REPORT

La fiducia nella cybersecurity nel 2026: la realtà di una sfida complessa

I risultati emersi da un sondaggio agnostico rispetto ai produttori, condotto tra 5.000 IT e Cybersecurity Manager

SOPHOS

Introduzione

Quando scelgono un produttore di soluzioni di cybersecurity, le organizzazioni gli affidano effettivamente la propria resilienza operativa critica, ovvero persone, dati e fatturato.

Eppure, nonostante questo rapporto di dipendenza, un nuovo studio di ricerca di Sophos rivela che la maggior parte delle aziende non ripone fiducia nei produttori selezionati per tutelare la propria sicurezza.

Per comprendere meglio il livello effettivo di fiducia nella sicurezza informatica, Sophos ha commissionato un sondaggio globale indipendente e agnostico rispetto ai produttori, condotto tra 5.000 decision maker in ambito informatico e di cybersecurity situati in 17 paesi. Il sondaggio, svolto dall'istituto di ricerca Vanson Bourne, offre un quadro realistico e statisticamente significativo di come si instaura e si perde la fiducia tra acquirenti e produttori nel settore della cybersecurity.

5.000

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

I principali dati emersi

La fiducia è scarsa: solo il 5% degli IT Manager afferma che sia loro stessi che l'azienda nutrono piena fiducia nei loro produttori di soluzioni di sicurezza informatica.

Le prove verificate sono un fattore fondamentale per instaurare un rapporto di fiducia: i team IT e i vertici aziendali concordano sul fatto che gli elementi verificabili che dimostrano maturità in materia di cybersecurity costituiscono il principale indicatore di affidabilità.

Valutare l'affidabilità dei produttori rimane una sfida: secondo il 79% delle organizzazioni è difficile valutare l'affidabilità dei nuovi fornitori di servizi di sicurezza informatica, mentre il 62% lo ritiene problematico anche per i produttori attuali. Gli intervistati hanno citato diversi fattori che hanno minato la loro fiducia nei produttori, primo fra tutti il fatto che le informazioni fornite dal produttore non fossero abbastanza oggettive o dettagliate.

Questa mancanza di fiducia implica delle conseguenze: il 51% degli intervistati afferma che la mancanza di fiducia genera il timore che l'organizzazione sia più propensa a subire un incidente informatico grave.

Spesso personale operativo e dirigenti si trovano in disaccordo: il 78% degli intervistati sostiene che il proprio team IT e la leadership aziendale/il consiglio di amministrazione hanno opinioni divergenti sull'affidabilità dei produttori di servizi di cybersecurity utilizzati dall'azienda. Quasi un terzo delle imprese che hanno partecipato al sondaggio commissionato da Sophos afferma che questa divergenza di opinioni si verifica "Spesso".

L'affidabilità è difficile da valutare

Solo il 5% degli IT Manager afferma che sia loro stessi che l'azienda nutrono piena fiducia nei loro produttori di soluzioni di sicurezza informatica.

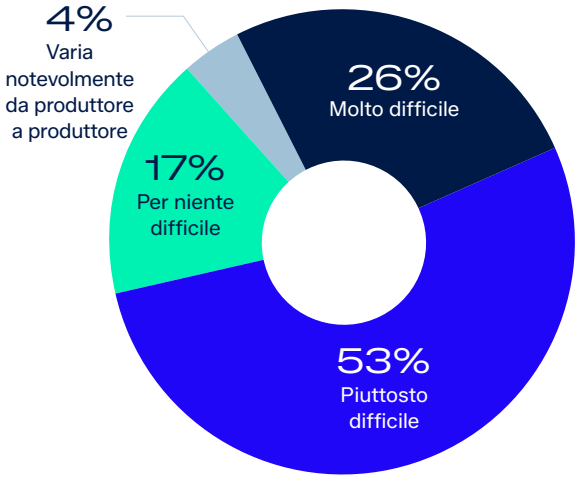
Quando ci si affida al proprio produttore di servizi di cybersecurity per garantire la sicurezza della rete e il corretto svolgimento delle attività operative, la fiducia è fondamentale. I fornitori di servizi di sicurezza informatica hanno il compito di difendere la tua azienda 24/7, anche di notte e nei fine settimana, nonché quando i membri del tuo team IT sono in ferie. Per i titolari di piccole imprese, che spesso non hanno neppure personale IT dedicato, i prodotti o servizi di cybersecurity dei loro fornitori possono agire come un vero e proprio dipendente.

