

Antivirus tradizionali e soluzioni di rilevamento e risposta per gli endpoint a confronto

E-book



Introduzione

Una ogni 11 secondi: la frequenza con cui si prevede che un'azienda cadrà vittima di un attacco ransomware entro il 2021.1

Le minacce informatiche continuano a diffondersi, con il COVID-19 che crea altre opportunità che fanno gola ai potenziali hacker. Per gli MSP la sicurezza su più livelli rappresenta senza dubbio la migliore difesa dalle minacce presenti e future per le reti e gli utenti finali dei loro clienti.

In questo modello sono due le soluzioni disponibili per proteggere gli utenti finali: gli antivirus tradizionali e rilevamento e risposta per gli endpoint (EDR). Entrambe offrono vantaggi agli MSP, ma i livelli di protezione che mettono a disposizione sono differenti. Nessuna delle due rappresenta una soluzione adatta a tutte le esigenze e ambedue risolvono diversi problemi.

Per stabilire quale utilizzare è opportuno considerare diversi fattori, ad esempio il tipo di azienda che va protetta, i relativi utenti finali e i costi ecc. N-able mette a disposizione entrambe le soluzioni per aiutare gli MSP a garantire il migliore livello di servizio ai clienti. Tratteremo di entrambe le soluzioni. Per una rapida panoramica delle differenze alla fine di questo documento è presente uno schema riepilogativo.

Antivirus: protezione robusta, facilità d'uso e costi ridotti

Con gli antivirus tradizionali gli MSP gestiscono gli aggiornamenti automatici ai programmi e alle definizioni dei virus, pertanto non è necessario alcun intervento da parte degli utenti. Eventuali virus o malware rilevati vengono immediatamente messi in quarantena. Si tratta di una prima linea di difesa semplice e intuitiva per i dipendenti poiché non richiede competenze tecniche e riesce a tenere alla larga molte minacce.

Tuttavia, gli antivirus tradizionali richiedono frequenti aggiornamenti alle definizioni (firme dei virus). La protezione garantita dalla soluzione è adeguata solo se il fornitore esegue gli opportuni aggiornamenti. Ogni giorno vengono diffuse nuove minacce e la garanzia che gli aggiornamenti vengano messi a disposizione tempestivamente è una situazione ideale. Spesso le minacce vengono individuate solo quando il danno è già stato fatto.

Posto questo difetto critico, perché scegliere una soluzione antivirus? Prima di tutto, naturalmente, per la facilità d'uso. Il fatto che i clienti non debbano intervenire significa che hanno un aspetto in meno di cui occuparsi. Si tratta di una proposta di valore adeguata a un prezzo accessibile. Ed ecco altri vantaggi, fra gli altri:

- **Una sola fonte di gestione:** il cliente fa riferimento all'MSP come unica fonte di implementazione, gestione, aggiornamenti alle definizioni e resoconti per le minacce. In questo modo, gli MSP conquisteranno la fiducia dei clienti, il che potrebbe favorire maggiori ricavi in altre aree.
- **Sicurezza "bloccata":** i criteri dei programmi antivirus azzerano gli interventi da parte degli utenti finali, i quali non possono forzare un aggiornamento o disinstallare il programma senza le opportune autorizzazioni.
- **Monitoraggio 24/7:** gli MSP impostano il programma delle scansioni, aggiornano il software e avviano gli aggiornamenti alle definizioni. Come già detto, queste operazioni non richiedono alcun intervento da parte dei clienti o dei relativi utenti finali.
- **Rimedi rapidi:** è possibile classificare le minacce appena si verificano.

- **Costi:** le soluzioni antivirus hanno un costo più contenuto per utente rispetto a quelle di rilevamento e risposta per gli endpoint. Questo rappresenta il secondo principale punto a favore per la vendita dopo l'aspetto legato alla protezione efficace. Tuttavia, come vedremo più avanti i margini stanno diventando inferiori. E, dato il panorama di minacce odierno, i clienti potrebbero non riuscire a permettersi una soluzione di rilevamento e risposta per gli endpoint.

