SOPHOS

Il Punto di Vista degli MSP 2024

Approfondimenti sugli strumenti di cybersecurity, sui rischi, sulle sfide e sulle opportunità commerciali di 350 MSP.

Whitepaper Sophos. Maggio 2024

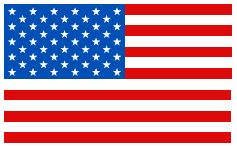
Introduzione

Il report offre approfondimenti su cinque aspetti fondamentali delle attività degli MSP:

- Strumenti RMM e PSA
- Gestione della cybersecurity
- Servizi MDR
- Sfide e rischi affrontati dagli MSP e dai loro clienti
- Impatto delle assicurazioni informatiche

I dati si basano sui risultati di un sondaggio indipendente e agnostico rispetto ai vendor, a cui hanno partecipato 350 MSP in Stati Uniti (200), Regno Unito (50), Germania (50) e Australia (50). Il sondaggio è stato condotto per conto di Sophos dall'azienda di ricerca indipendente Vanson Bourne a marzo 2024.

350 MSP
in quattro paesi



Stati Uniti
200 partecipanti

Regno Unito
50 partecipanti

Germania
50 partecipanti

Australia
50 partecipanti

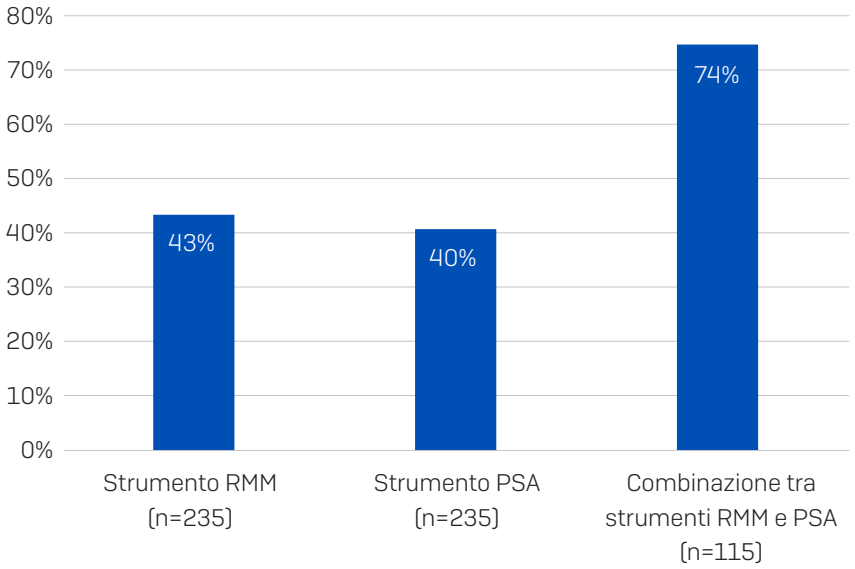
Strumenti RMM e PSA

Gli strumenti di monitoraggio e gestione da remoto (Remote Monitoring and Management, RMM) e automazione dei servizi professionali (Professional Services Automation, PSA) permettono di fornire servizi MSP in maniera efficace ed efficiente. Allo stesso tempo, aiutano a ridurre i costi operativi. Dal sondaggio sono emersi due spunti importanti su queste tecnologie fondamentali per gli MSP.

La combinazione tra strumenti RMM e PSA offre livelli di soddisfazione molto più alti, rispetto all'uso di un singolo strumento

Quasi tre quarti (74%) degli MSP che hanno adottato un approccio basato sulla combinazione di strumenti RMM/PSA hanno dichiarato di essere "molto soddisfatti" della loro soluzione, rispetto ad appena il 43% degli MSP che utilizzano un singolo strumento RMM e al 40% di quelli che impiegano un singolo strumento PSA.

Partecipanti al sondaggio che hanno dichiarato di essere "molto soddisfatti" dei propri strumenti RMM e PSA attuali

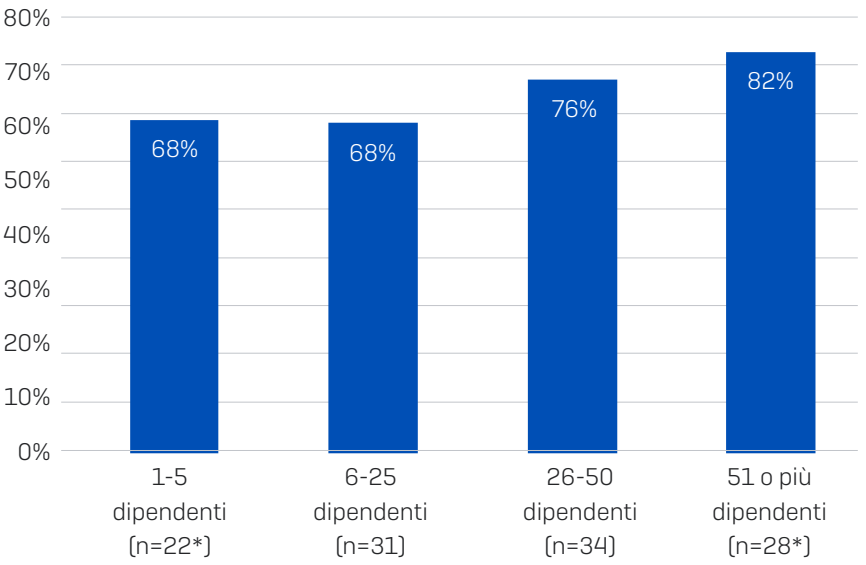


Qual è il livello di soddisfazione della tua organizzazione con gli strumenti RMM e PSA che utilizza attualmente?
Base di partecipanti indicata nel grafico

