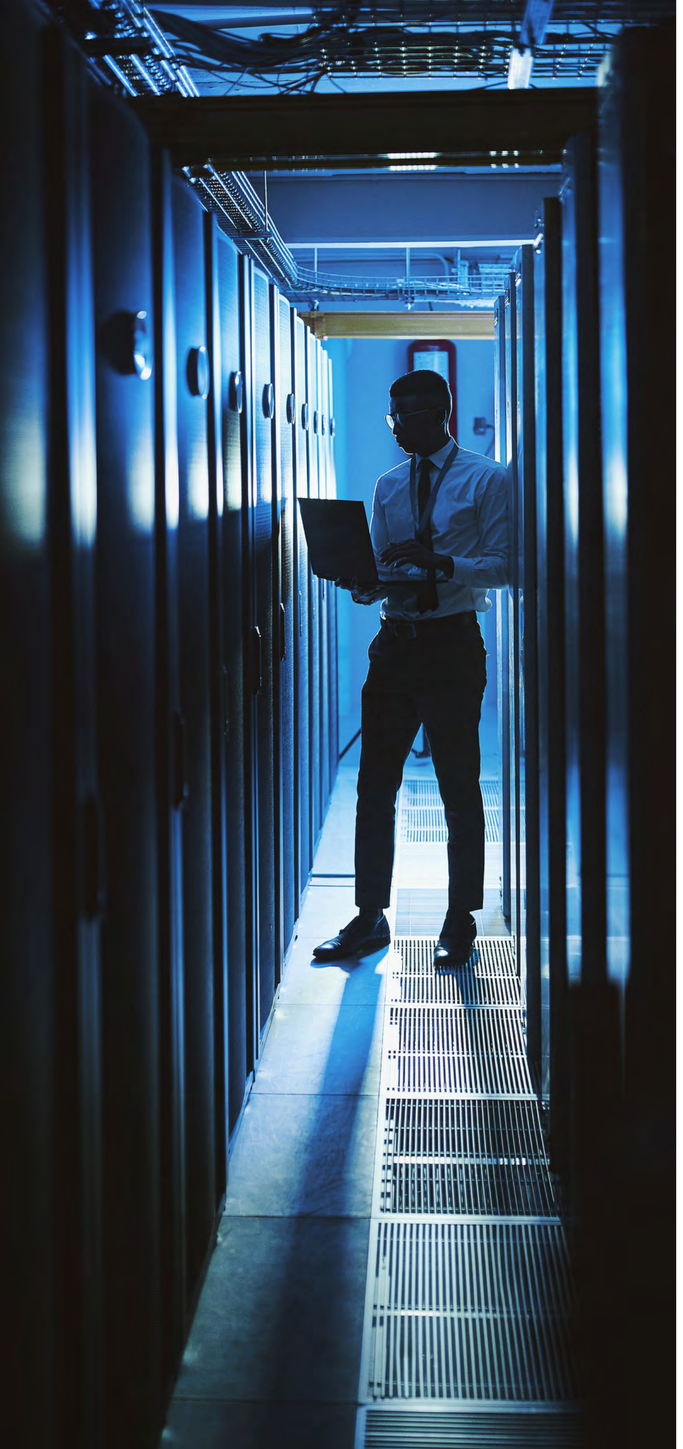
Enterprise Strategy Group | Getting to the bigger truth.™

Cosa si aspettano i team addetti alla sicurezza dai fornitori MDR

Dave Gruber, Principal Analyst

SETTEMBRE 2022



Obiettivi della ricerca

L'utilizzo dei servizi MDR (Managed Detection and Response, di rilevamento e risposta gestiti) è diventato una strategia molto diffusa nei programmi di sicurezza moderni. Tuttavia, le organizzazioni IT non devono lasciarsi ingannare dal nome: infatti, i fornitori di servizi MDR offrono molto di più dei servizi di rilevamento e risposta di base, poiché aiutano i responsabili IT e della sicurezza ad accelerare lo sviluppo dei programmi e a migliorare il profilo di sicurezza. Con la prolungata carenza delle competenze richieste nell'ambito della sicurezza informatica, i servizi MDR riescono a portare immediatamente online risorse esperte insieme a processi e strumenti all'avanguardia di efficacia comprovata, in grado di aiutare i team addetti alla sicurezza a prendere il controllo e prepararsi al futuro successo del proprio programma.

Per comprendere queste tendenze e valutare lo stato generale dell'attuale offerta di servizi di rilevamento e risposta gestiti, ESG ha intervistato 373 professionisti della sicurezza, che si occupano in prima persona di tecnologie per la sicurezza informatica, inclusi i relativi prodotti, servizi e processi.

OBIETTIVI DELLO STUDIO:

Determinare come, dove e perché i servizi MDR vengono utilizzati a supporto dei programmi di sicurezza.

Ottenere informazioni rilevanti sui fattori che contano di più per le operazioni IT, i dirigenti della linea aziendale e gli utenti finali.

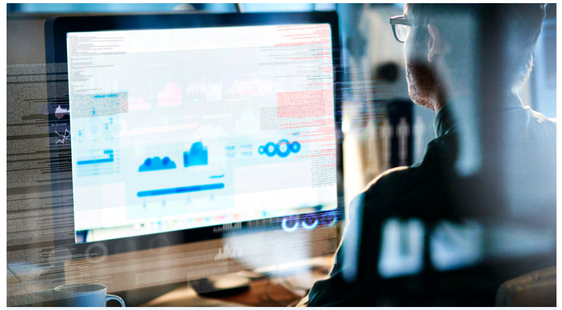
Isolare gli specifici casi d'uso dei servizi MDR e i profili delle organizzazioni che se ne avvalgono.

Stabilire quali macro tendenze del settore influiscono sulla selezione dei fornitori di servizi MDR.

TORNA AL SOMMARIO

RISULTATI PRINCIPALI

FAI CLIC PER MAGGIORI INFORMAZIONI



I tre fattori chiave che determinano l'impegno iniziale MDR

Le organizzazioni sono motivate da valutazioni proattive, lacune operative e dal coinvolgimento IR.

Diversi casi d'uso sono supportati dai servizi MDR

Un coinvolgimento che dura nel tempo è determinato da molti fattori tra cui la presenza di esperti, la Threat Intelligence, l'acquisizione delle competenze, la copertura, lo sviluppo dei programmi e molti altri.

I servizi MDR promuovono buoni risultati di sicurezza

Le organizzazioni riscontrano una maturità avanzata, un minor numero di attacchi riusciti, migliori competenze informatiche e una maggiore fiducia da parte dei dirigenti.

È previsto uno stack tecnologico aperto, ma i servizi MDR devono offrire tutti i meccanismi

Ci si aspetta che i fornitori di servizi dispongano di uno stack tecnologico completo, se necessario, ma per ottimizzare i risultati, questi strumenti devono poter essere integrati con l'infrastruttura esistente.

I modelli di impegno dei clienti MDR contano

A fronte della variazione dei modelli, è possibile costruire un rapporto di fiducia attraverso comunicazioni regolari e incentrate sulla persona.

Le macro tendenze del settore influiscono sulla selezione dei servizi MDR

Il movimento XDR (Extended Detection and Response, risposta e rilevamento estesi), il supporto del framework MITRE ATT&CK e la modernizzazione del SOC sono di fondamentale importanza.