Prima che le organizzazioni possano decidere di chi fidarsi, si trovano ad affrontare una sfida ancora più fondamentale: valutare prima di tutto l'affidabilità di un produttore.

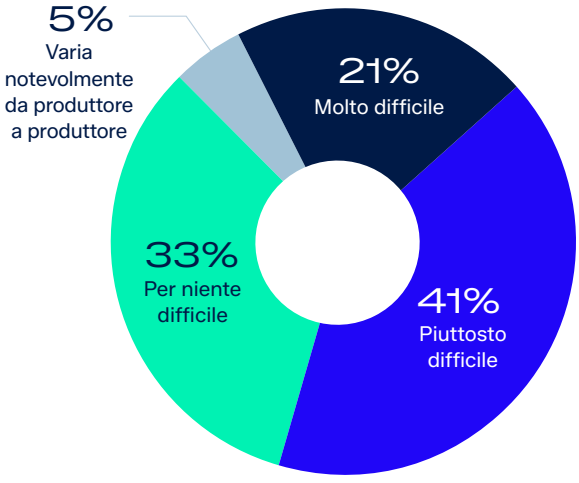
Secondo il sondaggio, il 79% degli intervistati sostiene che sia difficile valutare l'affidabilità di nuovi produttori o partner di cybersecurity, un dato che mette in luce una difficoltà diffusa nello svolgere attività come confrontare i prodotti, verificare le affermazioni e capire se un potenziale produttore sia realmente in grado di proteggere l'azienda. Inoltre, il 62% non è in grado di valutare correttamente l'affidabilità dei produttori con cui sta già collaborando: un segnale che la mancanza di fiducia non scompare una volta firmato il contratto (Figura 1).

79%

Percentuale di aziende intervistate che affermano che per loro è difficile valutare l'affidabilità di nuovi produttori o partner di cybersecurity



Valutare l'affidabilità di **nuovi** produttori e partner di cybersecurity



Valutare l'affidabilità di produttori e partner di cybersecurity **esistenti**

Figura 1: In generale, quanto è difficile (nel caso in cui lo sia) per la tua organizzazione valutare l'affidabilità dei produttori e dei partner di cybersecurity? n=5.000

Gli ostacoli nel processo di valutazione della fiducia

Gli intervistati hanno segnalato diversi ostacoli che impediscono di riporre facilmente fiducia in un fornitore, la maggior parte dei quali sono legati alla trasparenza. Per molte aziende non è facile interpretare le affermazioni dei produttori, valutare i dettagli tecnici o trovare le informazioni necessarie per prendere decisioni senza timore.

Quasi la metà (47%) ritiene che le informazioni fornite dai produttori non siano abbastanza oggettive o dettagliate, mentre il 45% pensa che tali informazioni siano difficili da interpretare o da comprendere. Un ulteriore 43% ammette di non possedere le competenze o le conoscenze necessarie per valutare correttamente i produttori, il 41% si trova ad affrontare informazioni contraddittorie, e il 38% fa fatica anche solo a reperire le informazioni di cui ha bisogno (Figura 2).

Figura 2: Perché per la tua organizzazione è difficile valutare l'affidabilità dei produttori di soluzioni di cybersecurity? n=4.483

La principale differenza tra piccole imprese (con meno di 250 dipendenti) e grandi aziende (con oltre 1.000 dipendenti) è il fatto che le PMI tendono maggiormente a non possedere le competenze o le conoscenze necessarie per valutare in maniera efficace l'affidabilità dei produttori: gli intervistati delle PMI che hanno indicato questo aspetto come un problema sono infatti l'8% in più rispetto a quelli delle grandi aziende (Figura 3).