Il livello di soddisfazione per l'utilizzo di una combinazione di strumenti RMM/PSA aumenta in base alle dimensioni dell'MSP

Poco più di due terzi (68%) degli MSP con fino a 25 dipendenti si ritengono soddisfatti della propria combinazione di strumenti RMM/PSA, una percentuale che sale al 76% per gli MSP con 26-50 dipendenti e all'82% per gli MSP con 51 o più dipendenti. Data la probabilità che gli MSP con più dipendenti forniscano servizi a un maggior numero di clienti, i risultati suggeriscono che a una quantità elevata di clienti corrisponde la possibilità di trarre maggiore vantaggio dall'uso di una combinazione di strumenti RMM/PSA.

Partecipanti al sondaggio che hanno dichiarato di essere "molto soddisfatti" dei propri strumenti RMM e PSA attuali



Qual è il livello di soddisfazione della tua organizzazione con gli strumenti RMM e PSA che utilizza attualmente?
Base di partecipanti indicata nel grafico.
* Il numero di partecipanti in questa fascia è basso, per cui i risultati vanno considerati indicativi, piuttosto che significativi dal punto di vista statistico.

Consiglio: per gli MSP che utilizzano un unico strumento RMM/PSA potrebbe essere raccomandabile passare a una soluzione che prevede una combinazione di strumenti RMM/PSA. Questa strategia potrebbe aumentare il livello di soddisfazione, specialmente se si desidera ampliare la clientela.

Gestione della cybersecurity

Partnership con vendor di cybersecurity

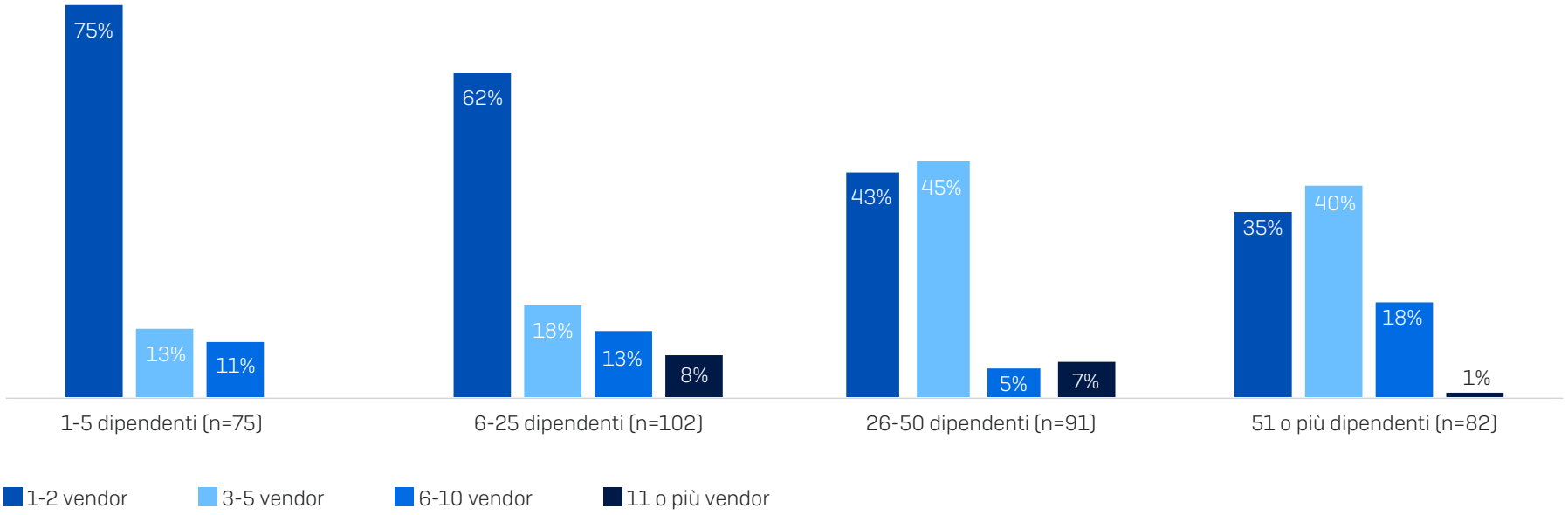
La cybersecurity è uno degli aspetti principali di cui si occupa la maggior parte degli MSP. Dallo studio è emerso che tipicamente gli MSP collaborano con pochi vendor per proteggere i propri clienti:

- Il 53% si affida a 1-2 vendor di cybersecurity
- L'83% collabora con 1-5 vendor di cybersecurity
- Il 4% utilizza 11 o più vendor di cybersecurity

I dati mostrano anche che, generalmente, il numero di vendor di cybersecurity utilizzati aumenta in maniera direttamente proporzionale alle dimensioni dell'organizzazione MSP. A collaborare con uno o due vendor di cybersecurity è il 75% degli MSP con meno dipendenti (1-5) e appena il 35% degli MSP con 51 o più dipendenti.

