Luglio 2025

Report di mercato

The MSP Customer Insight Report 2025

Di cosa hanno bisogno le organizzazioni di tutto il mondo dai propri provider di servizi gestiti per la sicurezza informatica

Barracuda®
Your business, secured.

Sommario

Introduzione

Questo report esplora quello di cui le organizzazioni di tutto il mondo hanno bisogno e si aspettano dai propri provider di servizi gestiti (MSP) per quanto riguarda i servizi di sicurezza informatica. Si basa sui risultati di un nuovo sondaggio internazionale sui clienti MSP commissionato da Vanson Bourne.

Gli MSP sono diventati fondamentali per le aziende. La maggior parte delle organizzazioni intervistate sta già esternalizzando alcune o tutte le proprie esigenze di sicurezza informatica agli MSP, mentre altre stanno ne stanno esplorando l'opportunità.

Questo report serve a far capire agli MSP di cosa hanno bisogno i loro clienti attuali ora e in futuro, come sono e dove trovare i potenziali clienti, e cosa spinge i clienti verso un concorrente.

Nel complesso, i risultati dimostrano che:

- I clienti hanno bisogno degli MSP per gestire la propria sicurezza man mano che crescono le loro esigenze.
- Nei prossimi anni, i clienti avranno particolarmente bisogno di aiuto per l'implementazione di applicazioni di IA/apprendimento automatico e per la sicurezza della rete: e per questo sono disposti a pagare di più.

Metodologia

Barracuda ha incaricato la società indipendente di ricerche di mercato Vanson Bourne di condurre un sondaggio globale su 2.000 responsabili senior in materia di sicurezza in ruoli IT e aziendali in organizzazioni con un numero di dipendenti compreso tra 50 e 2.000, provenienti da un'ampia gamma di settori negli Stati Uniti, Regno Unito, Francia, DACH (Germania, Austria, Svizzera), Benelux (Belgio, Paesi Bassi, Lussemburgo), i Paesi nordici (Danimarca, Finlandia, Norvegia, Svezia), Australia, India e Giappone. Il sondaggio è stato condotto ad aprile e maggio 2025.

Introduzione

- La maggior parte dei clienti MSP prenderà in considerazione il cambio di fornitori e alla base di questa azione vi sono le preoccupazioni relative alla capacità degli MSP di assisterli nel porre rimedio e nel recupero da un attacco informatico.

Ci auguriamo che questo report aiuti gli MSP a definire le proprie strategie future, individuare nuove opportunità e colmare eventuali lacune. Barracuda è qui per aiutarti in ogni fase del percorso. Insieme possiamo garantire che più organizzazioni siano resilienti dal punto di vista informatico e protette mentre affrontiamo le sfide delle minacce in continua evoluzione.

Risultati principali

85%

delle organizzazioni con 1.000—2.000 dipendenti si affidano agli MSP per il supporto alla sicurezza, rispetto al 61% di quelle con 50—100 dipendenti

48%

delle organizzazioni si rivolge agli MSP per ricevere supporto di sicurezza 24 ore su 24

52%

delle organizzazioni si rivolge agli MSP per chiedere aiuto quando il numero degli strumenti di sicurezza diventa ingestibile: la ragione principale citata

51%

delle organizzazioni si rivolge agli MSP per essere aiutate a evolvere le proprie strategie di sicurezza man mano che crescono: il secondo motivo più citato

39%

delle organizzazioni si aspetta di aver bisogno dei prossimi anni del supporto degli MSP con strumenti e applicazioni di IA e machine learning, il motivo principale citato

92%

delle organizzazioni è disposto a pagare di più per il supporto con l'integrazione degli strumenti di sicurezza

45%

cambieranno MSP se non potranno notare prove di competenze, esperienza e capacità di supportarli con sicurezza 24/7: il motivo principale citato

La base clienti per gli MSP

Le minacce informatiche continuano a evolversi in quanto gli attaccanti sfruttano strumenti di intelligenza artificiale e servizi criminali a pagamento per lanciare attacchi sempre più sofisticati e per farlo più rapidamente, in volumi maggiori e con maggiore precisione.

I professionisti IT e della sicurezza sono esposti a un bombardamento costante di tali minacce. Per proteggere l'organizzazione e i suoi asset, è necessario disporre di soluzioni di sicurezza avanzate, funzionalità di monitoraggio, gestione e mitigazione attive 24 ore su 24, nonché di una profonda conoscenza del panorama delle minacce. Poche organizzazioni possono soddisfare tutte tali esigenze internamente.

Risultato chiave: il 73% delle organizzazioni intervistate esternalizza i servizi di sicurezza a un MSP

Il 96% delle organizzazioni intervistate è già impegnato o sta considerando di lavorare con un MSP: il 73% afferma di aver già esternalizzato i servizi di sicurezza a un MSP, con un ulteriore 18% che attualmente sta valutando i fornitori e un altro 5% che sta considerando la possibilità di utilizzare un MSP.