Soluzioni di rilevamento e risposta per gli endpoint: prevenzione e protezione professionali

Si tratta di soluzioni complete che offrono tutte le funzionalità di un antivirus, ma di livello superiore poiché offrono una maggiore sicurezza e (cosa più importante) la tranquillità assoluta. Tra le diverse funzionalità, ricordiamo:

- Monitoraggio
- Rilevamento delle minacce
- Elenco di accessi consentiti o bloccati
- Risposta alle minacce
- Integrazione con altre soluzioni di sicurezza informatica
- Funzionalità avanzate rispetto a rilevamento minacce e messa in quarantena

Come nel caso degli antivirus, sono gli MSP che gestiscono queste soluzioni senza che sia necessario alcun intervento da parte degli utenti finali. Dato il numero di minacce diffuse ogni giorno, la gestione di un elevato numero di endpoint può essere più complicata con un semplice antivirus e le altre point solution. Ecco dove risiede la differenza tra soluzioni antivirus e soluzioni di rilevamento e risposta per gli endpoint.

Queste ultime sono proattive. Insieme al software di monitoraggio e agli agent per gli endpoint, il machine learning integrato e l'intelligenza artificiale avanzata consentono a queste soluzioni di identificare i vettori delle minacce che mostrano un comportamento sospetto e di neutralizzarli prima che vengano riconosciuti come dannosi. Invece che affidarsi agli aggiornamenti alle definizioni, cercano comportamenti anomali. Ad esempio, se viene rilevata la modifica a diversi file contemporaneamente, è probabile che sia in corso un attacco all'endpoint.

Con N-able™ Endpoint Detection and Response (EDR), l'elaborazione viene eseguita in locale sull'endpoint, a differenza di altre soluzioni che richiedono una risorsa e lunghi caricamenti su cloud per l'analisi e l'elaborazione delle minacce. Il ripristino è rapido e automatizzato.

Accettare che una minaccia abbia seminato danni nei sistemi non è sufficiente: è necessario scoprire come e perché si è arrivati a questo punto. È in questo ambito che eccellono le soluzioni di rilevamento e risposta per gli endpoint. N-able EDR offre il contesto reale, grazie a una storia visiva (Figura 1).

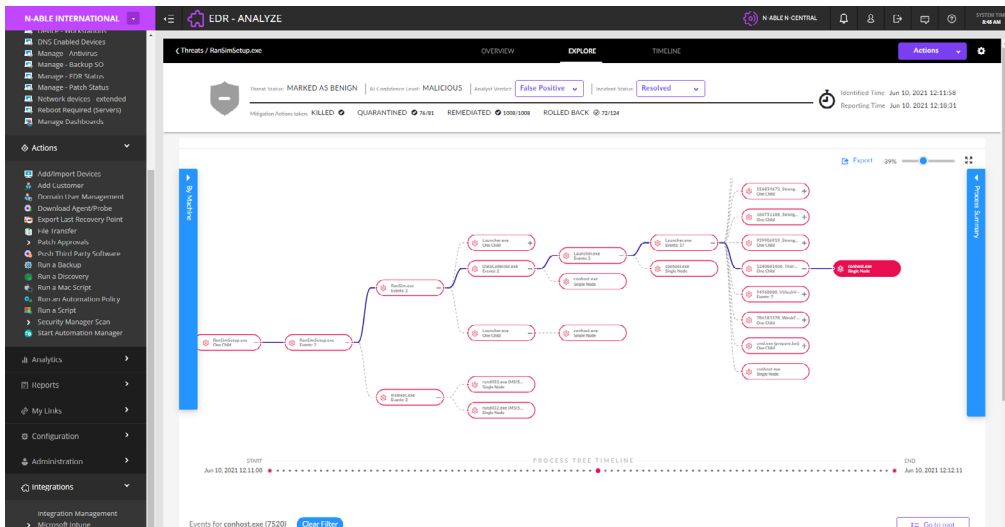


Figura 1: storia visiva

Da qui è possibile visualizzare il processo che ha dato origine all'attacco e le relative modalità di replica e diffusione. Qui sono inoltre disponibili i dati sulla struttura della minaccia che forniranno informazioni fruibili per aiutare gli utenti finali a capire il loro ruolo nella diffusione della minaccia, se è questo il caso.

