

Cos'è il servizio di rilevamento e risposta per gli endpoint?

e-book



Ransomware. Malware zero-day. Attacchi senza file. Phishing ed escalation dei privilegi.

Tutti questi aspetti rappresentano chiari pericoli per le reti, le imprese e le informazioni di identificazione personale dei tuoi clienti.

Per anni le soluzioni antivirus sono state il principale approccio per proteggere gli endpoint dei clienti. Tuttavia, con l'evoluzione del panorama delle minacce, è stata registrata la diffusione di nuove soluzioni concepite per risolvere alcuni dei problemi legati agli antivirus.

Negli ultimi anni, in particolare, si è diffuso l'uso del concetto di rilevamento e risposta per gli endpoint (EDR). Queste soluzioni sono state lanciate sul mercato specificamente per permettere di adattarsi al panorama di minacce informatiche in evoluzione, nell'ottica che tale panorama continuerà a evolvere più rapidamente di quanto gli esseri umani riescano a concepire. Vuoi saperne di più di queste soluzioni e del perché si distinguono dagli altri approcci?

Qui parleremo di queste soluzioni e spiegheremo perché i sistemi di rilevamento e risposta per gli endpoint sono essenziali per il futuro della sicurezza informatica.

Che cos'è esattamente una soluzione di rilevamento e risposta per gli endpoint?

Anton Chauvin di Gartner® ha dato vita all'espressione "rilevamento e risposta per gli endpoint" per descrivere una "suite di nuovi strumenti finalizzati alla visibilità, dalla prevenzione al rilevamento per l'endpoint".¹ Queste soluzioni hanno diverse funzionalità che vanno ad aggiungersi a quelle dei tradizionali antivirus. Tutte le funzioni dei moderni antivirus vengono espletate a livello avanzato dalle soluzioni di rilevamento e risposta per gli endpoint, il che offre una sicurezza migliorata e la massima tranquillità agli utenti. Tra le diverse funzionalità di tali soluzioni ricordiamo:

- Monitoraggio
- Rilevamento delle minacce
- Possibilità di creare elenchi di divieto/esclusione
- Risposta alle minacce
- Integrazione con altre soluzioni di sicurezza informatica

Le soluzioni EDR hanno sviluppato diversi approcci per aumentare il livello di protezione che i fornitori di IT e i professionisti IT possono offrire ai propri utenti, dall'impiego dell'intelligenza artificiale per monitorare e rilevare nuove minacce o comportamenti sospetti per gli endpoint al rollback automatico dopo un attacco ransomware.

¹ "A Short History of EDR", Reed Exhibitions Ltd, [infosecurity-magazine.com/opinions/history-edr/](https://www.infosecurity-magazine.com/opinions/history-edr/) (consultato nel mese di settembre 2020).

Il ruolo delle soluzioni EDR nell'universo della sicurezza informatica

Queste soluzioni hanno lo scopo di proteggere gli endpoint. Dato il numero di minacce che si diffondono ogni giorno, gli antivirus e altri prodotti tradizionali per la sicurezza degli endpoint non riescono a stare al passo con la gestione degli attacchi su un elevato numero di endpoint. I tradizionali antivirus hanno un approccio passivo, poiché riescono solo a rilevare e a mettere in quarantena le minacce già note e precedentemente identificate.

Molte soluzioni antivirus operano in base alle tradizionali firme dei virus. Quando un file malware viene individuato, esso genera un hash che viene poi aggiunto a un database di firme di virus. I programmi antivirus, quindi, eseguono scansioni per individuare eventuali file corrispondenti alla firma nota di un virus presente nel database, quindi mettono tali file in quarantena.

Ed è proprio qui il nocciolo della questione: gli antivirus necessitano di frequenti aggiornamenti delle firme. Questo vuol dire che c'è spesso uno scarto temporale fra quando viene scoperto il nuovo virus e quando i clienti possono considerarsi protetti da esso. In più, le minacce non ancora individuate possono operare indisturbate, prima che gli utenti ricevano l'aggiornamento. Gli antivirus hanno un approccio reattivo.

