SOPHOS

EBOOK

EDR, XDR, MDR

Qual è la differenza? E qual è la scelta giusta per la tua azienda?

INDICE DEI CONTENUTI

EDR, XDR, MDR

Qual è la differenza? E qual è la scelta giusta per la tua azienda?

Gli IT e Cybersecurity Manager si trovano ad affrontare pressioni sempre più pesanti per rafforzare la resilienza informatica senza gravare eccessivamente su team e budget già al limite. Con l'aumento del volume delle minacce e la rapida diffusione di attacchi sempre più sofisticati, investire in modo intelligente nelle proprie capacità di rilevamento e risposta è un must.

Sia che tu operi su scala globale o che gestisca un team composto da poche persone, è fondamentale che il tuo approccio alla sicurezza sia in linea con il profilo di rischio e le realtà operative della tua organizzazione. Per molti manager, scegliere il giusto approccio di rilevamento e risposta alle minacce significa anche decidere se optare per una gestione autonoma o collaborare con un partner di fiducia. Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) e Managed Detection and Response (MDR) sono tutte soluzioni che garantiscono vantaggi unici, ma la vera sfida consiste nell'identificare quale sia la scelta in grado di offrire più valore alla tua organizzazione. EDR e XDR sono strumenti che aiutano il tuo team a rilevare le minacce, svolgere indagini e avviare una risposta più rapida. MDR è un servizio di monitoraggio e risposta alle minacce operativo 24/7, fornito da analisti esperti che di solito utilizzano XDR e altre tecnologie.

Comprendere quali sono le caratteristiche uniche che contraddistinguono ciascuno di questi approcci e come possono completarsi a vicenda è il primo passo verso la creazione di una strategia di sicurezza in grado di proteggerti oggi e di rafforzare la tua resilienza in futuro.

Perché il rilevamento e la risposta sono importanti

Poter contare su una protezione endpoint efficace rimane una prima linea di difesa essenziale. Tuttavia, i cybercriminali più sofisticati sfruttano credenziali legittime, attacchi basati sull'imitazione di utenti attendibili e strumenti informatici nativi utilizzati in modo improprio per eludere i sistemi di difesa. Questi attacchi potrebbero sembrare innocui per un singolo strumento di prevenzione, ed è proprio per questo motivo che vanno a segno.

Funzionalità di rilevamento e risposta come EDR, XDR e MDR colmano questa lacuna critica. Aiutano a identificare e neutralizzare le minacce che superano le misure di prevenzione, prima che possano trasformarsi in incidenti devastanti.

CHE COS'È EDR?

Endpoint Detection and Response (EDR) fa parte di una strategia di protezione endpoint continua. Aiuta i team a monitorare, rilevare e rispondere alle minacce e agli incidenti di sicurezza su dispositivi endpoint quali laptop, desktop e server.

I principali vantaggi di EDR:

Visibilità in tempo reale sulle attività degli endpoint (ad esempio l'esecuzione di file, il comportamento dei processi e i movimenti laterali), per permettere ai team di individuare e bloccare rapidamente le minacce, prima che possano diffondersi.

Rilevamento delle minacce più elusive, grazie all'identificazione di indicatori comportamentali, per consentirti di intercettare gli attacchi che spesso sfuggono ai tradizionali strumenti di prevenzione.

Automatizzazione di azioni di risposta come l'isolamento degli endpoint interessati o la terminazione dei processi dannosi, per ridurre il tempo di permanenza dei cybercriminali ed evitare che ottengano ulteriore accesso.

Scopri come Sophos EDR può proteggere i tuoi endpoint e server contro attacchi avanzati e coordinati da menti umane, tanto in ufficio, quanto sulla rete o nel cloud.

CHE COS'È XDR?

Extended Detection and Response (XDR) incrementa la visibilità sulle minacce grazie all'integrazione di dati provenienti dall'intero ecosistema di sicurezza, ben oltre il semplice livello di endpoint e server. Include firewall, infrastrutture cloud, sistemi di identità, soluzioni di posta elettronica e di backup e ripristino, nonché strumenti di produttività, endpoint e server, e molto di più. XDR permette di mettere in correlazione le attività sospette con maggiore efficacia, aiutandoti a identificare anche gli attacchi multivettore più sofisticati, che potrebbero sfuggire a singoli strumenti isolati.

Mentre EDR svolge un'analisi approfondita degli endpoint, XDR estende la visibilità e mappa le interazioni tra tutti i sistemi. Offre una visione olistica degli attacchi, semplificando il rilevamento di minacce multivettore a più fasi, che altrimenti passerebbero inosservate.