La storia si aggiorna in tempo reale durante un attacco, ma con N-able EDR sono disponibili tutte le difese necessarie. L'agent EDR rappresenta un vero e proprio analista di un centro operativo per la sicurezza. Tra le opzioni di ripristino sono disponibili eliminazione, messa in quarantena, applicazione di rimedi e rollback dell'attacco (Figura 2), a seconda della configurazione dell'agent per ciascun utente finale. Nel caso di un attacco ransomware, è possibile ripristinare lo stato precedente all'attacco per un endpoint infetto (solo per sistemi operativi Windows®).

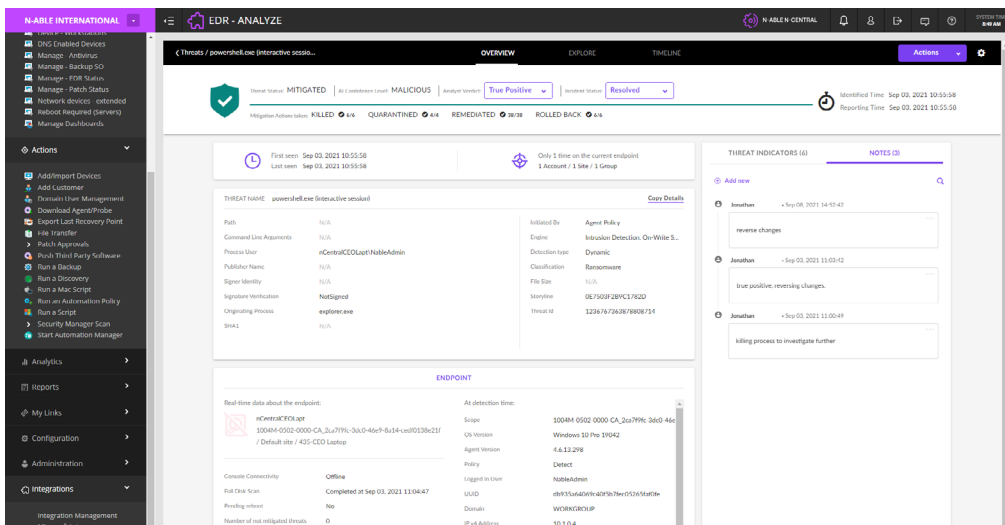


Figura 2: operazioni di eliminazione, messa in quarantena, applicazione di rimedi e rollback

Protezione dei dispositivi: tipologie di utenti

N-able mette a disposizione soluzioni antivirus e di rilevamento e risposta per gli endpoint: basta considerare un aspetto per determinare l'approccio necessario. Qual è la tipologia di utenti finali che va protetta? Per stabilirlo, ecco alcune categorie:

- **Responsabile risorse umane:** probabilmente sulla macchina ha archiviato informazioni in grado di identificare le persone, vale a dire confidenziali. Se un criminale informatico avesse accesso a tali dati durante una violazione, individui e aziende potrebbero subire danni catastrofici. Ecco perché è necessario sventare gli attacchi in tempo reale, prima che prendano piede e causino danni ingenti. Una soluzione di rilevamento e risposta per gli endpoint è la scelta più ovvia per questo tipo di utenti finali. I potenziali rischi e i costi derivanti giustificano ampiamente la spesa aggiuntiva.
- **Responsabile marketing:** probabilmente sulla sua macchina conserva file importanti, ma non informazioni in grado di identificare le persone. Per questo motivo, una combinazione di antivirus, backup e crittografia del disco offre una difesa robusta e su più livelli, per cui sarà possibile limitarsi a una soluzione antivirus per abbassare i costi. La maggioranza degli utenti appartiene a questa categoria.
- **Dirigenti:** questi rappresentano il rischio massimo in caso di violazione poiché conservano sulle proprie macchine sia informazioni in grado di identificare le persone sia altri dati di alto valore per l'impresa. I dati di questi utenti non solo vanno protetti, ma bisogna anche garantirne il ripristino con la funzionalità di rollback. In questo caso, è opportuno installare la soluzione di rilevamento e risposta per gli endpoint.