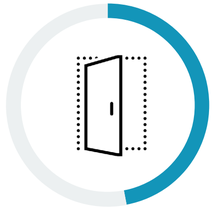
I tre fattori chiave che promuovono l'impegno iniziale dei fornitori di servizi MDR

Le valutazioni proattive generano con maggiore probabilità il primo coinvolgimento dei fornitori di servizi MDR

Cosa spinge i team addetti all'IT e alla sicurezza a rivolgersi a un fornitore di servizi di rilevamento e risposta gestiti? Se pensiamo ai servizi MDR in senso stretto, la prima risposta che ci viene in mente riguarda le lacune nelle competenze sulle operazioni di sicurezza, nella copertura o nei processi. Tuttavia, è emerso che più della metà (57%) delle organizzazioni ha dichiarato che le valutazioni proattive della sicurezza sono state un fattore che ha spinto a rivolgersi per la prima volta a un fornitore di servizi MDR. Non a caso, l'impegno con i fornitori MDR inizia spesso con le valutazioni della sicurezza, tra cui quelle relative alle vulnerabilità, che possono far emergere i punti deboli del profilo di sicurezza, in termini di programmi, strumenti, copertura e competenze. Il terzo fattore determinante è la risposta a crisi/incidenti che mette in evidenza le lacune nel programma di sicurezza. Anche le esigenze operative, come la risposta agli incidenti, sono spesso fattori trainanti che determinano il coinvolgimento di fornitori di servizi MDR.

Fattori che hanno determinato il coinvolgimento iniziale con i fornitori di servizi MDR.

57%
Valutazioni della sicurezza

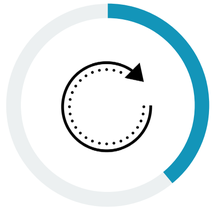


47%
Valutazione e gestione delle vulnerabilità

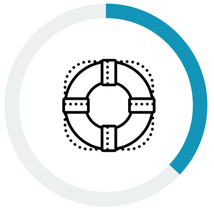
46%
Servizi di Threat Intelligence

39%
Risposta/mitigazione degli incidenti

39%
Rilevamento degli incidenti



39%
Correzione/ripristino dagli incidenti



37%
Risposta a violazioni o a incidenti di grandi dimensioni

36%
Risposta agli incidenti di crisi/violazioni che rivelano lacune nel nostro programma

34%
Analisi degli incidenti

33%
Valutazione e assegnazione di priorità agli avvisi quotidiani

30%
Rilevazione delle minacce informatiche

25%
Red teaming e simulazione di violazioni e attacchi

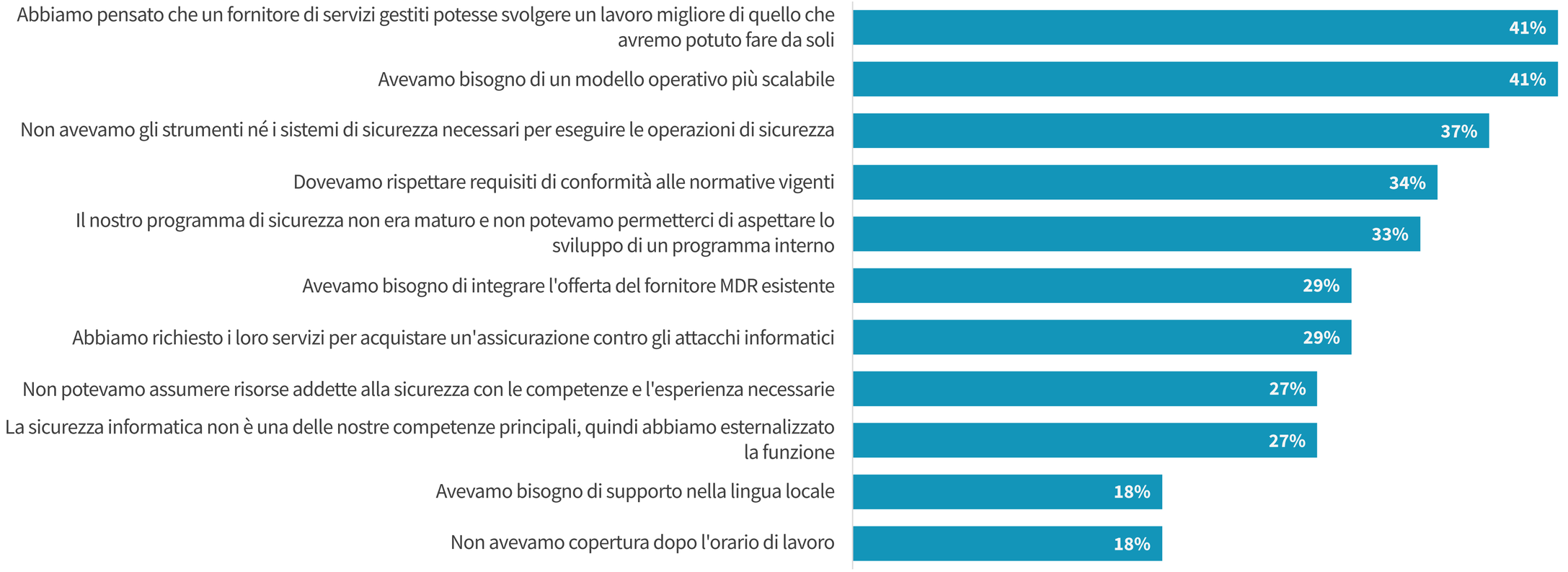
TORNA AL SOMMARIO

Fattori determinanti per l'attuale coinvolgimento con i servizi MDR

Poiché i team addetti alla sicurezza hanno difficoltà ad adeguare i loro programmi per rispondere all'ampliamento della superficie di attacco e alla complessità e all'espansione del panorama delle minacce, molte organizzazioni si rivolgono ai fornitori di servizi MDR per adattare i propri modelli operativi e accelerarne lo sviluppo. Per le organizzazioni, i servizi MDR rappresentano un modo per velocizzare lo sviluppo dei programmi e colmare le lacune esistenti. Oltre quattro organizzazioni su dieci ritengono che i fornitori di servizi MDR possano semplicemente svolgere un lavoro migliore di quello che farebbero le risorse interne. Un terzo segnala programmi di sicurezza poco maturi e la mancanza degli strumenti e dei sistemi necessari. Altri fattori importanti includono, inoltre, un elenco sempre più lungo di procedure e controlli di sicurezza necessari per assicurare la protezione dalle minacce informatiche, nonché i requisiti di conformità alle normative vigenti.

Per quanto riguarda la carenza di competenze e di copertura, sebbene le organizzazioni riconoscano le lacune, assegnano loro una priorità inferiore rispetto agli obiettivi generali di crescita e sviluppo dei programmi.

Fattori che motivano le organizzazioni a impegnarsi con gli attuali fornitori di servizi MDR.