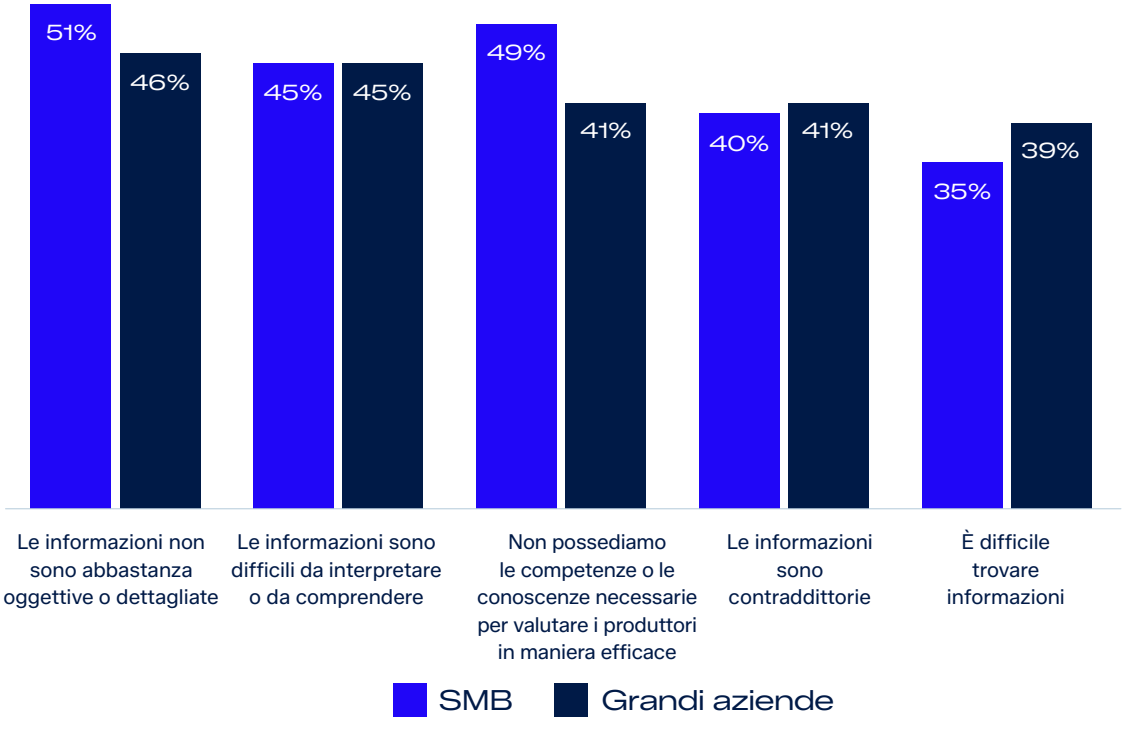


Figura 3: Perché per la tua organizzazione è difficile valutare l'affidabilità dei produttori di soluzioni di cybersecurity? n=504 (PMI), 2.260 (grandi aziende).

La mancanza di fiducia implica delle conseguenze

Questo studio di ricerca dimostra che la mancanza di fiducia tra un produttore di soluzioni di sicurezza e i propri clienti costituisce un grave problema sotto diversi aspetti. Alla domanda sull'impatto derivato dal non riporre piena fiducia nei propri produttori di servizi di cybersecurity, gli intervistati hanno evidenziato una serie di conseguenze sia dal punto di vista emotivo che operativo:

- **Il 51%** dichiara di nutrire una crescente preoccupazione sulla possibilità che la propria azienda possa subire un incidente informatico grave.
- **Il 45%** afferma che ciò aumenta la probabilità che la propria organizzazione decida di cambiare produttore, un processo costoso e destabilizzante per la maggior parte delle aziende.
- **Il 42%** prevede un inasprimento dei requisiti di supervisione.
- **Il 41%** sostiene di provare un senso di sicurezza minore riguardo al proprio livello di cybersecurity.
- **Nel 38%** dei casi, i partecipanti al sondaggio temono che l'azienda o loro stessi possano aver scelto un produttore non adeguato.