C'è invece una maggiore probabilità che ad affidarsi a sei o più vendor di cybersecurity siano gli MSP con più dipendenti, a confronto con quelli con organizzazioni più piccole: rispettivamente il 20% (cifra arrotondata) e l'11%. Sebbene da un lato instaurare partnership con più vendor di cybersecurity possa aumentare la quantità di servizi a disposizione dei clienti, dall'altro aumenta i costi ricorrenti correlati alla gestione dei vendor, nonché le sfide dovute alla necessità di integrare tecnologie diverse.

Numero di vendor di cybersecurity utilizzati per proteggere i clienti



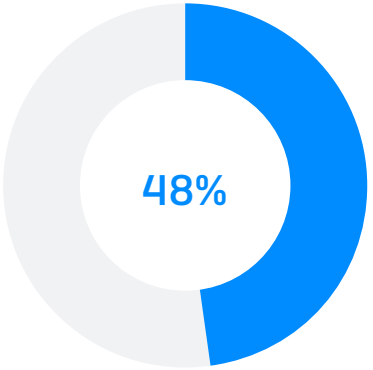
Quanto vendor di cybersecurity utilizza attualmente la tua organizzazione per proteggere i clienti? n=350. Base di partecipanti indicata nel grafico. Le risposte "Non lo so" sono state omesse.

Consolidare le piattaforme di cybersecurity

Il sondaggio rivela che per gli MSP esiste un'ottima probabilità di incrementare l'efficienza e ridurre i costi, consolidando le piattaforme di cybersecurity.

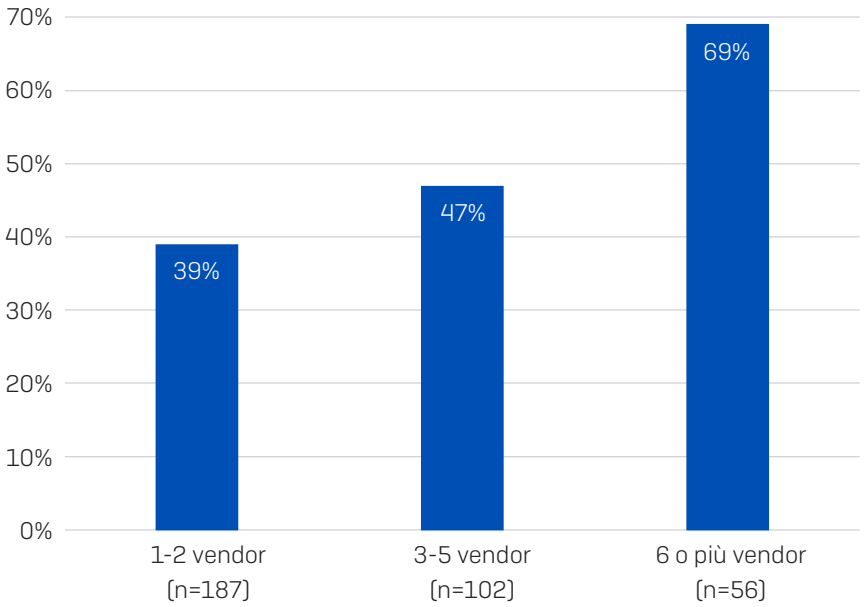
Gli MSP che al momento si affidano a più piattaforme stimano che risparmierebbero, in media, il 48% del tempo quotidiano attualmente dedicato alle attività di gestione, se potessero gestire tutti gli strumenti di sicurezza da un'unica piattaforma.

Stima del risparmio di tempo quotidiano di gestione che deriverebbe dal consolidare tutti i prodotti in un'unica piattaforma di cybersecurity



Il potenziale risparmio in termini di tempo di gestione aumenta in maniera direttamente proporzionale al numero di vendor di cybersecurity utilizzati attualmente. Gli MSP che collaborano con sei o più vendor di cybersecurity ritengono che ridurrebbero di più di due terzi (69%) i tempi quotidiani di gestione, se potessero gestire tutti gli strumenti di sicurezza da un'unica piattaforma. Un'abbreviazione delle tempistiche di questa entità comporterebbe una differenza tangibile in termini di redditività. Allo stesso tempo, concederebbe ai team più tempo da dedicare ad attività che generano un utile.

Media stimata del risparmio di tempo quotidiano di gestione che deriverebbe dal consolidare tutti i prodotti in un'unica piattaforma di cybersecurity - Dati suddivisi in base al numero di vendor utilizzati



Potresti fornire una stima del tempo di gestione che la tua organizzazione potrebbe risparmiare ogni giorno, se potesse gestire tutti gli strumenti di cybersecurity da un'unica piattaforma? Base di partecipanti indicata nel grafico.