Diversi casi d'uso sono **supportati dai servizi MDR**

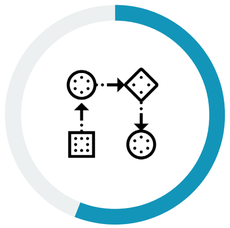
"Quasi la metà delle organizzazioni si avvale di un fornitore di servizi MDR **per esternalizzare completamente le operazioni di sicurezza."**

Casi d'uso chiave: Accesso a risorse competenti e sviluppo dei programmi di sicurezza

I fornitori di servizi MDR possono soddisfare diversi casi d'uso. Sebbene tra i fattori che compaiono in cima all'elenco vi siano l'accelerazione dello sviluppo del programma di sicurezza e l'accesso a risorse competenti in materia, quasi la metà delle organizzazioni si avvale di un fornitore di servizi MDR per esternalizzare completamente le operazioni di sicurezza. L'altra metà utilizza i servizi MDR per integrare il programma interno, colmare le lacune di copertura, accedere a ulteriori strumenti di Threat Intelligence e aggiungere funzionalità di rilevamento delle minacce. Va anche notato che quasi la metà delle organizzazioni esternalizza completamente le operazioni di sicurezza oppure vorrebbe farlo.

Casi d'uso dei servizi MDR nell'ambito dei programmi di sicurezza delle organizzazioni.

56%
Accesso a risorse esperte di sicurezza

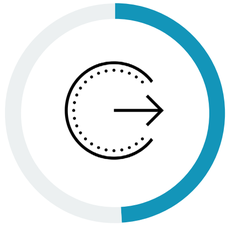


56%
Sviluppo del programma di sicurezza

54%
Integrazione del programma interno per le operazioni di sicurezza

50%
Copertura

50%
Threat Intelligence



49%
Outsourcing completo delle operazioni di sicurezza

49%
Rilevamento proattivo delle minacce

TORNA AL SOMMARIO

Di solito il coinvolgimento dei fornitori di servizi MDR aumenta nel tempo

Il coinvolgimento dei fornitori di servizi MDR, in genere, aumenta nel corso tempo: vengono aggiunti nuovi servizi per rafforzare l'analisi degli incidenti, la mitigazione e la risposta per tutti i tipi di situazioni, da un evento di grave crisi/violazione alle attività di risposta quotidiane. I servizi offerti dai moderni fornitori MDR superano le tradizionali funzionalità reattive delle SecOps, poiché sono proattivi e supportano la Threat Intelligence, il rilevamento delle minacce, le simulazioni degli attacchi, le verifiche della sicurezza e la gestione delle vulnerabilità. Esaminando questa ampia offerta, è evidente che i fornitori di servizi MDR offrono molto di più del rilevamento e della risposta di base e che stanno diventando partner a pieno titolo dei programmi di sicurezza, poiché possono aiutare le organizzazioni di qualsiasi dimensione ad adeguare i propri programmi.

Attività di sicurezza aggiunte dopo il coinvolgimento iniziale dei fornitori di servizi MDR.

"I fornitori di servizi MDR offrono **molto di più del rilevamento e della risposta di base.**"

TORNA AL SOMMARIO

Molto di più di rilevamento e risposta: i fornitori di servizi MDR sono diventati partner operativi e strategici a lungo termine

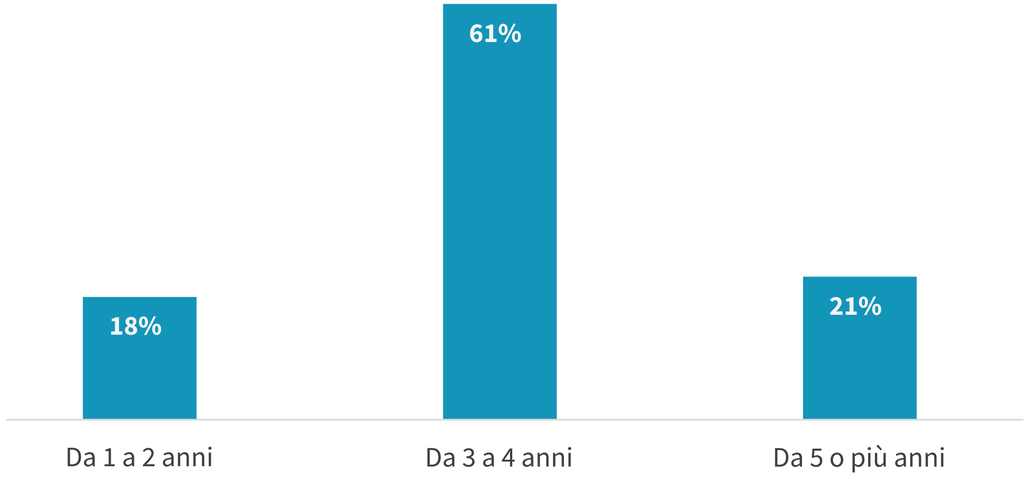
Con il prolungamento del coinvolgimento dei servizi MDR e con la conseguente crescita delle relazioni, i fornitori assumeranno un ruolo sempre più strategico. Questo è chiaramente dimostrato dal fatto che più di tre quarti (77%) delle organizzazioni descrive il proprio fornitore di servizi MDR come partner operativo strategico in termini di allineamento al proprio programma di sicurezza. Si tratta di relazioni durature, infatti l'82% delle organizzazioni ha dichiarato di avvalersi di un fornitore di servizi MDR da almeno tre anni, la maggior parte ne utilizza più di uno, mentre il 34% collabora con tre o più fornitori per supportare i casi d'uso e gli asset che costituiscono la propria superficie di attacco.

Come sono visti i fornitori di servizi MDR dalle organizzazioni per cui lavorano?

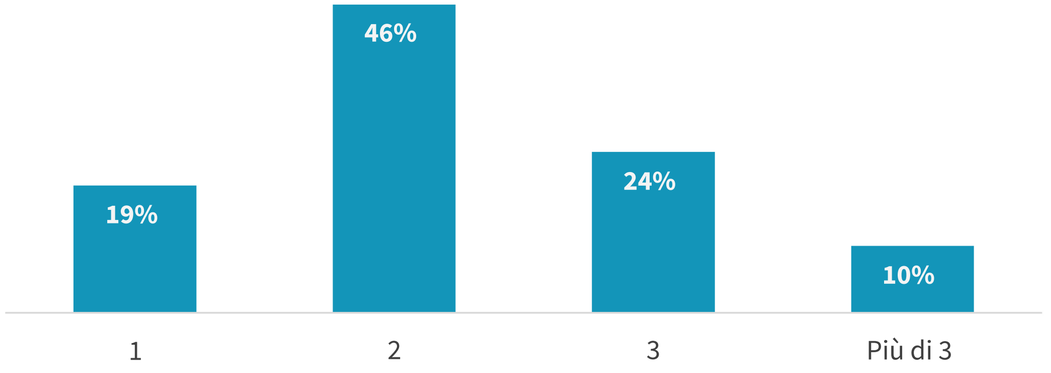
77%

Un partner operativo strategico **che ha migliorato il nostro programma di sicurezza complessivo**

Durata della collaborazione tra organizzazioni e un fornitore di servizi MDR.



Numero di fornitori di servizi MDR con cui collaborano le organizzazioni.