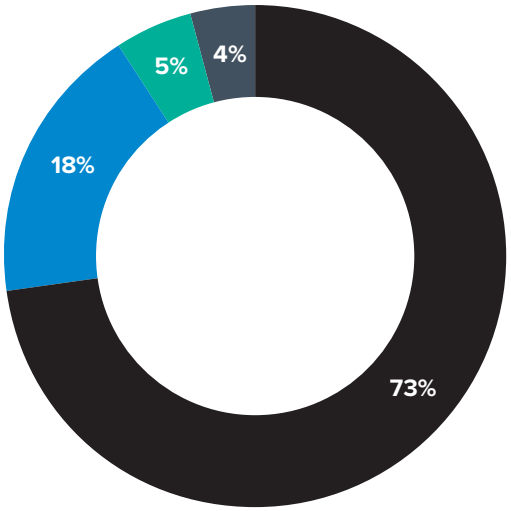

FIGURA 1

La tua organizzazione esternalizza attività di sicurezza IT a un Managed Service Provider (MSP)?

n=2.000

- Sì
- Attualmente stiamo valutando i fornitori
- Stiamo considerando la possibilità
- No

Dietro questi numeri si nascondono alcune interessanti variazioni.

Ad esempio, le organizzazioni intervistate più grandi sono più propense a utilizzare gli MSP rispetto a quelle più piccole.

Risultato chiave: l'85% degli intervistati con 1.000—2.000 dipendenti si affida agli MSP per il supporto alla sicurezza, rispetto al 61% di quelli con 50—100 dipendenti

Questo livello più elevato di coinvolgimento degli MSP può riflettere il fatto che le organizzazioni più grandi presentano una maggiore complessità in termini di sicurezza e dispongono di una gamma più ampia di strumenti da gestire.

Ad esempio, le organizzazioni intervistate più grandi tendono a preoccuparsi più di quelle più piccole per la crescente complessità del loro ambiente di sicurezza (42%) e degli attacchi informatici (46%). Per le aziende intervistate più piccole, le percentuali corrispondenti sono del 32% e del 34%.

Un leggermente preoccupante 10% delle organizzazioni intervistate più piccole non ha piani per coinvolgere un MSP per ricevere aiuto per la sicurezza informatica. Le aziende più piccole generalmente dispongono di meno risorse interne per la protezione, per cui questo approccio potrebbe lasciarle vulnerabili agli attacchi.

I settori più propensi a esternalizzare la sicurezza informatica agli MSP sono la pubblica amministrazione locale (84%) e l'istruzione (78%). Esiste un livello inferiore di coinvolgimento nel settore del tempo libero e dell'intrattenimento (60%), nel commercio al dettaglio (65%) e nella manifattura (57%).

Tra i Paesi intervistati, le organizzazioni nel Regno Unito e nel Benelux sono quelle più propense a collaborare con un MSP (con il 79% e l'81% rispettivamente). I livelli più bassi di collaborazione si osservano nei paesi nordici (54%) e in Giappone (59%).

I clienti hanno bisogno degli MSP per essere aiutati a gestire la propria sicurezza man mano che crescono

La ricerca dimostra che, dal punto di vista dei clienti, il partner MSP ideale offre sia un supporto pratico, focalizzato su prodotto e tecnologia, sia un aiuto più strategico per quanto riguarda i piani di sicurezza e la conformità.

L'analisi dei primi due risultati suggerisce che gli MSP svolgono un ruolo chiave nell'assistere le organizzazioni nella gestione delle implicazioni di sicurezza legate alla crescita aziendale.