Per contro, quello delle soluzioni EDR è proattivo. Costituite da un software di monitoraggio e dagli agent degli endpoint, le soluzioni EDR impiegano il machine learning integrato e l'intelligenza artificiale avanzata per identificare comportamenti sospetti e porvi rimedio a prescindere che sia presente una firma. Ad esempio, se viene rilevata la modifica a diversi file contemporaneamente, è probabile che si tratti del risultato di un attacco all'endpoint e non di un errore umano.

Ma anche i criminali informatici hanno imparato a essere proattivi: molti di essi hanno ideato metodi per eludere i controlli delle soluzioni antivirus tradizionali. Alcuni potrebbero sviluppare malware in grado di cambiare regolarmente le firme per evitare la corrispondenza con una firma nota presente nel database dell'antivirus oppure potrebbero addirittura sferrare un attacco senza file e configurare un nuovo account amministratore con privilegi elevati su un endpoint. Una soluzione EDR cerca comportamenti anomali sugli endpoint (rispetto a uno standard) e prende le opportune misure. In questo modo, potrà sventare gli attacchi dei criminali proattivi mediante l'impiego di difese altrettanto proattive.

Gli antivirus riescono solo a rilevare e a mettere in quarantena le minacce già note e precedentemente identificate.

L'unica costante è il cambiamento

Il mondo assiste a stravolgimenti costanti e questo vale anche per le tecnologie. Il cloud ha cambiato immensamente le nostre vite, dalla diffusione dell'e-commerce alle soluzioni di livello enterprise cui si affidano ogni giorno miliardi di individui. Eppure, via via che le tecnologie evolvono, i criminali informatici individuano nuove modalità per sfruttare questi cambiamenti e compromettere i dati delle aziende. I dati rappresentano senza dubbio la principale risorsa dei tuoi clienti: come contribuisce alla loro salvaguardia?

Come il cloud, l'intelligenza artificiale e il machine learning promettono di stravolgere il modo di fare impresa e le nostre vite. Intelligenza artificiale e machine learning sono alla base delle soluzioni EDR e fungono da motore che alimenta una protezione avanzata dalle minacce, permettendo di riconoscere e di sventare minacce avanzate.

Una soluzione EDR impiega il machine learning per stabilire lo standard comportamentale di un endpoint. Partendo da questa base, la soluzione di rilevamento e risposta per gli endpoint individua comportamenti che si discostano dallo standard. Ecco il punto di forza delle soluzioni EDR, che si pongono domande quali:

- Questo endpoint ha già eseguito questa attività in passato?
- Questo file o comportamento mostra schemi anomali?
- Perché alcuni file messi in sicurezza vengono visualizzati o selezionati?

In sostanza, le soluzioni EDR impiegano l'IA per individuare segnali di una compromissione senza doversi basare su indicazioni di compromissione già note (che potrebbero essere sovvertite). I virus polimorfi avanzati (quelli in grado di generare versioni modificate di se stessi per contrastare il rilevamento) e le minacce zero-day (che prendono di mira e sfruttano una vulnerabilità precedentemente sconosciuta) possono eludere le soluzioni antivirus tradizionali. Le soluzioni EDR non solo si pongono le giuste domande, ma forniscono anche le risposte necessarie a sventare la minaccia, con la possibilità di eliminare, mettere in quarantena, implementare correzioni ed eseguire il rollback.

Modalità di risposta alle minacce da parte delle soluzioni EDR

Queste soluzioni non si limitano a rilevare le minacce, ma possono anche intervenire opportunamente per sventarle. Quando l'agent di un endpoint rileva una minaccia, un'adeguata soluzione EDR reagisce immediatamente tramite il sistema di monitoraggio centralizzato. Il sistema di monitoraggio centralizzato analizza e mette in correlazione le minacce. A seconda della soluzione EDR impiegata, è possibile persino monitorare visivamente la genesi della minaccia e il percorso all'endpoint. La possibilità di visionare la cronologia di un attacco ti consente di comprendere il ciclo di vita dell'attacco stesso. Potrai utilizzare queste informazioni per prevenire le minacce future, ma anche per dimostrare il valore dei tuoi servizi di sicurezza ai clienti.