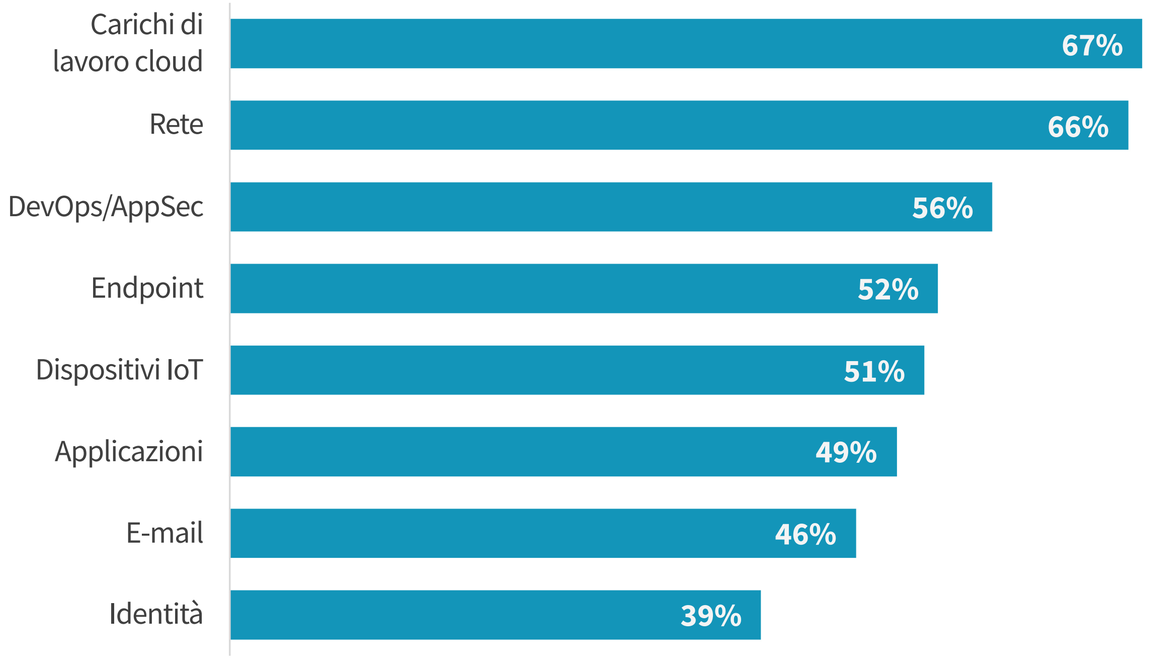
TORNA AL SOMMARIO

> Pochi coinvolgono i fornitori di servizi MDR **per coprire l'intera superficie di attacco."**

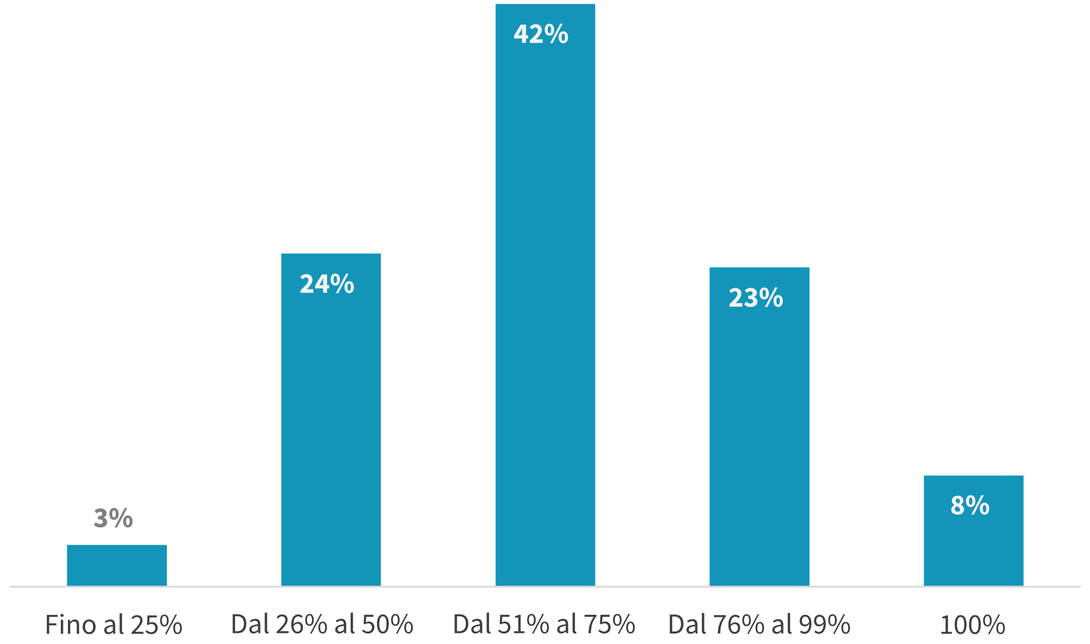
I fornitori di servizi MDR devono monitorare tutti i tipi di asset, ma raramente l'intero ambiente

Quando si tratta di copertura della superficie di attacco, la maggior parte delle organizzazioni si aspetta che i fornitori di servizi di MDR supportino le operazioni di sicurezza per tutti i tipi di asset IT. Tuttavia, pochi li coinvolgono per coprire l'intera superficie di attacco. Nello specifico, più di due terzi segnalano che il proprio fornitore di servizi MDR è responsabile di una copertura che non supera il 75% del proprio ambiente, mentre solo l'8% dichiara che il fornitore di servizi MDR offre una copertura del 100%.

Estensione della copertura offerta dagli attuali fornitori di servizi MDR alle organizzazioni.



Percentuale di superficie di attacco che rientra nella responsabilità dei fornitori di servizi MDR.



TORNA AL SOMMARIO


I servizi MDR
determinano
il raggiungimento
di buoni risultati in
termini di sicurezza

I fornitori di servizi MDR contribuiscono a migliorare le risorse on-site e la maturità del programma di sicurezza

Quando si tratta dei risultati effettivi raggiunti, i fornitori di servizi MDR aiutano le organizzazioni a ridurre il numero di attacchi riusciti, accelerare lo sviluppo complessivo del programma di sicurezza e avviare opportunità di investimento in iniziative di sicurezza più strategiche. In particolare, la metà afferma che il proprio fornitore di servizi MDR sta contribuendo a migliorare le competenze in materia di sicurezza delle proprie risorse interne e il 45% ha dichiarato aver investito in iniziative di sicurezza più strategiche. Più di quattro organizzazioni su dieci affermano di aver subito molti meno attacchi e/o di aver assistito a un miglioramento complessivo del programma di sicurezza. Dal punto di vista della linea aziendale, il 42% rileva un aumento della fiducia da parte dei dirigenti e/o del Consiglio di amministrazione, mentre il 38% afferma di riuscire a soddisfare gli obiettivi di conformità o i requisiti dell'assicurazione contro le minacce informatiche. A conferma di questi risultati di business positivi, è stato registrato un aumento significativo del numero di organizzazioni che hanno classificato la maturità dei propri programmi di sicurezza come elevata dopo aver coinvolto un fornitore di servizi MDR.

