le organizzazioni devono definire chiari protocolli di supporto post-incidente e garantire che la crescente stima da parte del Senior Management si traduca in investimenti continui nelle persone, e non solo nelle tecnologie.

Conclusione

Il report "La vera storia del ransomware 2026" rivela un panorama delle minacce in fase di transizione.

Ci sono segnali concreti di progresso: le richieste e i pagamenti del riscatto sono in calo, il recupero dei dati basato sui backup ha raggiunto livelli quasi record e le organizzazioni sono sempre più efficaci nel negoziare gli esiti quando pagano il riscatto. La drastica diminuzione degli attacchi basati sulle vulnerabilità soggette a exploit suggerisce che l'individuazione guidata dall'IA e gli investimenti continui nella gestione delle patch stanno producendo i loro frutti.

Il segnale più incoraggiante emerso dalle statistiche potrebbe essere la maggiore stima da parte del Senior Management nei confronti dei team di cybersecurity. Quando la leadership presta attenzione, le risorse seguono. Le tendenze operative positive evidenziate in questo report, dal miglioramento dell'utilizzo dei sistemi di backup a risultati di negoziazione più favorevoli, potrebbero riflettere proprio questa dinamica.

Allo stesso tempo, le sfide che restano da affrontare sono significative. Oltre la metà degli attacchi ransomware riesce ancora a crittografare i dati, i costi di riparazione dei danni ammontano in media a 1,7 milioni di $ per incidente e l'impatto umano per i team di cybersecurity è pressoché universale.

Il fatto che due terzi delle vittime del ransomware abbiano ricondotto l'incidente a una compromissione dell'identità **sottolinea il ruolo critico che la protezione dell'identità svolge nella catena di difesa contro i ransomware**. Le organizzazioni che considerano l'identità come un livello di sicurezza fondamentale, anziché un elemento secondario, si trovano in una posizione migliore per prevenire gli attacchi fin dall'inizio.

Le organizzazioni devono anche prepararsi per **la sfida di cybersecurity cruciale del prossimo decennio: le minacce potenziate dall'IA**. I dati offrono già un'indicazione del perché: il 62% delle vittime ha indicato una lacuna di sicurezza, nota o sconosciuta, come uno dei fattori determinanti dell'attacco subito, mentre il 58% ha segnalato una mancanza di personale o competenze. Entrambe le lacune diventano più rilevanti man mano che l'IA accelera la velocità e la portata degli attacchi, con i cybercriminali che la utilizzano per individuare più rapidamente i punti deboli e orchestrare attacchi su molteplici punti di controllo alla velocità della macchina.

Il modello emerso dai risultati di quest'anno (dai migliori esiti ottenuti grazie al rilevamento tempestivo degli attacchi da parte dei firewall, all'aumento del recupero dei dati basato sui backup) punta in un'unica direzione: **quando le difese operano in sinergia anziché in modo isolato, i risultati migliorano**. Colmare il divario rispetto agli attacchi dell'era dell'IA dipenderà meno dall'aggiunta di ulteriori strumenti e più dalla capacità di connettere quelli già esistenti, affinché il contesto, il rilevamento e la risposta possano muoversi alla velocità richiesta dalle minacce attualmente in circolazione.

Le organizzazioni che avranno maggiori probabilità di resistere agli attacchi ransomware nei prossimi anni saranno quelle che manterranno alta l'attenzione del Senior Management su questo tema, adottando allo stesso tempo sistemi di difesa integrati e guidati dall'IA, e investendo non solo in tecnologie e processi, ma anche nelle persone che ogni giorno difendono i sistemi da queste minacce.

Metodologia

Questo sondaggio è stato condotto da Vanson Bourne per conto di Sophos nel primo trimestre del 2026. Sono stati intervistati 2.158 decision maker in ambito IT e Cybersecurity che lavorano in aziende colpite da ransomware nei 12 mesi precedenti, e che sono 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 saperne di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione, visita il nostro sito web.

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

2026-06-09 IT (DD)