Queste ripercussioni segnalate si vanno ad aggiungere alle pressioni operative già esercitate sui team IT e di cybersecurity.

Valutazioni divergenti tra reparto IT e leadership

Un'altra sfida importante è rappresentata dalle divergenze tra chi utilizza quotidianamente gli strumenti di sicurezza informatica e chi ne approva i contratti. il 78% degli intervistati sostiene che il proprio team IT e la leadership aziendale o il consiglio di amministrazione hanno opinioni divergenti sull'affidabilità dei produttori di servizi di cybersecurity, e quasi un terzo dichiara che tali divergenze si verificano "Spesso" (Figura 4).

Gli intervistati hanno indicato che i vertici aziendali continuano a essere fortemente coinvolti nelle decisioni di acquisto. Solo l'1% delle organizzazioni dichiara che il consiglio di amministrazione o la leadership aziendale non svolgono alcun ruolo nel processo decisionale relativo all'acquisto di soluzioni di cybersecurity.

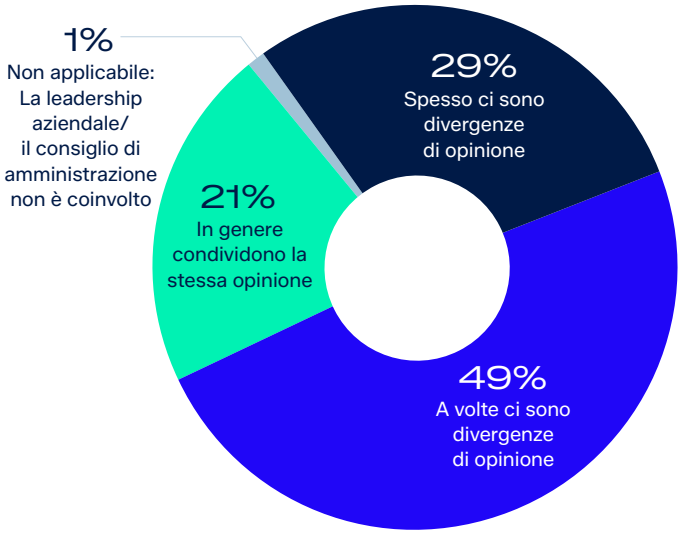


Figura 4: Esistono divergenze di opinione tra il team IT e la leadership aziendale/il consiglio di amministrazione riguardo all'affidabilità dei produttori di soluzioni di cybersecurity della tua organizzazione? n=5.000.

1%

Percentuale di organizzazioni intervistate che affermano che la leadership aziendale non svolge alcun ruolo nel processo decisionale relativo all'acquisto di soluzioni di cybersecurity.

Come generare fiducia nella cybersecurity

I partecipanti al sondaggio hanno indicato che pratiche di sicurezza trasparenti e fondate su dati verificabili sono elementi indispensabili per instaurare un clima di fiducia. Le aziende cercano produttori che suscitino fiducia, mostrando un comportamento aperto e trasparente, e applicando pratiche di sicurezza basate su prove concrete.

Sia tra i vertici aziendali che tra i team IT, le "Prove concrete che dimostrano maturità in materia di cybersecurity" sono risultate il principale fattore determinante per la fiducia nei produttori di soluzioni di sicurezza informatica. Tra queste prove figurano programmi Bug Bounty, un Trust Center pubblico, avvisi che contengono dettagli sulle vulnerabilità nei loro prodotti (e le correzioni che sono state apportate), valutazioni di terze parti e certificazioni.

Anche la risposta "Trasparenza e comunicazioni tempestive in caso di incidenti e divulgazioni" è risultata tra i fattori più importanti, classificandosi al secondo posto per la leadership aziendale e al terzo per i membri dei team IT.