Risultati ottenuti utilizzando un fornitore di servizi MDR

50%
Competenze migliorate del personale addetto alla sicurezza grazie al fornitore di servizi MDR

45%
Investimenti in iniziative di sicurezza più strategiche

42%
Numero notevolmente inferiore di attacchi riusciti

42%
Miglioramento significativo del programma di sicurezza

42%
Aumento della fiducia dei dirigenti e/o del Consiglio di amministrazione

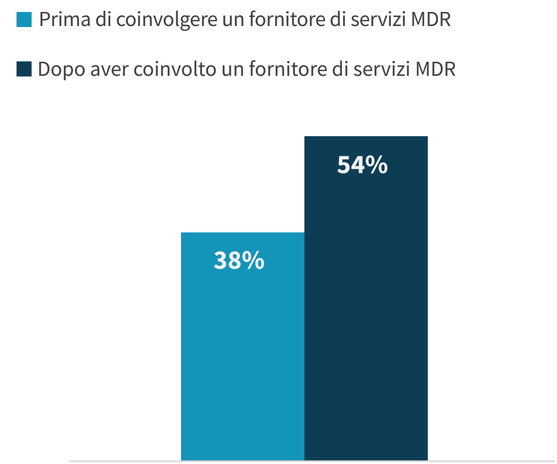
38%
Requisiti relativi a conformità/assicurazioni informatiche soddisfatti

38%
Riduzione dei costi operativi della sicurezza

35%
Riduzione della pressione sul team di sicurezza interno

32%
Riduzione delle spese per l'assicurazione informatica

Maturità del programma MDR.



Molto maturo: presenta processi formali, operazionalizzati, esperti nel personale, copertura completa e visibilità della superficie di attacco, profili di rischio, programma di risposta agli incidenti formale e testato, collaborazione IT, analisi e strumenti di sicurezza altamente efficaci, ecc.

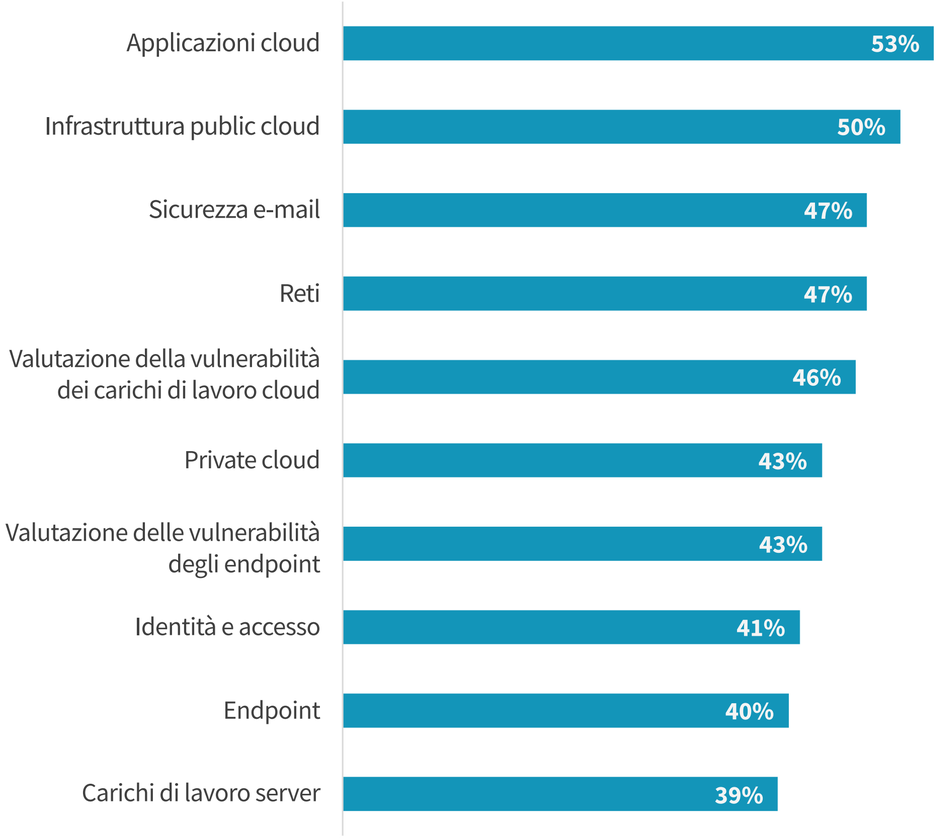
TORNA AL SOMMARIO

È previsto uno stack tecnologico aperto, **ma i servizi MDR devono offrire tutti i meccanismi**

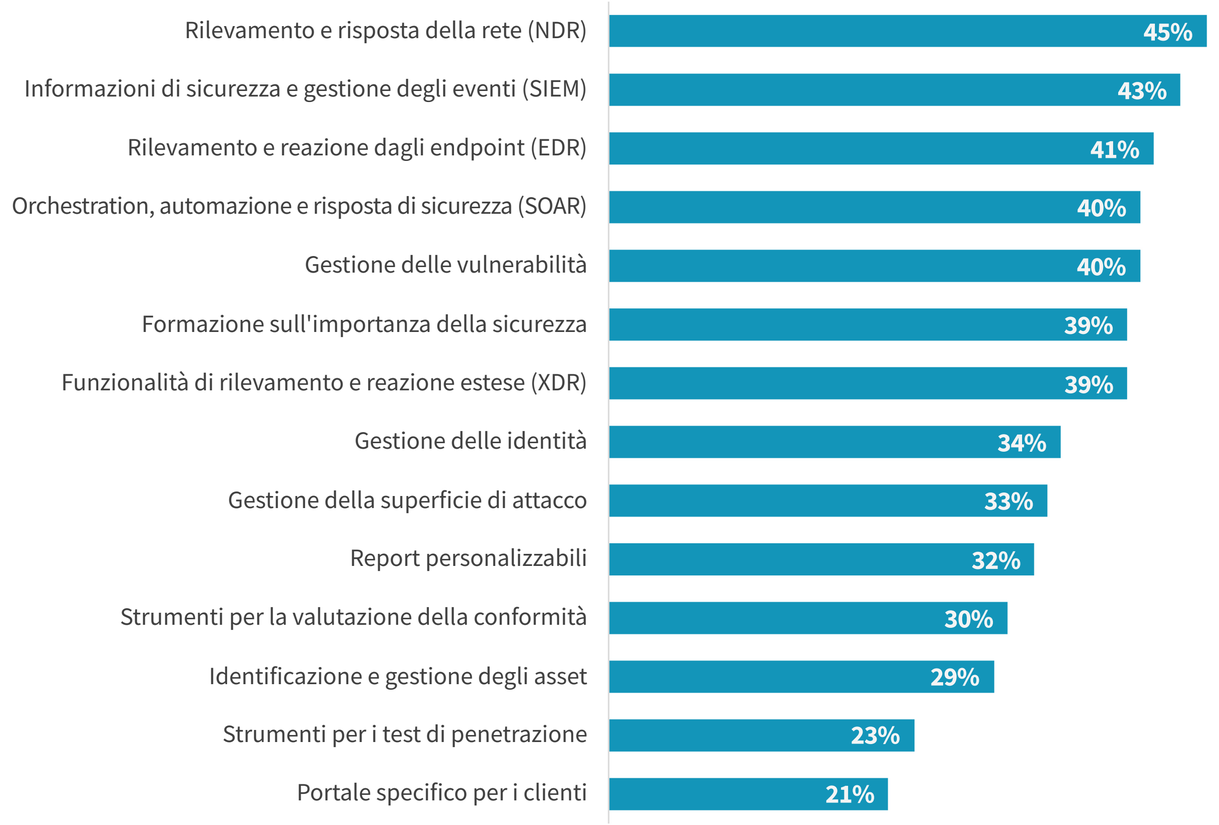
Il cloud e le operazioni di sicurezza sono i criteri tecnologici chiave per la selezione dei servizi MDR