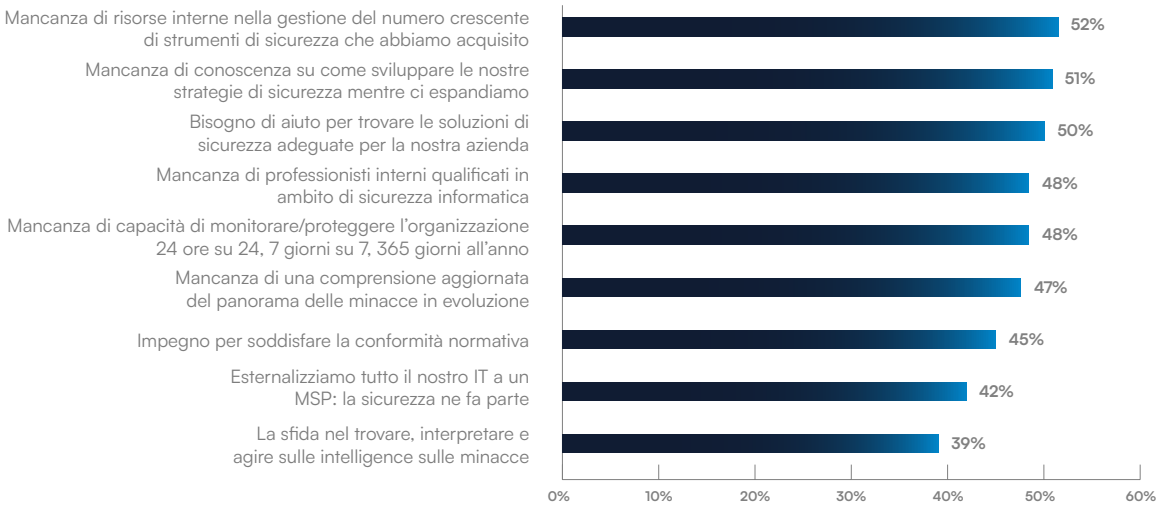

FIGURA 2

I motivi per esternalizzare la sicurezza a un MSP

n=2.000

Risultato chiave: il 52% delle organizzazioni si rivolge agli MSP per assistenza quando il numero di strumenti di sicurezza diventa ingestibile

Il supporto per gestire uno stack sempre crescente di prodotti per la sicurezza è stato il motivo più comune per cui ci si è rivolti agli MSP. È probabile che numerosi di questi strumenti provengano da fornitori diversi e che la maggior parte non si integri tra loro.

Questa cifra sale al 60% tra gli intervistati nel settore manifatturiero. È probabile che le aziende manifatturiere abbiano un numero significativo di dispositivi IoT e sistemi connessi, e quindi una maggiore probabilità di proliferazione degli strumenti per la sicurezza.

Altri risultati dello studio mostrano che la mancanza di integrazione può aumentare l'esposizione e il rischio per la sicurezza, rendendo più difficile e costoso gestire la sicurezza e rilevare e mitigare le minacce.

Risultato chiave: il 51% delle organizzazioni si rivolge agli MSP per aiutare a far evolvere le proprie strategie di sicurezza mentre crescono

Il secondo motivo più citato per rivolgersi a un MSP per il supporto alla sicurezza riflette l'evoluzione del ruolo dei fornitori di servizi come consulenti per la sicurezza: il 51% si rivolge al proprio partner di servizi per essere aiutato a migliorare e ad aggiornare le proprie strategie di sicurezza man mano che l'organizzazione si espande e cambia. Le organizzazioni del settore dell'istruzione e della sanità erano particolarmente inclini a indicare questo motivo come il principale per coinvolgere un MSP (entrambe al 55%).

Gli istituti formativi sono anche tra i più propensi a preoccuparsi della crescente complessità della loro sicurezza IT (48% rispetto al 38% complessivo), il che suggerisce che stanno lottando per proteggere un numero crescente di asset digitali. Per loro rivolgersi a un MSP per chiedere aiuto è una cosa naturale.

Risultato chiave: il 48% delle organizzazioni si rivolge agli MSP per un supporto alla sicurezza attivo 24 ore su 24

La maggior parte delle organizzazioni riconosce che la sicurezza informatica è un'attività costante e questo richiede livelli di personale e investimenti che molte di queste non hanno a livello interno. Affidarsi a un MSP per l'assistenza nel monitoraggio e nella risposta alle minacce e agli avvisi di sicurezza 24 ore su 24, 7 giorni su 7, è un altro fattore chiave di coinvolgimento.

Numerosi MSP ora gestiscono, spesso insieme ai fornitori di sicurezza, un centro operativo di sicurezza gestito (SOC) che offre una copertura così esperta. Per ottenere il livello più completo di sicurezza, questo può essere combinato con una soluzione gestita di rilevamento e risposta estesa (XDR) in grado di coprire l'ampia superficie di attacco, inclusi endpoint, e-mail, cloud, applicazioni e reti.

Per numerose delle organizzazioni intervistate, il coinvolgimento con gli MSP è anche strettamente legato alla mancanza di professionisti interni di sicurezza informatica, citata come motivo dal 48%. La carenza di competenze sembra essere una sfida universale in quanto la proporzione rimane costante nelle aziende di tutte le dimensioni.

Nel caso del 42% degli intervistati, la sicurezza viene esternalizzata a un MSP e integrata con altri servizi IT. Questo rappresenta sia un'opportunità che un rischio per gli MSP, in particolare quando si tratta di clienti che decidono di trasferire la propria attività. A tal proposito vedere la sezione sui fattori decisivi.