Fattori che determinano la fiducia nei produttori di soluzioni cybersecurity

Fattori	Leadership aziendale/ CdA	Team IT/di cybersecurity	Fattori di influenza
Fattori principali	N°1	N°1	Prove concrete che dimostrano maturità in materia di cybersecurity, ad esempio: programmi Bug Bounty, Trust Center, avvisi, valutazioni di terze parti, certificazioni
	Nº2	N°3	Trasparenza e comunicazioni tempestive in caso di incidenti e divulgazioni
	N°3	N°4	Commenti di esperti dopo incidenti informatici gravi, ad esempio dichiarazioni rilasciate alla stampa o in televisione
	N°4	Nº2	Fornitura costante di servizi e prodotti di cybersecurity di alta qualità
	Nº5	Nº5	Risultati ottenuti in report compilati da analisti, ad es. Gartner Magic Quadrant
Fattori secondari	Nº6	#9	Trasparenza nelle procedure di sicurezza interna
	Nº7	Nº7	Risultati ottenuti in test indipendenti, ad es. MITRE, SE Labs
	#8	Nº6	Assistenza reattiva e affidabile
	#9	#8	Raccomandazione del tuo rivenditore/partner di cybersecurity
Fattori terziari	#10	#13	Qualità delle pubblicazioni sulla ricerca in materia di minacce
	#11	#12	Presenza in testate giornalistiche finanziarie e di business
	#12	#11	Esperienze di altri (colleghi/clienti)
	#13	#10	Esperienze personali

Quali sono/sarebbero i principali fattori di influenza sul livello di fiducia della leadership aziendale/del consiglio di amministrazione nei confronti di un produttore di soluzioni di cybersecurity? Risposte classificate al primo posto
Quali sono/sarebbero i principali fattori di influenza sul livello di fiducia dei team IT/di cybersecurity nei confronti di un produttore di soluzioni di cybersecurity? Risposte classificate al primo posto

Sophos si impegna a guadagnarsi la fiducia di clienti e partner

Sophos sa benissimo che la fiducia va conquistata, non pretesa. Ed è per questo motivo che lavoriamo instancabilmente per guadagnarcela ogni giorno, seguendo un'etica di trasparenza e integrità, e impegnandoci a tutelare la sicurezza e la privacy.

Il fulcro delle nostre attività è il Sophos Trust Center, dove pubblichiamo avvisi di sicurezza, documentiamo le vulnerabilità dei prodotti e le correzioni apportate, definiamo il nostro profilo di conformità alle normative e condividiamo i modi in cui proteggiamo i dati dei clienti.

Questa trasparenza è dimostrata anche dall'indagine "Pacific Rim" di Sophos X-Ops, che ha documentato pubblicamente una campagna di cinque anni, condotta da cybercriminali basati in Cina. Durante le indagini, abbiamo condiviso tattiche, tecniche e procedure (TTP) dettagliate, nonché indicatori di compromissione (IoC) e linee guida difensive per aiutare le organizzazioni a incrementare la resilienza nell'intero settore della sicurezza.

Rivelando le sofisticate attività di questi attacchi governativi, collaborando con enti nazionali e altri produttori e documentando con franchezza sia i propri punti di forza che le proprie debolezze, Sophos ribadisce che la fiducia va conquistata giorno dopo giorno, attraverso l'onestà, la responsabilità e l'impegno a salvaguardare l'intero ecosistema digitale esteso.

Maggiori Informazioni

Per saperne di più sul nostro impegno a instaurare un rapporto di fiducia con clienti e partner, e sulle risorse che mettiamo a disposizione per aiutarti a valutare il livello di fiducia che puoi riporre in Sophos, visita il Trust Center o rivolgiti al tuo partner o commerciale Sophos di riferimento.

SOPHOS

Per saperne di più, visita il Trust Center o parla con il tuo partner o commerciale Sophos di riferimento.

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