I clienti MDR si aspettano che il proprio fornitore di servizi sia in grado di offrire una copertura di sicurezza completa da tutti i vettori di attacco. Inoltre, si aspettano che utilizzi i meccanismi di sicurezza già esistenti, che vanno da un set completo di controlli di sicurezza, inclusi endpoint, rete, cloud ed e-mail, a uno stack completo di strumenti per le operazioni di sicurezza, tra cui SIEM (Security Information and Event Managament, Informazioni di sicurezza e gestione degli eventi), SOAR (Security Orchestration, Automation and Response, Orchestrazione, automazione e risposta di sicurezza), EDR (Endpoint Detection and Response, Rilevamento e reazione dagli endpoint), NDR (Network Detection and Response, Rilevamento e risposta della rete), XDR (Extended Detection and Response, Funzionalità di rilevamento e reazione estese), gestione della superficie di attacco, rilevamento degli asset e gestione delle vulnerabilità.

Tecnologie di rilevamento/agent che le organizzazioni si aspettano da un fornitore MDR.



Tecnologie per le operazioni di sicurezza che le organizzazioni si aspettano da un fornitore MDR.



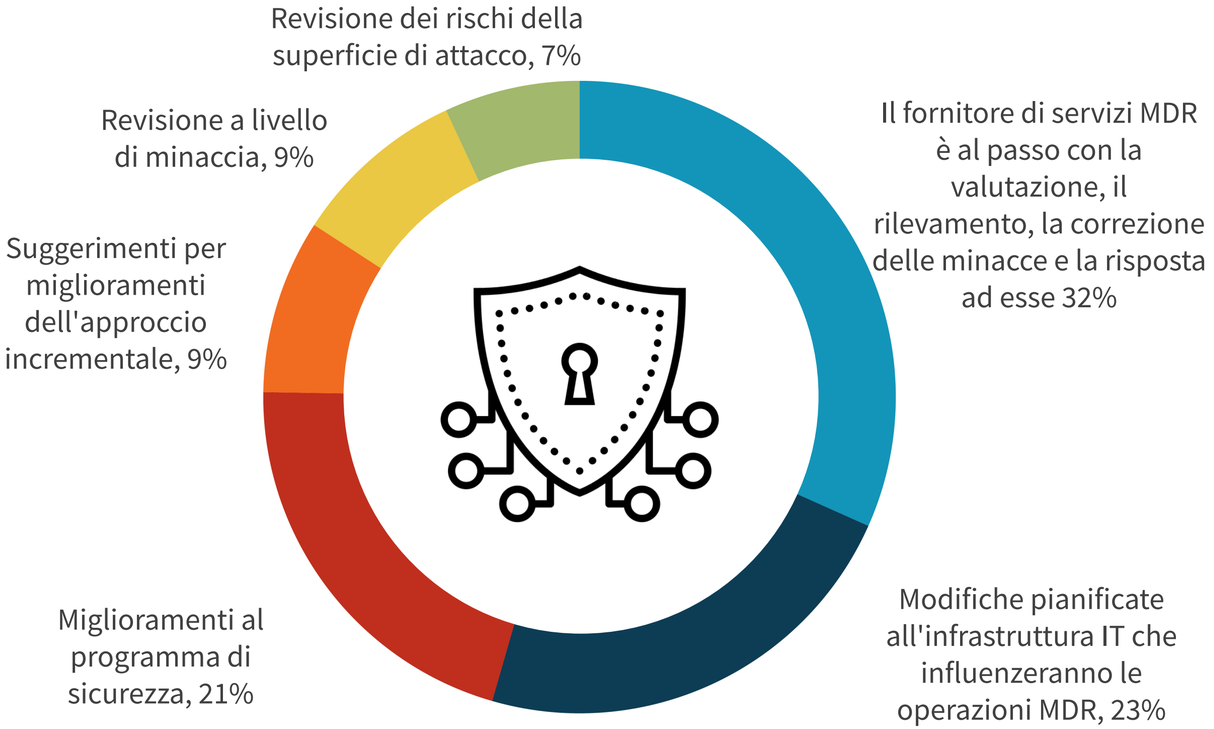
TORNA AL SOMMARIO

I modelli di impegno dei clienti MDR **contano**

Revisioni operative MDR: quali sono gli aspetti più importanti

I leader della sicurezza sottolineano che i modelli di coinvolgimento MDR contano molto e chiedono ai fornitori di servizi MDR non solo di stare al passo con il rilevamento delle valutazioni, la risposta e la correzione, ma anche di rimanere aggiornati sulle modifiche pianificate dell'infrastruttura IT, i continui miglioramenti del programma di sicurezza, la revisione dei rischi della superficie di attacco e del livello di minaccia, il tutto mentre continuano a suggerire azioni per un miglioramento incrementale del profilo di sicurezza. Sebbene queste aspettative siano alte, dimostrano perché la maggior parte delle organizzazioni considera il proprio fornitore di servizi MDR un partner strategico.

L'aspetto più importante delle revisioni operative svolte dai fornitori di servizi MDR.



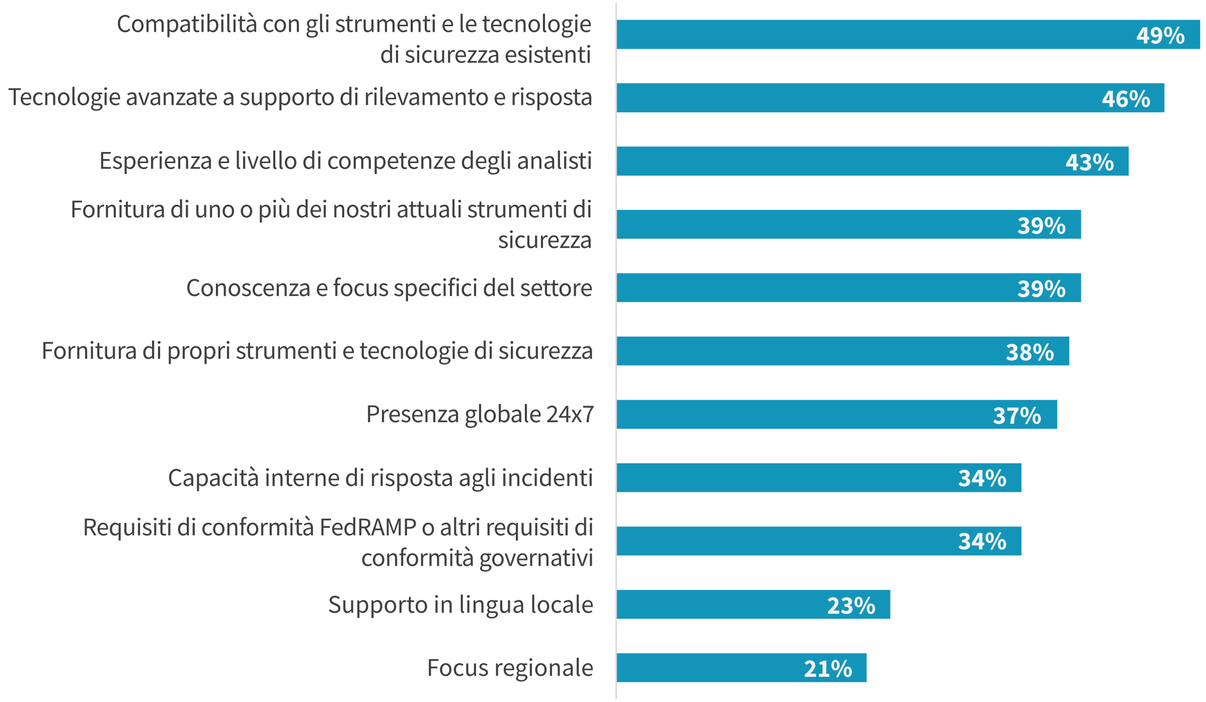
"I leader della sicurezza sottolineano che i **modelli di coinvolgimento MDR contano molto.**"