In futuro, i clienti avranno bisogno di maggiore supporto per l'IA e la sicurezza di rete

Nei prossimi due anni, è molto probabile che i clienti chiedano aiuto agli MSP per l'implementazione di strumenti e applicazioni di IA e apprendimento automatico. Questo è seguito dall'assistenza per le implementazioni di sicurezza di rete, come le misure zero-trust e le soluzioni SASE (Secure Access Service Edge).

Risultato chiave: nei prossimi due anni il 39% delle organizzazioni prevede di aver bisogno del supporto MSP con strumenti e applicazioni di machine learning e IA

L'IA e la sicurezza di rete sono aree di crescente attenzione aziendale, vulnerabilità di sicurezza e complessità tecnica. Possono essere difficili da comprendere, soprattutto per il 48% delle organizzazioni con carenza di personale.

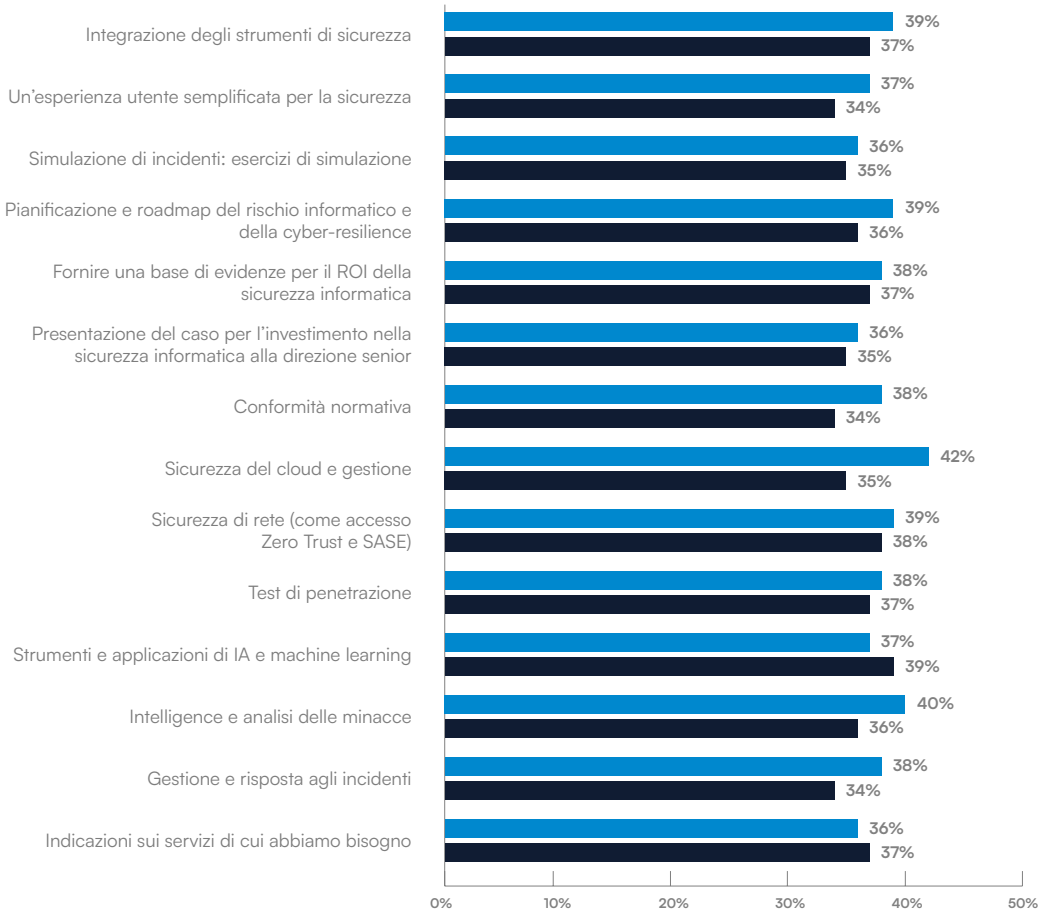

FIGURA 3

Opportunità di sicurezza per gli MSP: dove le organizzazioni prevedono di aver bisogno del supporto dei fornitori di servizi nei prossimi 1-2 anni

n=2.000

- Già utilizzato da MSP
- Si prevede di avere bisogno di supporto

I risultati mettono in luce i diversi percorsi per le organizzazioni di varie dimensioni.

Ad esempio, tra le organizzazioni con 50 - 100 dipendenti, la percentuale che cerca supporto futuro con l'IA sale al 44%, con il 29% già impegnato. Per le organizzazioni più grandi, il 44% collabora con gli MSP sull'IA e il 37% prevede di aver bisogno di supporto nei prossimi due anni.