Sebbene un antivirus e la crittografia del disco rappresentino modi validi per mettere in sicurezza gli endpoint, le soluzioni EDR mettono a disposizione funzionalità in grado di rendere a prova di futuro le macchine dei tuoi utenti, ad esempio analisi quasi in tempo reale di file e avvisi, analisi forensi dettagliate, protezione offline, possibilità di scollegare i dispositivi dalla rete per impedire un'ulteriore diffusione e, cosa più importante, il rollback del file infetto.

Scopriamo come una soluzione di rilevamento e risposta per gli endpoint può intervenire in caso di ransomware. Ecco cosa accade di norma durante un attacco ransomware: un utente apre un allegato o un'e-mail o visita una pagina web con uno script malevolo. Improvvisamente visualizza una notifica che lo informa che i suoi file sono stati sottoposti a crittografia. Il criminale informatico restituirà i file al legittimo proprietario solo dopo il pagamento di un'ingente somma di denaro, ma non c'è alcuna garanzia che i dati gli vengano poi effettivamente restituiti; ecco perché molte aziende non vogliono rischiare con il pagamento.

Le soluzioni di rilevamento e risposta per gli endpoint con funzionalità di rollback dopo un attacco ransomware offrono un grande valore ai clienti. Questa funzionalità impiega tecnologie avanzate per acquisire istantanee dell'endpoint a intervalli regolari (configurati a discrezione dell'amministratore). Se l'attacco ransomware va a buon fine, bastano pochi clic per eseguire il rollback dell'immagine del disco dell'endpoint precedente all'attacco, il che ti permette di aiutare i clienti a risparmiare tempo e denaro.

Una soluzione EDR è adatta alle tue esigenze e a quelle dei tuoi clienti?

Prima di implementare una soluzione EDR è necessario considerare le tue capacità e le esigenze dei clienti. Come già detto in precedenza, questo approccio non è l'unico modo per mettere un endpoint in sicurezza. Per stabilire la soluzione adatta è necessario considerare i tuoi dati e i casi d'uso. Se da un lato le soluzioni EDR sono perfette per chi gestisce dati sensibili sulle risorse umane (che generalmente includono anche informazioni di identificazione personale), potrebbero non essere necessarie per altri utenti che salvano i dati personali su cloud o che dispongono di un solido client di backup combinato alla crittografia del disco e a un antivirus.

Tuttavia, se i tuoi clienti prendono decisioni in base ai prezzi e vogliono affidarsi ad altre soluzioni, vale la pena discutere con loro della possibilità di implementare una soluzione di rilevamento e risposta per gli endpoint. Potrebbe essere opportuno anche considerare la possibilità di consigliare o persino di imporre loro l'adozione di una soluzione EDR. Per i neofiti, una funzionalità di rollback successiva a un attacco ransomware potrebbe valere da sola il costo della soluzione. Se qualcuno fosse colpito da un attacco ransomware, una soluzione di rilevamento e risposta per gli endpoint può rilevarlo, bloccarlo, ripristinare l'endpoint in pochi secondi e impedire la diffusione del ransomware in tutta la rete. Questa possibilità potrebbe evitare tempi di inattività lunghi e far risparmiare ingenti somme di denaro e tempo ai clienti finali. In più, le soluzioni EDR offrono una protezione più completa rispetto agli antivirus da soli. Queste soluzioni non sono le uniche per mettere in sicurezza gli ambienti dei clienti, ma potrebbe valere la pena discuterne con loro e caldeggiare l'implementazione di una protezione più completa.

Informazioni su N-able

N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e a espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore. n-able.com/it

Il presente documento viene fornito per puro scopo informativo e i suoi contenuti non vanno considerati come una consulenza legale. N-able non rilascia alcuna garanzia, esplicita o implicita, né si assume alcuna responsabilità legale per le informazioni qui contenute, per l'accuratezza, la completezza o l'utilità dei dati qui inclusi.

I marchi registrati, marchi di servizio e loghi sono di esclusiva proprietà di N-able Solutions ULC e N-able Technologies Ltd. Tutti gli altri marchi registrati sono di proprietà dei rispettivi titolari.