I vantaggi principali di XDR:

Correlazione dei segnali su più vettori di attacco, per individuare pattern e assegnare maggiore priorità agli avvisi ad alta affidabilità. Questo aiuta a ridurre le informazioni non pertinenti e a mettere in evidenza minacce complesse che colpiscono più sistemi.

Semplificazione dei flussi di lavoro delle indagini, per permettere al tuo team di rispondere alle minacce con maggiore rapidità e fiducia nelle tecnologie a sua disposizione. Gli analisti ottengono una visibilità superiore sulle dinamiche che hanno causato l'attacco, e su come impedire che si ripeta.

Supporto di flussi di lavoro di indagine e risposta con strumenti basati sull'IA, che accelerano l'analisi e la correzione dei problemi, per risolvere gli incidenti con maggiore rapidità e consapevolezza delle proprie capacità.

Scopri come Sophos XDR ti aiuta a rilevare attività sospette, svolgere indagini e intraprendere azioni di risposta nel tuo intero ecosistema informatico.

CHE COS'È MDR?

Managed Detection and Response (MDR) è un modello basato sui servizi, che offre la combinazione ottimale tra le tecnologie di IA e l'esperienza di analisti umani specializzati. Garantisce monitoraggio delle minacce, threat hunting e incident response 24/7. Si addice in particolar modo alle organizzazioni che non hanno tecnici operativi 24/7, che non possono contare sulla copertura completa di un SOC interno, che non hanno abbastanza personale disponibile, o che affrontano sfide legate a una crescente complessità dei sistemi.

MDR può essere implementato come servizio completamente gestito in outsourcing, oppure come estensione co-gestita del tuo team interno, per aiutarti a ridurre il tempo di permanenza dei cybercriminali e a bloccare incidenti come quelli causati dal ransomware, prima che abbiano conseguenze devastanti.

I principali vantaggi di MDR:

Protezione immediata 24/7. Le minacce non rispettano l'orario d'ufficio. l'88% degli attacchi ransomware si verifica al di fuori del normale orario di lavoro. MDR garantisce protezione a qualsiasi ora del giorno o della notte.

Accesso ad analisti di sicurezza esperti, che comprendono il comportamento dei cybercriminali e agiscono in modo tempestivo ed efficace. Questi specialisti gestiscono incidenti ogni giorno, assegnando la giusta priorità alle minacce e isolandole all'istante, per garantire la continuità operativa della tua azienda.

Eliminazione dello stress da eccesso di avvisi e delle attività di triage manuale. MDR rimuove le informazioni non pertinenti, aiutando il tuo team a concentrarsi sulle iniziative strategiche, invece di perdere tempo con falsi positivi.

Risoluzione rapida nei momenti critici. In incidenti nei quali la posta in gioco è alta, come nel caso del ransomware, i team MDR sono in grado di rilevare e isolare le minacce prima ancora che i team interni siano a conoscenza della loro esistenza, prevenendo così l'interruzione dei servizi e riducendo al minimo i rischi.

Scopri come Sophos MDR, con la sua piattaforma aperta basata sull'IA e il suo team di analisti esperti, può estendere il potenziale del tuo team e venire incontro alle tue esigenze, qualsiasi sia la fase del percorso di cybersecurity in cui ti trovi.

QUANDO CONSIDERARE UNA SOLUZIONE EDR, XDR O MDR

Soluzione	Potresti considerare questa soluzione se...	Potrebbe non essere la scelta più adatta se...
EDR	• Hai bisogno un sistema di rilevamento e risposta affidabile per i tuoi endpoint. • Desideri elevare le tue difese informatiche, oltre i limiti dei soli strumenti preventivi di protezione endpoint. • Stai creando una struttura di difesa a più livelli, in grado di supportare l'integrazione di XDR o MDR in futuro.	• Hai bisogno di maggiore visibilità sul tuo intero ambiente (cloud, identità, rete, backup, ecc.). • Ti servono rilevamento e risposta 24/7, senza bisogno di affidarti a un servizio in outsourcing e senza dover assumere altro personale.
XDR	• Vuoi una vista unificata per tutti i principali vettori di attacco, inclusi endpoint, firewall, rete, cloud, identità, backup e strumenti di produttività. • Desideri correlare più rapidamente le minacce e ridurre lo stress da eccesso di avvisi. • Cerchi un maggiore ritorno sui tuoi investimenti attuali e futuri nella sicurezza e nelle tecnologie informatiche.	• Monitori solo endpoint e server. • Ti serve un supporto più diretto di quello che può offrirti il tuo team. • Non hai abbastanza risorse interne per gestire una piattaforma XDR.
MDR	• Ti serve un servizio di rilevamento e risposta alle minacce gestito da esperti, che sia operativo 24/7. • Il tuo team soffre di stress da eccesso di avvisi o burnout, o fai fatica a trovare i giusti talenti. • Cerchi un partner proattivo che svolga indagini e neutralizzi le minacce per conto tuo. • Desideri migliorare la tua posizione cyberassicurativa, e magari ridurre i premi e aumentare la copertura della tua assicurazione attuale.	• Hai già un team SecOps interno consolidato, composto da un numero adeguato di dipendenti con le giuste competenze tecniche, che offre copertura affidabile 24/7. • La tua azienda non è pronta ad affidare parte delle tue attività di rilevamento e risposta a un servizio esterno.