TORNA AL SOMMARIO

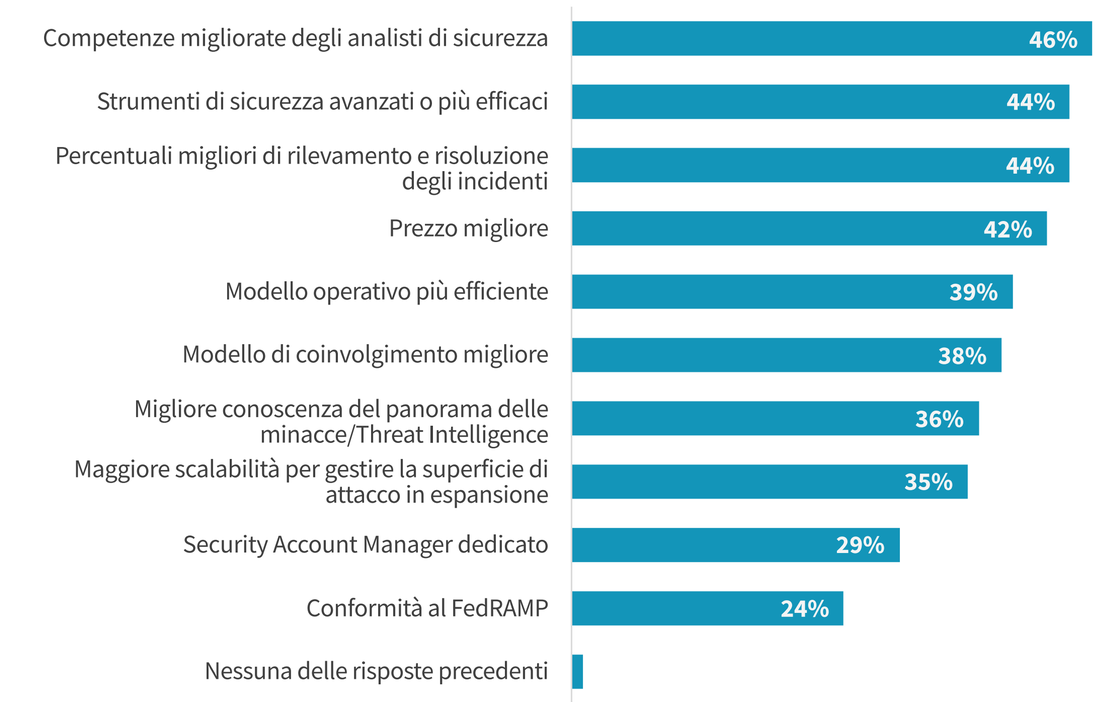
Le competenze e gli strumenti avanzati promuovono il cambiamento del fornitore di servizi MDR

Quali considerazioni sono importanti per le organizzazioni quando valutano e selezionano un fornitore di servizi MDR? Quasi la metà (49%) afferma di dover utilizzare l'ecosistema di strumenti e tecnologie di sicurezza esistente; mentre il 46% desidera funzionalità avanzate di rilevamento e risposta. Un altro 43% cerca un fornitore di servizi MDR che offra personale competente in materia di sicurezza. Questo aspetto è anche quello indicato più di frequente come cruciale per il passaggio a un nuovo fornitore di servizi. Altre motivazioni includono strumenti di sicurezza più avanzati e percentuali di rilevamento e risoluzione migliorate, anche se i prezzi e i modelli operativi rimangono fattori importanti.

Criteri importanti per la selezione dei fornitori di servizi MDR.



Fattori che porterebbero le organizzazioni a cambiare fornitori di servizi MDR.



TORNA AL SOMMARIO

Le macro tendenze del settore **influenzano la selezione dei fornitori MDR**

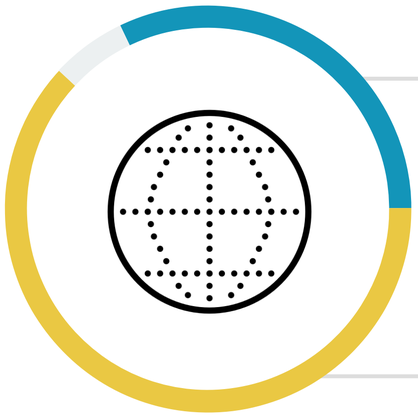
Più di nove organizzazioni su dieci

ritengono che il supporto di MITRE ATT&CK sia critico o molto importante.

Il supporto di MITRE e XDR è fondamentale per la maggior parte delle aziende nella selezione dei fornitori MDR

La scelta dei fornitori di servizi MDR spesso va oltre un semplice elenco di funzionalità e copertura. È influenzata anche dalle più ampie priorità del settore: più di nove organizzazioni su dieci definiscono il supporto del framework MITRE ATT&CK come critico (32%) o molto importante (62%). Inoltre, quasi tre quarti (73%) riportano che la tecnologia di sicurezza XDR è stata presa in considerazione durante il processo di selezione dei fornitori di servizi MDR. Mentre i due terzi delle organizzazioni consideravano importanti anche il servizio di accesso sicuro edge (Secure Service Access Edge, SASE) e la gestione della superficie di attacco (Attack Surface Management, ASM).

Importanza del supporto del framework MITRE ATT&CK da parte dei fornitori di servizi MDR.