Questo suggerisce che le organizzazioni più grandi comprendono già le limitazioni nella gestione dell'IA e del machine learning da sole e stanno collaborando attivamente con gli MSP per ottimizzare il loro uso dell'IA sia nell'IT sia nella sicurezza. Un quadro simile, ma con differenze minori, si osserva per la sicurezza di rete.

Vale anche la pena notare l'uso diffuso e la domanda di servizi strategici come la pianificazione del rischio informatico e della resilienza, la simulazione di risposta agli incidenti e la presentazione del caso per il ROI della sicurezza informatica.

I clienti sono disposti a pagare di più per i servizi che desiderano

Il sondaggio ha rilevato che quasi tutti i clienti MSP sono disposti a pagare di più per i servizi aggiuntivi di cui hanno bisogno nei prossimi due anni, e circa il 70% è disposto a pagare fino al 10% o al 25% in più.

Risultato chiave: il 92% delle organizzazioni è disposto a pagare di più per il supporto con l'integrazione degli strumenti di sicurezza

I servizi per i quali è più probabile che siano disposti a spendere di più includono strumenti e applicazioni di IA e machine learning, sicurezza del cloud e sicurezza di rete. I risultati rimangono costanti in tutte le dimensioni aziendali.

Nel complesso, gli strumenti e le attività operative ottengono risultati migliori quando si tratta di spese aggiuntive. Esiste una certa riluttanza a spendere di più per servizi meno tangibili come la simulazione degli incidenti, la presentazione del caso per gli investimenti nella sicurezza informatica o la guida sui servizi necessari.

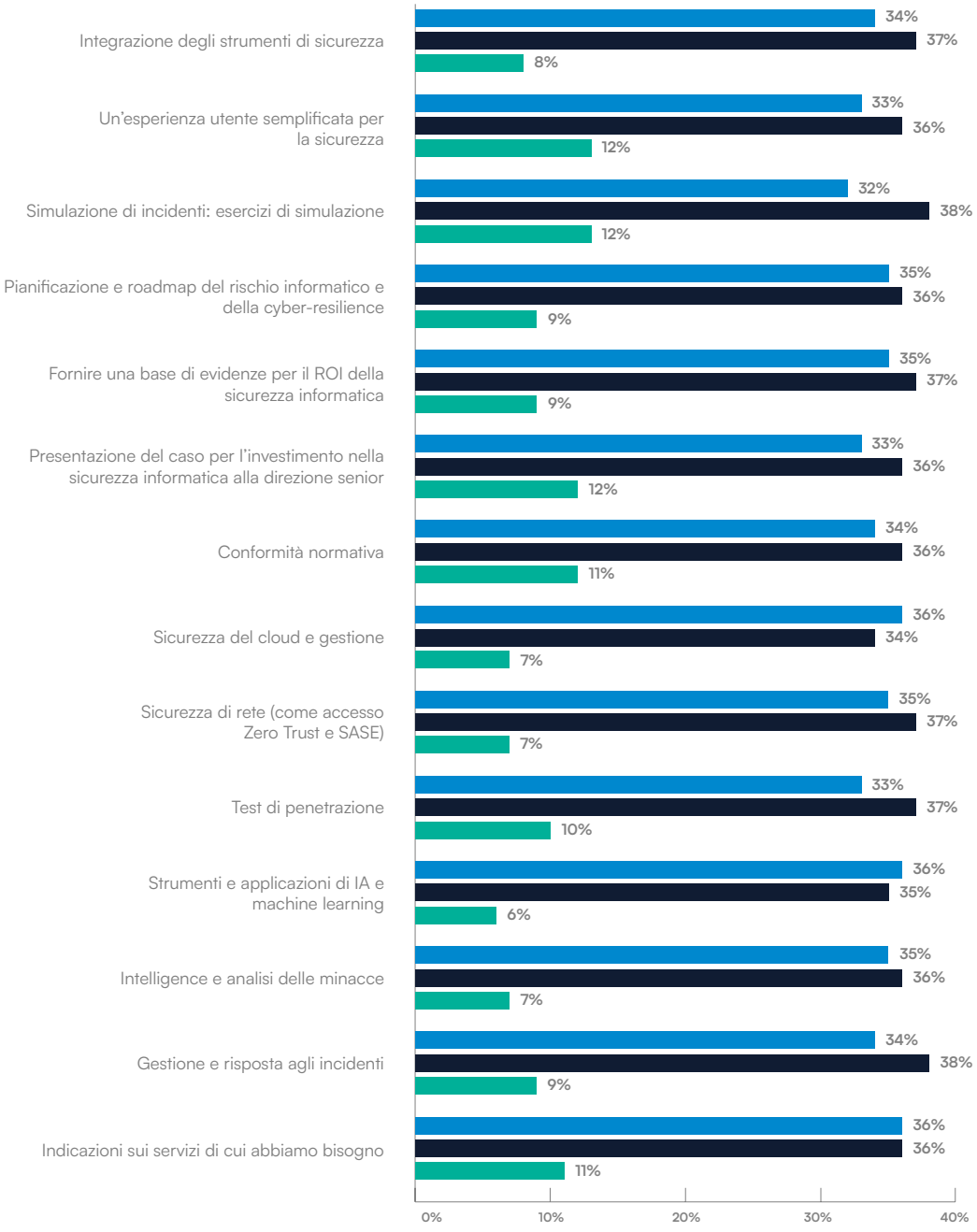

FIGURA 4

I costi aggiuntivi per le organizzazioni sono disposti a pagare per questi servizi dagli MSP nei prossimi 1 o 2 anni