Consiglio: agli MSP che utilizzano più piattaforme di cybersecurity consigliamo di esplorare le opzioni di consolidamento e i risparmi in termini di costo totale di proprietà che deriverebbero dal gestire tutti gli strumenti di sicurezza da un'unica piattaforma.

Servizi MDR

Adozione dei servizi MDR

La richiesta di servizi di Managed Detection and Response (MDR) sta aumentando rapidamente, per via della natura sempre più complessa delle minacce informatiche, quanto degli strumenti e delle tecnologie necessari per fermarle. I dati pubblicati recentemente da Gartner indicano un valore di mercato totale pari a 7,5 miliardi di $, nonché un Tasso di crescita annuale composto del 25,8%.

Con questi livelli di richiesta e crescita, non sorprende il fatto che la maggior parte (81%) degli MSP offra già opzioni di MDR, mentre gran parte degli altri MSP ha intenzione di aggiungere l'MDR ai servizi forniti ai propri clienti in un futuro molto prossimo. Tuttavia, dal sondaggio emerge una variazione notevole del livello di maturità in termini di adozione del servizio MDR nei quattro paesi analizzati.

Gli MSP negli Stati Uniti sono in cima alla classifica, con quasi tutti gli intervistati (94%) che dichiarano di offrire già un servizio MDR, rispetto al 70% in Germania, al 62% nel Regno Unito e al 58% in Australia. A livello globale, tra gli MSP che al momento non offrono MDR, quasi tutti i partecipanti al sondaggio hanno intenzione di aggiungere l'MDR ai servizi offerti nei prossimi anni, con quasi un terzo (32%) degli MSP nel Regno Unito che sostiene di avere in programma di aggiungere l'MDR nel 2024.

Offrono servizi MDR	**94%**	**62%**	**70%**	**58%**
Hanno intenzione di aggiungere l'MDR nel 2024	5%	32%	20%	18%
Hanno intenzione di aggiungere l'MDR nel 2025 o dopo	2%	6%	10%	22%

La tua organizzazione offre attualmente un servizio di Managed Detection and Response (MDR) ai clienti? n=350 (Stati Uniti: 200; Regno Unito: 50; Germania: 50; Australia: 50), alcune risposte sono state escluse.

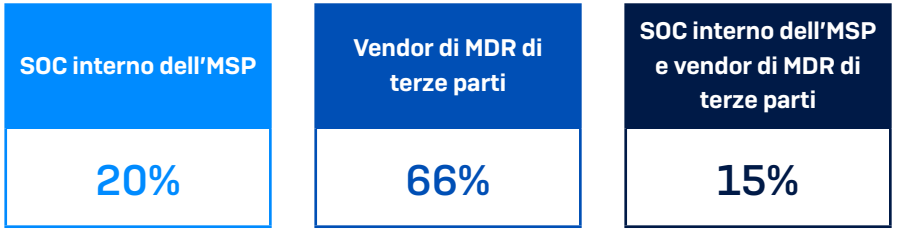
Erogazione di servizi MDR

Esistono tre principali modelli che gli MSP possono adottare per fornire servizi MDR: per mezzo del proprio Security Operations Center (SOC) interno, tramite vendor di terze parti, oppure attraverso una collaborazione tra il SOC dell'MSP e un vendor di terze parti.

Il sondaggio indica che il 66% degli intervistati si affida a un vendor di terze parti per fornire il proprio servizio MDR, il 20% utilizza il proprio SOC interno, mentre il 15% sfrutta la partnership con un vendor di terze parti che collabora con il proprio SOC. Complessivamente, l'80% (cifra arrotondata) degli MSP si affida, in misura variabile, a un vendor di terze parti per fornire il proprio servizio MDR.

Il 34% (cifra arrotondata) degli MSP ha un SOC interno che fornisce servizi MDR in maniera autonoma oppure in collaborazione con un vendor di terze parti. Le statistiche relative al provisioning interno sono straordinariamente omogenee tra le varie organizzazioni, con una differenza di appena il 4% tra la propensione più alta (37%, organizzazioni con 26-50 dipendenti) e più bassa (33%, tutte le altre organizzazioni) a utilizzare un SOC interno.

Metodo scelto per erogare i servizi MDR



Attualmente la tua organizzazione offre un servizio di Managed Detection and Response (MDR) ai clienti? n=282 intervistati che forniscono un servizio MDR. Alcune risposte sono state escluse.

Competenze richieste per i fornitori di MDR

Come abbiamo visto, quattro MSP su cinque utilizzano vendor di terze parti per fornire il proprio servizio MDR. Data la forte e crescente richiesta di servizi MDR, è fondamentale che gli MSP scelgano il giusto fornitore per i propri sistemi e per quelli dei clienti.

I fornitori di MDR svolgono la funzione di un'estensione del team dell'MSP, aggiungendo livelli di qualità e competenze che si riflettono direttamente sull'MSP. Inoltre, le opzioni offerte da un vendor di servizi MDR influiscono sulla quantità dei servizi che un MSP può fornire ai clienti, nonché sul livello di impegno che deve investire direttamente.