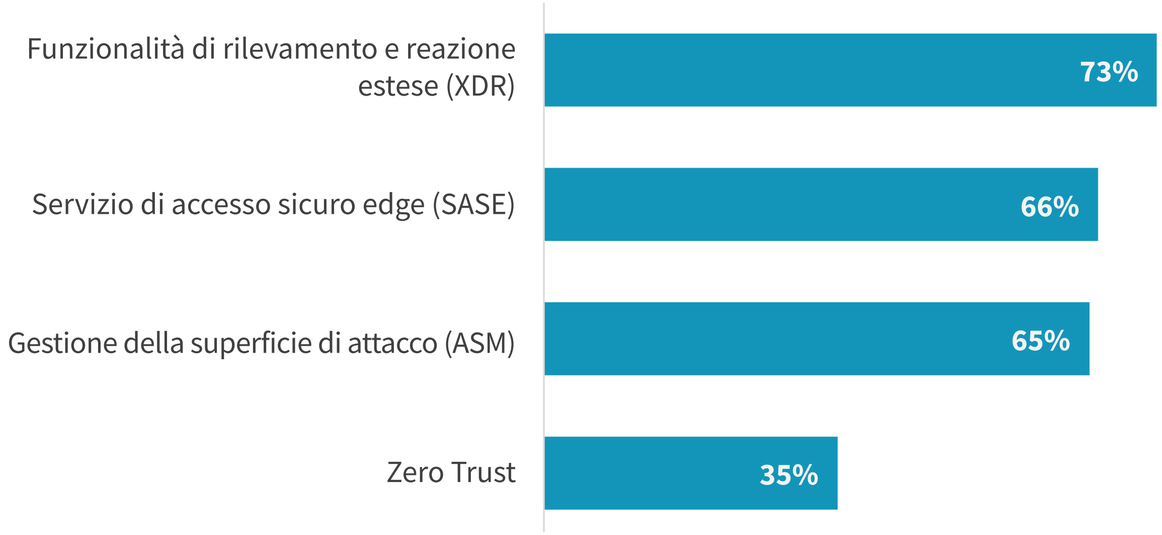
32%

Critico: non prenderemmo in considerazione un fornitore di servizi MDR che non supporta il framework MITRE ATT&CK

62%

Molto importante: preferiamo collaborare con un fornitore di servizi MDR che supporta il framework MITRE ATT&CK, ma potremmo prenderne in considerazione anche altri

Macro tendenze in materia di sicurezza considerate nel processo di selezione dei fornitori di servizi MDR.



TORNA AL SOMMARIO

MDR sta diventando una strategia di sicurezza molto diffusa

L'utilizzo dei servizi MDR è diventato un elemento centrale della strategia del programma di sicurezza, che ha promosso i fornitori di servizi MDR a partner strategici. I fornitori di servizi MDR aiutano i team addetti all'IT e alla sicurezza ad accelerare lo sviluppo del programma e migliorare il profilo di sicurezza; inoltre, consentono di ottenere vantaggi meno evidenti, come il raggiungimento degli obiettivi di conformità, l'acquisizione dell'assicurazione contro gli attacchi informatici e il miglioramento delle competenze e dei processi di sicurezza. La maggior parte delle organizzazioni considera i servizi MDR come parte integrante dell'investimento nel programma di sicurezza, con il 37% che definisce la MDR come un fattore critico e strategico, mentre un ulteriore 35% prevede di collaborare con il proprio fornitore di servizi MDR durante l'aggiornamento e l'implementazione delle strategie di sicurezza future.

ESG considera MDR una strategia di sicurezza importante e ormai diffusa. Suggerisce alle organizzazioni di esplorare nuovi casi d'uso che potrebbero accelerare lo sviluppo e il profilo del programma di sicurezza.

Dove si inserisce la MDR nel più ampio contesto della modernizzazione del SOC.

> La maggior parte considera i servizi MDR una **parte integrante dell'investimento nel programma di sicurezza."**

TORNA AL SOMMARIO

DELL Technologies

Dell Technologies (Borsa di New York: DELL) aiuta le organizzazioni e le persone a costruire il proprio futuro digitale e trasformare il loro modo di lavorare, vivere e socializzare. L'azienda fornisce ai clienti il portafoglio di tecnologie e servizi più ampio e innovativo del settore per l'era dei dati.

ULTERIORI INFORMAZIONI

INFORMAZIONI SU ESG

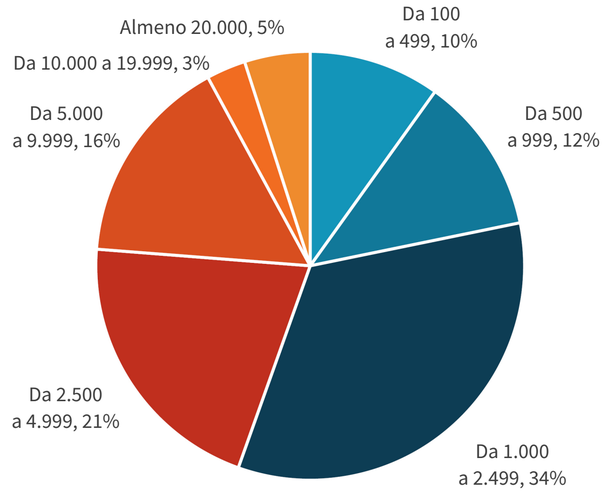
Enterprise Strategy Group è una società integrata di analisi della tecnologia, ricerca e strategia che offre intelligence di mercato, informazioni pratiche e servizi per i contenuti go-to-market alla community IT globale.

Metodologia di ricerca e dati demografici

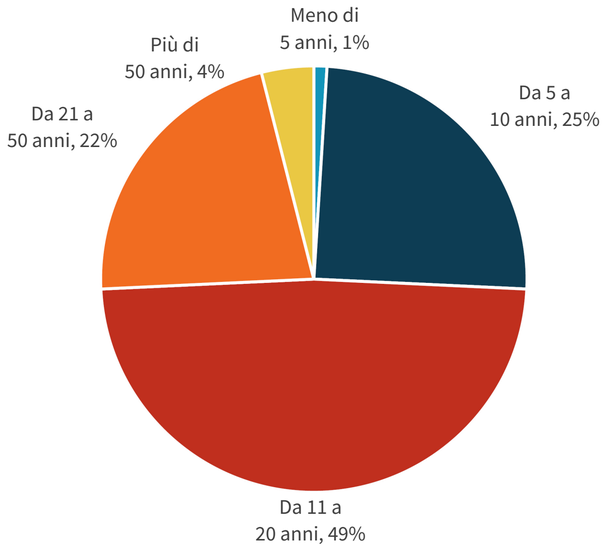
Per raccogliere i dati per questo report, ESG ha condotto una survey online completa, coinvolgendo i professionisti della sicurezza informatica provenienti da organizzazioni del settore pubblico e privato in Nord America (Stati Uniti e Canada) tra il 3 agosto 2022 e il 14 agosto 2022. Per partecipare a questa survey, gli intervistati dovevano essere professionisti della sicurezza informatica coinvolti personalmente nella tecnologia di sicurezza informatica, inclusi prodotti e servizi e processi. Tutti gli intervistati hanno ricevuto un incentivo per completare la survey sotto forma di premi in denaro e/o mezzi equivalenti.

Dopo aver escluso le persone non idonee, aver rimosso le risposte duplicate e aver verificato l'integrità dei dati delle risposte completate rimanenti (in base a una serie di criteri), è rimasto un campione finale complessivo di 373 professionisti della sicurezza informatica.

INTERVISTATI PER NUMERO DI DIPENDENTI



INTERVISTATI PER ETÀ DELL'AZIENDA



INTERVISTATI PER SETTORE

TORNA AL SOMMARIO

Enterprise Strategy Group è una società integrata di analisi della tecnologia, ricerca e strategia che offre intelligence di mercato, informazioni pratiche e servizi per i contenuti go-to-market alla community IT globale.