n=2.000

Tuttavia, quello a cui i clienti danno priorità e in cui sono disposti a investire appare molto diverso se visto attraverso il punto di vista di un incidente di sicurezza, come un incidente basato su e-mail o un attacco ransomware: a tal proposito guarda la sezione riportata di seguito relativa all'impatto di una violazione della sicurezza.

Gli MSP rischiano di perdere clienti se non riescono a dimostrare le propria capacità

I risultati mostrano che quando si tratta di affidarsi a un partner MSP, la fedeltà è limitata e dipende dalla fiducia del cliente nelle competenze, nella qualità e nella stabilità aziendale del fornitore di servizi. Solo il 2% degli intervistati ha dichiarato di non riuscire a immaginare di passare a un altro MSP. Per tutti gli altri, ci sono alcuni fattori decisivi evidenti.

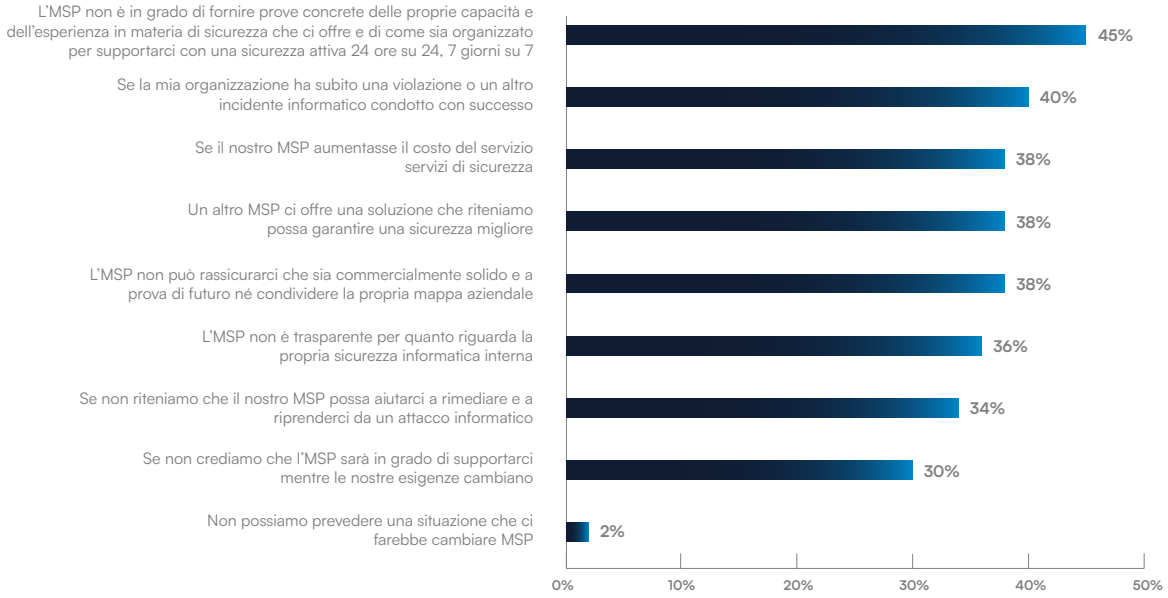

FIGURA 5

Cosa ti farebbe prendere in considerazione il passaggio a un altro MSP per il supporto alla sicurezza informatica?

n=2.000

Una violazione della sicurezza è un chiaro fattore di interruzione delle relazioni e per più di un terzo (38%) dei clienti MSP un aumento dei prezzi o un'offerta migliore da parte di un altro MSP li indurrebbe a cambiare fornitore.

Risultato chiave: il 45% cambierà MSP se non riesce a vedere notare di competenze, esperienza e capacità di supporto con sicurezza attiva 24/7

Per gli MSP interessati, non si tratta solo di perdere il business della sicurezza informatica: l'89% dei clienti in uscita che ha abbinato servizi IT alla sicurezza rimuoverà anche tali attività, contemporaneamente (46%) o successivamente (42%).