Poter usufruire di un servizio di Incident Response 24/7 è al primo posto tra le opzioni ritenute più importanti, con il 36% degli intervistati che sostiene che sia "essenziale", una percentuale che sale al 49% per gli MSP con 1-5 dipendenti. Con il 91% degli attacchi ransomware che hanno inizio al di fuori del normale orario lavorativo[1], poter contare su una protezione attiva a ogni ora del giorno e della notte è fondamentale per garantire una protezione efficace a un'organizzazione. Collaborando con un fornitore di servizi MDR che offre monitoraggio completo 24/7, gli MSP possono avere la tranquillità di una protezione costante per i propri clienti, senza il peso di dover effettuare internamente questo livello di provisioning a cura di esperti.

Al secondo posto si trova la *capacità di rilevare le minacce che rischiano di prendere il controllo di un account in Microsoft 365 e/o Google Workspace*, con un terzo (33%) degli MSP che la ritiene un requisito "essenziale", e con il 43% che la considera "molto importante".

Anche la *possibilità di ottenere dal fornitore di MDR ulteriori strumenti di sicurezza (in particolar modo firewall o strumenti di protezione della rete e degli endpoint)* è molto richiesta, con tre quarti dei partecipanti al sondaggio che la ritiene "essenziale" oppure "molto importante". Poter collaborare con un unico fornitore di strumenti di cybersecurity e servizi MDR riduce i costi di amministrazione e semplifica le operazioni.

Allo stesso tempo, lo studio indica chiaramente che gli MSP hanno bisogno di flessibilità e non vogliono avere restrizioni in termini di strumenti che possono utilizzare. Inoltre, non vogliono essere costretti ad acquistare strumenti di cybersecurity dal proprio fornitore di MDR. Il 71% degli intervistati sostiene che sia "essenziale" o "molto importante" che il vendor sia in grado di *utilizzare i dati di telemetria generati dagli strumenti di sicurezza già in proprio possesso, per il rilevamento e la risposta alle minacce.*

La capacità di offrire un servizio di Incident Response operativo 24/7 è il requisito N°1 per un vendor di MDR

OPZIONE	"ESSENZIALE"	"ESSENZIALE" O "MOLTO IMPORTANTE"
Servizio di**Incident Response 24/7**	36%	74%
Capacità di rilevare le minacce che rischiano di prendere il controllo di un account in **Microsoft 365 e/o Google Workspace**	33%	77%
Possibilità di ottenere **firewall/ protezione della rete** dal fornitore di MDR	31%	74%
Possibilità di ottenere protezione endpoint next-gen **dal fornitore di MDR**	28%	75%
Un'unica console per MDR e altre soluzioni di sicurezza	28%	74%
Garanzia in caso di violazioni	26%	70%
Capacità di utilizzare i dati di telemetria generati dagli **strumenti di sicurezza già in proprio possesso** per il rilevamento e la risposta alle minacce	25%	71%

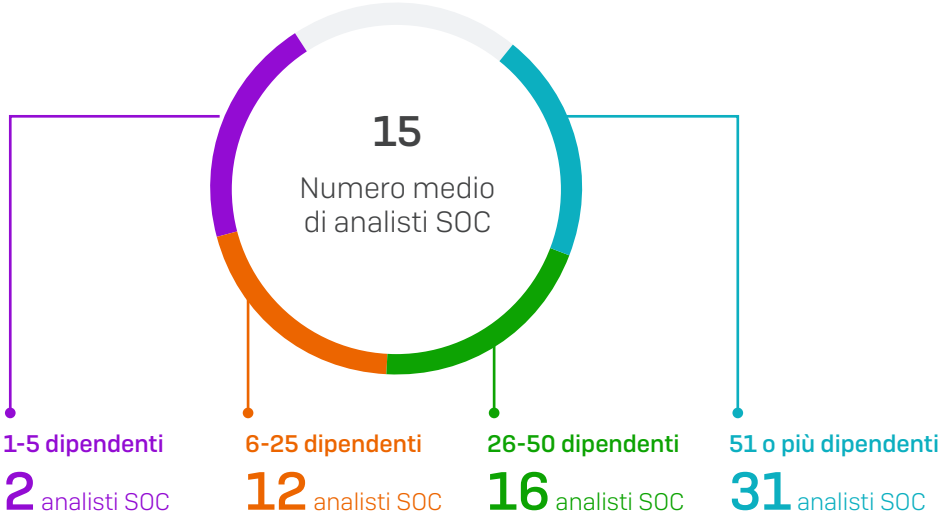
Se la tua organizzazione deve selezionare un fornitore di servizi MDR, quanto è importante che il fornitore di MDR offra le seguenti opzioni? n=350 (Stati Uniti: 200; Regno Unito: 50; Germania: 50; Australia: 50), alcune risposte sono state escluse.

Analisti SOC interni

Il 34% degli MSP che forniscono un servizio MDR ha un SOC, uno scenario che richiede un team interno di analisti specializzati. Dalla ricerca è emerso che, tipicamente, un SOC di un MSP include in media 15 analisti. Tuttavia, questa cifra nasconde una variazione notevole a seconda delle dimensioni dell'organizzazione.