ULTERIORI CONSIDERAZIONI PRIMA DI DECIDERE

Quando valuti le tue opzioni, esistono alcuni fattori critici che possono determinare se la scelta ideale per te sia EDR, XDR o MDR, e quale partner possa garantirti i risultati attesi.

I dati di intelligence sulle minacce sono importanti

L'efficacia di qualsiasi soluzione di rilevamento e risposta dipende dalla qualità dei dati di intelligence sulle minacce da cui è alimentata. Più ampie, approfondite e aggiornate sono le informazioni, più velocemente sarà possibile intercettare e bloccare le minacce. Assicurati che qualsiasi produttore tu prenda in considerazione sia in grado di descrivere l'origine e l'ambito dei propri dati sulle minacce.

Il servizio deve essere più di una semplice promessa

Anche le migliori tecnologie possono rivelarsi insufficienti, se non c'è anche un supporto reattivo. Sia che tu gestisca autonomamente i servizi o che ti affidi a un partner, è indispensabile che tu abbia la certezza di poter ricevere assistenza quando ne hai bisogno. Chiedi ai produttori come si articola concretamente il supporto: chi risponde, con quanta rapidità, cos'è incluso e come puoi ricevere assistenza durante un incidente attivo.

I costi non sono sempre trasparenti

Non dare per scontato che un'opzione sia intrinsecamente più cara. I prezzi variano notevolmente a seconda dell'implementazione e del supporto disponibile per ogni soluzione. Concentrati sulle tue esigenze specifiche e considera il tuo organico e gli investimenti attuali; valuta anche potenziali compromessi tra tecnologie e costi delle risorse interne, rispetto a quelle esterne.

Le soluzioni di rilevamento e risposta, in particolar modo MDR, possono influire sui costi delle cyberassicurazioni. Oggi come oggi, molte compagnie di assicurazioni hanno un occhio di riguardo verso le aziende che implementano un sistema di monitoraggio e risposta alle minacce operativo 24/7, il che può tradursi in una riduzione dei premi assicurativi o in condizioni migliori per la copertura.

Un'analisi completa del ritorno sull'investimento, che tenga conto dei risparmi operativi, della riduzione del rischio e persino dei vantaggi assicurativi può aiutarti a scoprire il costo effettivo e il valore reale di ciascun approccio.

IN CONCLUSIONE

1,53 milioni di $

Il costo medio di recovery in seguito a un attacco ransomware, senza tener conto di eventuali pagamenti del riscatto*.

40%

Percentuale di organizzazioni colpite dal ransomware, che afferma che la scarsa disponibilità di esperti di cybersecurity ha contribuito all'attacco*.

La posta in gioco è troppo alta per affidarsi al proprio intuito.

Scegliere la giusta strategia di rilevamento e risposta non è solo una questione di tecnologie, ma deve anche basarsi sulla responsabilizzazione del personale, sulla protezione delle attività operative aziendali e sull'implementazione di difese informatiche resilienti e capaci di resistere nel tempo.

*Report Sophos La vera storia del ransomware 2025

SOPHOS
DEFEAT CYBERATTACKS

SCOPRI DI PIÙ SULLE SOLUZIONI E SUI SERVIZI SOPHOS

Sophos ti aiuta a migliorare il rilevamento e la risposta alle minacce presenti e a quelle future, che possono emergere con l'evoluzione delle tue esigenze di sicurezza.

Parla con un esperto Sophos e troviamo insieme la soluzione più adatta per la tua azienda.