Vale la pena menzionare che il 38% dei clienti MSP afferma che cambierà fornitore in caso di aumento dei costi da parte dell'MSP. Insieme ai risultati sulla disponibilità a investire, questo suggerisce che i clienti MSP pagheranno volentieri di più per i servizi che desiderano e di cui hanno

bisogno, ma sono meno a loro agio con gli aumenti dei prezzi imposti arbitrariamente dall'MSP.

La buona notizia è che i potenziali ostacoli sono quasi tutte le aree che gli MSP possono affrontare investendo nella propria resilienza aziendale e di sicurezza e in quella dei loro clienti, rafforzando così la fiducia e la trasparenza.

Le organizzazioni colpite da una violazione investono maggiormente in sicurezza ed esternalizzazione

Una violazione e-mail o un attacco ransomware condotto con successo sposta le priorità di sicurezza.

Le differenze tra coloro che sono stati colpiti e coloro che non lo sono stati sono evidenti quando si osservano i servizi per i quali sono disposti a pagare di più e le attività che hanno compreso di non poter gestire efficacemente per intero. Questi risultati mettono in evidenza le aree in cui le vittime possono sentirsi particolarmente vulnerabili.

Risultato chiave: il 91% delle vittime di attacchi è disposto a pagare di più per un'esperienza utente di sicurezza semplificata, rispetto al 77% delle non-vittime

Ad esempio, il 91% delle vittime è disposto a pagare di più per un'esperienza utente semplificata in termini di sicurezza, rispetto al 77% di coloro che non sono stati colpiti. La cifra complessiva è dell'88%. Questo suggerisce che per numerose vittime, l'errore umano o una configurazione errata, entrambi facilmente innescati da interfacce utente complesse, potrebbe aver avuto un ruolo nell'attacco.

Le vittime sono anche più disposte a pagare di più per servizi di resilienza informatica, come la pianificazione della risposta agli incidenti, la conoscenza della normativa e della conformità e la guida strategica sui servizi di sicurezza. Questo suggerisce che le vittime sono disposte a investire in settori che le rendano meglio preparate a rispondere e a riprendersi da futuri attacchi.

Quando si tratta di attività svolte internamente o esternalizzate, si riscontra la stessa disparità: chi non è stato direttamente colpito da un incidente è più propenso a ritenere di poter gestire le cose da sé.

Risultato chiave: l'81% delle vittime di attacco prevede di esternalizzare la sicurezza del cloud e la gestione, rispetto al 73% delle non vittime

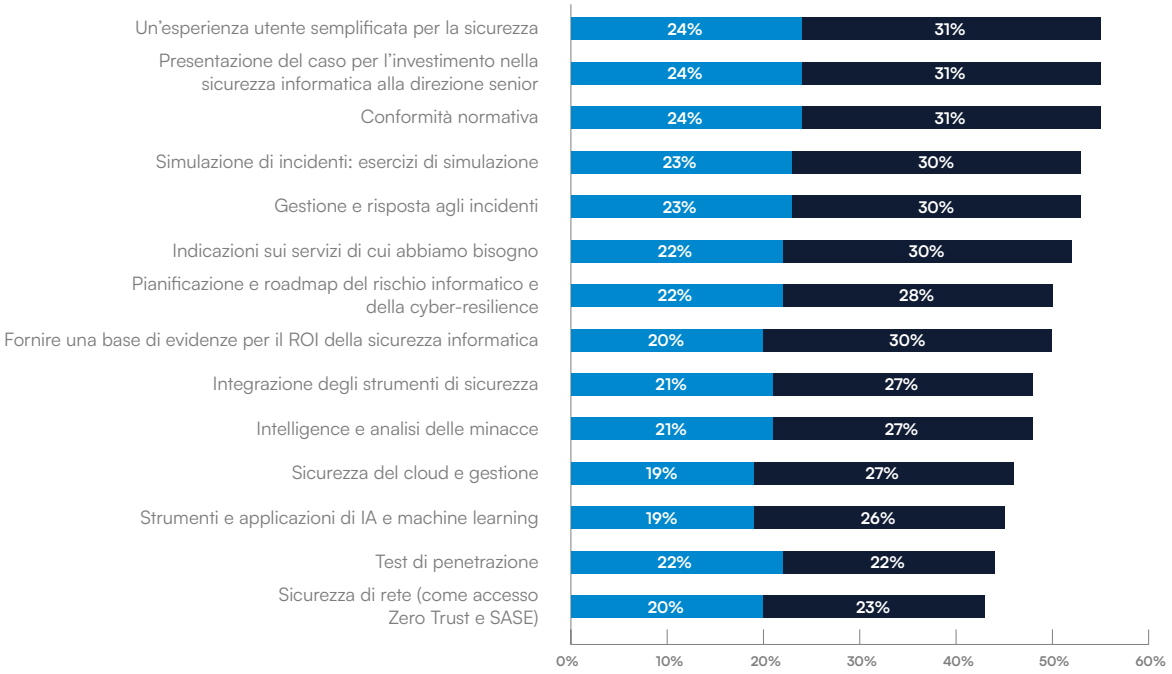

FIGURA 6

Le organizzazioni che intendono gestire internamente ciascuna delle seguenti attività nei prossimi 1 - 2 anni

n=2.000

- Ha subito una violazione delle e-mail o un attacco ransomware nell'ultimo anno
- Non ha subito una violazione delle e-mail o un attacco ransomware nell'ultimo anno