Gli MSP con 1-5 dipendenti hanno, in media, due analisti dedicati al monitoraggio degli ambienti dei clienti e alla risposta alle minacce. La quantità di analisti aumenta in maniera costante in base alle dimensioni dell'organizzazione, con gli MSP di dimensioni più grandi che dichiarano di avere in media 31 analisti SOC. Nota: il numero di partecipanti in ogni fascia individuale è basso, per cui i risultati vanno considerati indicativi, piuttosto che significativi dal punto di vista statistico.

Poiché i cybercriminali decidono deliberatamente di sferrare i loro attacchi di notte, durante il fine settimana e nei giorni festivi, il monitoraggio dei sistemi 24/7 è fondamentale per poter offrire un servizio MDR efficace. Per gli MSP con un numero minore di analisti SOC, poter contare solo sul personale interno può mettere molta pressione su risorse umane già limitate.



Considerando il SOC della tua organizzazione, quanti analisti interni si occupano del monitoraggio e della risposta a eventi sospetti negli ambienti dei clienti?

Consiglio: per gli MSP che al momento non offrono servizi MDR potrebbe essere utile considerarne l'aggiunta alla propria gamma di servizi il prima possibile, per evitare di rimanere indietro rispetto alla concorrenza. Durante il processo di selezione di un vendor di servizi MDR di terze parti, è importante identificare le opzioni che sono importanti per la tua organizzazione e valutare la capacità dei fornitori di mantenere le promesse fatte.

Sfide e rischi informatici

Le principali sfide affrontate dagli MSP al giorno d'oggi

Il mondo degli MSP è caratterizzato da cambiamenti costanti. Le minacce continuano a evolversi, causando un aumento delle innovazioni e dei progressi introdotti nei controlli di sicurezza e richiesti dai clienti.

Dal sondaggio è emerso che ***tenere il passo con le più recenti soluzioni/tecnologie di cybersecurity*** è la principale sfida affrontata dagli MSP al giorno d'oggi. Viene infatti indicata sia come singola sfida principale, sia come una delle principali tre sfide.

Data la rapidità con cui vengono introdotte innovazioni in questo ambito, non sorprende che molti MSP facciano a fatica a tenere il passo. Man mano che le minacce si evolvono, i controlli informatici che devono fermarle diventano sempre più complessi. Le tecnologie esistenti acquisiscono nuove capacità e allo stesso tempo nuovi prodotti vengono costantemente immessi sul mercato. Tenere il passo con tutti questi sviluppi non è solo difficile, ma comporta anche un notevole investimento di tempo.

La difficoltà riscontrata nel trovare una quantità adeguata di analisti di cybersecurity con le giuste competenze è la seconda sfida principale affrontata attualmente dagli MSP:

- *La copertura fuori orario ufficio (incluso di notte e al fine settimana)* è la 2ª singola sfida principale per gli MSP
- *L'aggiunta al proprio team di nuovi analisti di cybersecurity per riflettere la propria crescita* è la 2ª delle principali tre sfide

La disponibilità di analisti di cybersecurity specializzati è limitata e implica salari molto alti. A esacerbare ulteriormente il problema c'è anche il fatto che una copertura 24/7 richiede come minimo 5-6 analisti, il che non è fattibile per molti MSP.

Singola sfida principale

N°1	Tenere il passo con le più recenti soluzioni/tecnologie di cybersecurity
N°2	Copertura fuori orario ufficio (incluso di notte e al fine settimana)
N°3	Acquisizione di nuovi clienti

Principali tre sfide

N°1	Tenere il passo con le più recenti soluzioni/tecnologie di cybersecurity
N°2	Aggiunta al proprio team di nuovi analisti di cybersecurity parallelamente alla propria crescita
N°3	Tenere il passo con le nuove minacce informatiche

Considerando la tua organizzazione, quali sono le principali sfide che affronta ogni giorno? Ti preghiamo di classificare le prime tre. n=350

Rischi informatici

Il sondaggio ha esplorato quali sono i principali rischi informatici percepiti dagli MSP nei confronti della propria organizzazione e dei suoi clienti. I risultati rivelano sia punti in comune che differenze.

Due risposte occupano i primi posti delle classifiche sia per quanto riguarda i rischi percepiti per gli MSP che per i loro clienti:

- Credenziali e dati di accesso rubati
- Carenza di personale interno con capacità/competenze di cybersecurity adeguate

Gli attaccanti non usano metodi indiretti, ma accedono con credenziali legittime. Servendosi di dati e credenziali di accesso rubati, spesso acquistati sul dark web da un broker di accesso iniziale (IAB), i criminali assumono l'identità di dipendenti legittimi per penetrare nei sistemi delle loro vittime. Come dimostrato nel report Sophos La Vera Storia Del Ransomware 2024, il 29% degli attacchi ransomware verificatisi l'anno scorso ha avuto inizio con la compromissione delle credenziali di un utente, una percentuale che indica quanto sia grave il problema.