Bottom line

Per offrire una valutazione obiettiva, non possiamo non occuparci del problema dei costi. Le soluzioni di rilevamento e risposta per gli endpoint hanno un prezzo maggiore per licenza rispetto ai tradizionali antivirus, ma non sono proibitive. Molti clienti potrebbero opporsi all'idea di corrispondere costi aggiuntivi, ma c'è da dire che potrebbero non potersi permettere una soluzione del genere. Per farti un'idea dei potenziali costi per l'impresa, leggi il caso di studio di un cliente che ha scelto di non dotarsi di una soluzione di rilevamento e risposta per gli endpoint.

Se i tuoi clienti non dispongono di una soluzione per proteggere gli endpoint, consigliamo di proporli la soluzione di rilevamento e risposta per gli endpoint. In tal modo, non ci saranno costi di upgrade per il passaggio dall'antivirus alla soluzione di rilevamento e risposta per gli endpoint e la maggiore tranquillità giustifica la scelta. Per quanto riguarda i server, vanno trattati allo stesso modo delle risorse a elevato valore che ospitano, per cui una soluzione di rilevamento e risposta per gli endpoint è la scelta più giusta.

Se i tuoi clienti oppongono resistenza per i costi, concentrati non solo su ciò che il cliente perde passando a una soluzione di rilevamento e risposta per gli endpoint, ma su cosa guadagna. Generalmente basta solo un minuto per eseguire un rollback rispetto alle 4/6 ore necessarie per ricreare l'immagine di ciascun dispositivo e sono anche disponibili i dettagli di quello che è successo. Infine, qualora si verifici una violazione, la possibilità di perdere il cliente è elevata.

Un ultimo punto da tenere presente: le soluzioni di rilevamento e risposta per gli endpoint non sostituiscono il backup dei dati. Senza dubbio, il backup dei dati con archiviazione off-site è e resterà una best practice per l'igiene informatica. Insieme sono un'accoppiata vincente.

Antivirus e soluzioni di rilevamento e risposta per gli endpoint a colpo d'occhio

	ANTIVIRUS	RILEVAMENTO E RISPOSTA PER GLI ENDPOINT
Dati contestuali e di analisi forense per le minacce	Limitati	Completi
Eliminazione, messa in quarantena, applicazione di rimedi e rollback	Solo eliminazione/quarantena	Tutto
Utilizzo del database Common Vulnerabilities and Exposures (CVE)	No	Si
Protezione utenti offline	Richiede definizioni aggiornate	Si
Criteri per consentire/bloccare dispositivi USB per fornitore/classe/numero seriale/prodotto	No	Si
Criteri per contenere le minacce mediante disconnessione dalla rete	No	Si
Criteri per controllare le impostazioni del firewall dell'endpoint	No	Si
Utilizzo delle risorse	Moderato	Ridotto
Difesa da minacce wrapper/obfuscator e di variazione	Richiede definizioni aggiornate	Si
Difesa da attacchi senza file	No	Si
Difesa da minacce sconosciute e zero-day	Richiede definizioni aggiornate	Si
Impiega il rilevamento basato su firme	Si	Si

INFORMAZIONI SU N-ABLE

N-able (precedentemente SolarWinds MSP) permette ai provider di servizi gestiti (MSP) di aiutare le imprese di piccole e medie dimensioni a stare al passo con l'evoluzione digitale. Grazie a una piattaforma tecnologica flessibile e a potenti integrazioni, aiutiamo gli MSP a monitorare, gestire e proteggere sistemi, dati e reti dei clienti finali. Il nostro portfolio sempre in crescita di soluzioni di sicurezza, automazione e backup è stato concepito per i professionisti della gestione di servizi IT. N-able semplifica gli ecosistemi complessi e permette ai clienti di risolvere le sfide più urgenti. Forniamo un'assistenza completa e proattiva, tramite programmi di arricchimento per partner, formazione pratica e risorse finalizzate alla crescita, per aiutare gli MSP a offrire un valore eccezionale e a raggiungere il successo su ampia scala.

n-able.com/it

N-ABLE, N-CENTRAL e gli altri marchi e loghi di N-able sono di esclusiva proprietà di N-able Solutions ULC e N-able Technologies Ltd. e potrebbero essere marchi di common law, marchi registrati o in attesa di registrazione presso l'Ufficio marchi e brevetti degli Stati Uniti e di altri paesi. Tutti gli altri marchi menzionati qui sono utilizzati esclusivamente a scopi identificativi e sono marchi (o potrebbero essere marchi registrati) delle rispettive aziende.