Conclusione

I risultati mostrano che nel 2025 gli MSP affronteranno numerose e promettenti opportunità, ma anche alcune sfide.

Ad esempio, numerosi clienti desiderano aiuto per gestire la proliferazione degli strumenti di sicurezza. Tuttavia, assistere più clienti nel gestire diversi prodotti può rapidamente diventare un compito impegnativo per i fornitori. I fornitori in ambito di sicurezza hanno un ruolo fondamentale nel supportare gli MSP nell'integrazione delle attività di gestione, risposta e reporting tramite dashboard centralizzate e consolidamento dei prodotti. Allo stesso modo, i fornitori possono aiutare gli MSP a soddisfare la chiara domanda di monitoraggio della sicurezza 24/7 con SOC gestiti.

Vi è poi la necessità di supportare i clienti attraverso la conformità e le normative e con l'implementazione di strumenti e applicazioni di IA e machine learning.

Inoltre, gli MSP devono prepararsi per i clienti che desiderano servizi più proattivi e predittivi, come l'intelligence sulle minacce, la pianificazione della risposta agli indicenti, la gestione del rischio e la consulenza strategica.

Come se ciò non bastasse, gli MSP devono inoltre considerare la propria sostenibilità commerciale e fornire prove di competenza e di un solido modello di business, altrimenti rischiano di perdere clienti a favore dei concorrenti. Questo richiede un portafoglio di prodotti avanzato e innovativo, ma anche facile da acquistare, implementare e utilizzare per i clienti. Richiede inoltre che i fornitori in ambito di sicurezza siano impegnati a collaborare.

Conclusione

In che modo Barracuda può essere di aiuto

Noi di Barracuda siamo impegnati al 100% nel canale e nell'aiutare i nostri partner a raggiungere il successo e crescere.

BarracudaONE™

BarracudaONE è una piattaforma di sicurezza informatica basata su IA che offre prodotti integrati accessibili da una dashboard centralizzata per massimizzare la protezione e la resilienza informatica, pur essendo facile da acquistare, implementare e utilizzare.

La piattaforma semplifica l'amministrazione degli strumenti di sicurezza per un MSP per tutti i suoi clienti, garantendo che gli strumenti siano configurati correttamente, che gli avvisi siano centralizzati e che vengano forniti report che dimostrano il valore che un MSP apporta ai propri clienti in termini di sicurezza.

BarracudaONE è disponibile senza costi aggiuntivi per gli MSP, altri partner di canali e clienti che già utilizzano Barracuda Email Protection, Barracuda Cloud-to-Cloud Backup e Barracuda Data Inspector. La piattaforma offre un'interfaccia centralizzata per gli MSP e i partner per gestire facilmente soluzioni e licenze.

Barracuda Managed XDR™

Gli MSP, i partner e gli utenti finali possono rafforzare ulteriormente il loro livello di sicurezza con Barracuda Managed XDR, un servizio attivo 24/7 che offre rilevamento e risposta alle minacce da parte di esperti, supportati dal pluripremiato SOC di Barracuda.

Informazioni su Barracuda

Barracuda è un'azienda leader globale nel settore della sicurezza informatica che offre una protezione completa contro le minacce complesse per le aziende di qualsiasi dimensione. La nostra piattaforma basata sull'IA protegge e-mail, dati, applicazioni e reti con soluzioni innovative, XDR gestito e una dashboard centralizzata per ottimizzare la protezione e rafforzare la resilienza informatica. Scelto da centinaia di migliaia di professionisti IT e provider di servizi gestiti in tutto il mondo, Barracuda offre difese potenti e facili da acquistare, implementare e utilizzare.

Informazioni Vanson Bourne

Vanson Bourne è uno specialista indipendente nella ricerca di mercato nel settore tecnologico. La sua reputazione per un'analisi solida e credibile basata sulla ricerca si fonda su principi di ricerca rigorosi e sulla capacità di raccogliere le opinioni dei decisori senior in tutte le funzioni tecniche e aziendali, in tutti i settori e in tutti i principali mercati. Per ulteriori informazioni, visita il sito vansonbourne.com.