MSP

Singolo rischio principale		Principali tre rischi	
N°1=	Carenza di personale interno con capacità/competenze di cybersecurity adeguate	N°1	Credenziali e dati di accesso rubati
N°1=	Reti wireless non sicure	N°2	Errori di configurazione negli strumenti di sicurezza
N°3	Mancanza di strumenti di cybersecurity	N°3	Reti wireless non sicure

Clienti degli MSP

Singolo rischio principale		Principali tre rischi	
N°1	Carenza di personale interno con capacità/competenze di cybersecurity adeguate	N°1	Credenziali e dati di accesso rubati
N°2	Vulnerabilità senza patch	N°2	Mancanza di strumenti di cybersecurity
N°3	Strumenti di accesso remoto	N°3	Vulnerabilità senza patch

Chi o quali consideri siano i principali rischi di cybersecurity per la tua organizzazione/per i clienti della tua organizzazione? n=350

Nonostante i continui progressi in ambito di tecnologie di cybersecurity e intelligenza artificiale, l'intervento umano rimane un fattore cruciale per una cybersecurity efficace. C'è infatti bisogno di professionisti specializzati, in grado di configurare, distribuire, gestire, rispondere e aggiornare le soluzioni tecnologiche. E le tecnologie, da sole, non sono in grado di bloccare automaticamente tutte le minacce informatiche. La carenza di personale tecnico specializzato è un fatto noto, e le organizzazioni tendono sempre maggiormente ad affidarsi agli MSP per colmare le proprie lacune, il che complica ulteriormente la sfida.

Mentre i principali rischi percepiti sono identici sia per quanto riguarda gli MSP che per i loro clienti, osservando gli altri risultati emergono alcune differenze di valutazione.

Le *reti wireless non sicure* sono uno dei principali rischi percepiti dagli MSP per la propria organizzazione (1° posto a pari merito come "singolo rischio principale" e 3° posto nei "principali tre rischi"). L'uso di reti wireless non sicure può implicare diversi pericoli, inclusa l'intercettazione dei dati e il loro utilizzo per estrarre informazioni sull'accesso e sulle password, che possono permettere ai cybercriminali di accedere ad account personali e aziendali.

Anche *gli errori di configurazione negli strumenti di sicurezza* sono uno dei principali rischi percepiti per gli MSP. Firewall, protezione endpoint e altri strumenti sono efficaci solo se configurati correttamente.

Le *vulnerabilità a cui non sono state applicate patch* costituiscono uno dei principali rischi percepiti dagli MSP per i propri clienti (2° "singolo rischio principale" e 3° fra i "principali tre rischi"). Con il 32% degli attacchi ransomware che, l'anno scorso, hanno avuto inizio per via dell'exploit di una vulnerabilità a cui non erano state applicate patch, gli MSP fanno bene a considerare questo fattore come uno dei pericoli principali che minacciano i loro clienti.

Consiglio: per ridurre la quantità di vendor e i costi di gestione quotidiana di fronte a questa ampia varietà di sfide e rischi, per gli MSP potrebbe essere utile cercare partner di cybersecurity in grado di offrire una gamma completa di servizi e strumenti. Inoltre, la gestione può essere semplificata implementando soluzioni che includano una protezione efficace e adattiva contro le minacce in continua evoluzione, senza bisogno di configurazioni e distribuzioni complesse. Agli MSP consigliamo anche di sfruttare i servizi dei fornitori di MDR per ampliare ed estendere le competenze e l'esperienza dei propri team di cybersecurity interni, affidandosi a partner in grado di offrire il giusto sostegno per il loro business model e che possano adattarsi alle loro esigenze, man mano che cambiano e si evolvono.

Impatto delle assicurazioni informatiche

L'uso di una cyberassicurazione come strategia per trasferire il rischio informatico ha subito un aumento costante, con il 90% delle organizzazioni di medie dimensioni che gode di una copertura assicurativa, secondo i dati emersi dalla ricerca condotta da Sophos. Il 50% delle organizzazioni ha stipulato una polizza cyberassicurativa indipendente, mentre il 40% possiede una copertura aziendale più completa che include l'ambito informatico, ad es. come parte di una polizza di responsabilità civile generale.

La decisione sempre più diffusa di stipulare un'assicurazione informatica ha causato un aumento dei livelli di engagement del canale, con il 99% degli MSP che segnalano un incremento delle richieste di supporto e soluzioni in grado di soddisfare i requisiti delle cyberassicurazioni.

A livello globale, la richiesta più comune dei clienti (47%) è un servizio MDR che sia in grado di migliorarne la posizione assicurativa, seguita a distanza ravvicinata dal bisogno di assistenza per le richieste di indennizzo assicurativo (45%). Entrambe queste esigenze offrono ottime opportunità di guadagno per gli MSP, in termini di fatturazione per l'erogazione di MDR e di servizi professionali.

ESIGENZA DEL CLIENTE	GLOBALE				
MDR per migliorare l'assicurabilità	**47%**	49%	38%	56%	36%
Assistenza con le **richieste di indennizzo assicurativo**	**45%**	49%	46%	30%	42%
EDR per migliorare l'assicurabilità	**34%**	31%	32%	28%	52%
Tecnologie e servizi non EDR/MDR per migliorare l'assicurabilità	**33%**	31%	22%	48%	40%

La tua organizzazione ha riscontrato un aumento nell'esigenza di supporto e di soluzioni in grado di soddisfare i requisiti di cybersecurity dei clienti? n=350 (Stati Uniti: 200; Regno Unito: 50; Germania: 50; Australia: 50).

Un terzo (34%) degli MSP indica di aver ricevuto richieste da clienti che desiderano aggiungere Endpoint Detection and Response (EDR) allo stack di sicurezza, per migliorare la propria assicurabilità. È interessante sottolineare che, ad eccezione dell'Australia, la richiesta di MDR per motivi assicurativi è significativamente più alta rispetto alla richiesta di EDR, il che riflette come la presenza di un servizio MDR specializzato e operativo 24/7 possa offrire una maggiore riduzione del rischio rispetto a un team interno già oberato di lavoro.

Un terzo (33%) degli intervistati ha dichiarato di aver notato una maggiore richiesta di tecnologie e servizi non EDR/MDR da parte di clienti che desiderano migliorare la propria assicurabilità. Sebbene lo studio non abbia approfondito questo aspetto, è probabile che i requisiti includessero strumenti di autenticazione a più fattori (Multi-Factor Authentication, MFA) e di protezione per e-mail/rete: tutti componenti necessari/desiderati dalle compagnie di assicurazioni.

Consiglio: l'offerta di servizi e tecnologie in grado di migliorare l'assicurabilità dei clienti è un'ottima opportunità per gli MSP e consigliamo alle organizzazioni di potenziare il supporto fornito in questi ambiti, per sfruttare la possibilità di incrementare il fatturato.

Conclusione

Di fronte all'inevitabilità degli attacchi informatici, gli MSP hanno molte opportunità per far crescere l'azienda e incrementare la redditività. Dalla possibilità di ridurre i costi quotidiani con il consolidamento delle piattaforme di gestione, fino all'ottimizzazione delle interazioni con vendor di MDR di terze parti per ampliare i servizi offerti, e all'allineamento delle proprie attività con le esigenze cyber-assicurative dei clienti, gli MSP possono far crescere la propria azienda e allo stesso tempo elevare la protezione dei clienti contro il ransomware e i rischi di violazione.

Il mercato degli MSP può essere un ambiente competitivo. Utilizzare queste informazioni per accelerare la crescita, gli MSP possono sfruttare il pieno potenziale di tutte le opportunità che si presenteranno in futuro.

Programma Sophos MSP

Sophos aiuta gli MSP a far crescere l'azienda e incrementare la redditività. Grazie a difese innovative e adattive, nonché a un sistema completo di cybersecurity per MSP, offre tutte le certezze informatiche necessarie per concretizzare il successo.

- Con una linea completa di servizi e prodotti di cybersecurity a portata di un tocco, potrai soddisfare le esigenze attuali e future dei tuoi clienti
- Riduci i costi legati alla gestione delle attività quotidiane e libera più ore fatturabili con la piattaforma di sicurezza Sophos Central, che ti permette di gestire tutti i sistemi di sicurezza dei tuoi clienti da un'unica console
- Iscriviti al Programma Sophos MSP per ottenere margini estremamente vantaggiosi, ottimi incentivi e opzioni di fatturazione aggregata

1 Active Adversary Report for Business Leaders, Sophos, 2023

Per scoprire di più sul programma Sophos MSP, visita sophos.com/MSP e per esplorare Sophos MDR, visita sophos.com/MDR

Sophos MDR: con Incident Response 24/7 inclusa come standard

Sophos MDR è il servizio di rilevamento e risposta gestito più affidabile al mondo, che supera qualsiasi altro vendor in termini di adozione da parte delle organizzazioni. Con il rilevamento 24/7 e la risposta con intervento umano diretto inclusi come componenti standard, gli MSP e i loro clienti avranno la tranquillità di una protezione a qualsiasi ora del giorno e della notte, fornita dagli esperti Sophos. Le caratteristiche principali includono:

- Correzione 24/7 con intervento umano
- Incident Response completa
- Supporto diretto e dedicato 24/7
- Contatto dedicato per la risposta agli incidenti
- Scelta delle modalità di risposta
- Garanzia in caso di violazioni
- Threat hunting proattivo
- Compatibilità con la protezione endpoint Sophos e non Sophos
- Rilevamento delle minacce che rischiano di prendere il controllo di un account in Microsoft 365 e Google Workspace
- E molte altre ancora.

Sia che tu stia cercando un servizio completamente in outsourcing o un'estensione flessibile del tuo SOC interno, Sophos MDR può aiutarti a far crescere la tua azienda.

"Sophos MDR ha salvato molti clienti da conseguenze potenzialmente catastrofiche per la loro azienda. I nostri margini sono aumentati del 100%, con un fatturato che ha raggiunto un incremento del 300%."

James Wagner, Presidente, The ITeam

2024-05-21 (WP-NP)

SOPHOS