Presentazione della soluzione di rilevamento e risposta per gli endpoint integrata in RMM

Monitorate e gestite gli endpoint da una singola dashboard, sin da subito

Le minacce alla sicurezza si moltiplicano e si trasformano ogni giorno. Una volta risolta una minaccia, i criminali informatici trovano un altro punto debole da sfruttare per accedere a reti e sistemi. I clienti si aspettano che il proprio MSP stia al passo con queste minacce in continua evoluzione e che li protegga.

SolarWinds® RMM include il servizio SolarWinds Endpoint Detection and Response (EDR) integrato, con tecnologia SentinelOne®. Questo significa che potrete implementare, configurare e monitorare senza difficoltà la protezione degli endpoint, contenere rapidamente le minacce e ridurre le interruzioni per i vostri clienti.

Q. Che cos'è la funzionalità di rilevamento e risposta per gli endpoint?

A differenza degli antivirus tradizionali, EDR offre il monitoraggio continuo, acquisisce e conserva i dati e impiega l'IA comportamentale per rilevare le minacce. Se rileva una minaccia su un dispositivo, l'agent EDR può automaticamente metterla in quarantena per contenerla e annullare gli effetti dell'attacco ripristinando una versione integra precedente (solo per sistemi operativi Windows®). Inoltre, è in grado di fornire dati fruibili per effettuare ulteriori analisi.

Q. Perché adottare la soluzione EDR integrata?

È necessario proteggere se stessi e i clienti dalle minacce alla sicurezza andando oltre un tradizionale antivirus. Via via che si diffonde sempre di più la distribuzione della forza lavoro, SolarWinds EDR dà una marcia in più a qualsiasi servizio di sicurezza e alla vostra attività di MSP poiché vi consente di:

- Proteggere i clienti con una sicurezza di livello enterprise
- Generare maggiori ricavi ricorrenti
- Acquisire visibilità e dati fruibili sugli attacchi
- Porre rimedio a eventuali problemi riducendo al contempo le percentuali di abbandono dei clienti
- Garantire tranquillità, grazie a una protezione avanzata dalle minacce

Q. Che cosa significa integrata?

La console SolarWinds EDR è incorporata in SolarWinds RMM per facilitare il lavoro degli MSP. È possibile utilizzare RMM e le relative funzionalità di automazione per:

- Implementare e aggiornare le ultime versioni dell'agent EDR per dispositivi Windows, utilizzando la funzionalità nativa di RMM
- Configurare rapidamente norme, esclusioni e altre impostazioni per EDR
- Sfruttare i flussi di lavoro PSA per gestire gli avvisi di EDR, incluse le notifiche di eventuali infezioni ai dispositivi
- Visualizzare i widget riepilogativi della dashboard per consultare lo stato dettagliato o riepilogativo di tutti i dispositivi
- Ridurre gli avvisi e mitigare le minacce tramite il centro minacce dotato di una barra di stato avanzata, senza chiudere la pagina
- Automatizzare i controlli di servizio per la piattaforma

Q. Come faccio a richiedere una prova?

Se disponete già di RMM, potete attivare una prova di 30 giorni della funzionalità EDR integrata direttamente dall'applicazione. Basta seguire questa procedura:

1. Attivate la prova in "Integration Management View" (Vista gestione integrazioni) di RMM, disponibile nel menu di navigazione a sinistra
2. Aprite il menu "Integrations" (Integrazioni) nel riquadro di navigazione a sinistra
3. Selezionate "Integration Management" (Gestione integrazioni)
4. Fate clic su "Activate" (Attiva)
5. Create le norme EDR
6. Abilitate la funzionalità EDR tramite SolarWinds RMM

Q. Posso attivare una prova della soluzione EDR integrata se sto utilizzando la versione standalone con SolarWinds RMM?

Sì. È possibile eseguire la migrazione degli agent EDR esistenti implementati sugli endpoint già gestiti da SolarWinds RMM e registrati in una console di gestione di SolarWinds EDR alla soluzione EDR integrata.

Q. Cos'altro devo considerare se sto utilizzando la versione standalone di SolarWinds EDR con SolarWinds RMM?

È necessario disattivare l'autenticazione a due fattori a livello di account della console EDR standalone per eseguire la corretta migrazione dei dispositivi. Questo si applica all'autenticazione a due fattori a livello di account e non a livello di utente singolo. La procedura per disabilitare l'autenticazione a due fattori è descritta qui.

La procedura di attivazione è automatizzata. Tuttavia, richiede la creazione degli opportuni criteri e l'attivazione della funzionalità EDR integrata su un dispositivo o su una serie di dispositivi.

La creazione di criteri nell'interfaccia integrata non garantisce la migrazione diretta dei criteri né la conversione delle esclusioni dalla soluzione EDR standalone ai criteri della soluzione EDR integrata. Al termine del periodo di prova, dovrete coinvolgere il reparto commerciale di SolarWinds per confermare la migrazione delle licenze dalla versione standalone ai contratti integrati.

Q. Quali widget sono disponibili nella dashboard?

- Minacce non risolte: per indagare sulle minacce della massima priorità
- Endpoint infetti: per visualizzare gli endpoint che necessitano di ispezione
- Agent S1 che richiede attenzione: per visualizzare gli agent che vanno riavviati o sottoposti ad altre misure
- Stato di rete agent S1: per visualizzare la disponibilità degli agent SentinelOne
- Copertura versione agent S1: per osservare le metriche sulla versione dell'agent nella rete
- Rilevamento minacce per motore: per valutare le tipologie di minacce

Q. Quali considerazioni sulla migrazione è opportuno fare se uso già SentinelOne EDR?

Soluzione SolarWinds EDR standalone:

- Con gli agent EDR standalone già implementati sui dispositivi gestiti da RMM, tali agent saranno disponibili per una migrazione sostitutiva con cui l'agent EDR verrà trasferito in modo facile e veloce dalla dashboard standalone esistente alla nuova dashboard integrata.
- Sebbene sia una procedura automatizzata, la sostituzione richiede la creazione degli opportuni criteri e l'attivazione manuale (come descritto in precedenza) della funzionalità EDR sugli endpoint o sul gruppo di endpoint. La creazione di criteri nell'interfaccia integrata non garantisce la migrazione diretta dei criteri né la migrazione delle esclusioni dalla soluzione EDR standalone alla soluzione EDR integrata.
- Disponendo della versione standalone di SolarWinds EDR, una volta attivata la funzionalità EDR integrata per RMM, i dispositivi verranno automaticamente trasferiti alla dashboard integrata. Pertanto, questi endpoint non saranno più visibili nella dashboard di SolarWinds EDR standalone, ma saranno disponibili e gestibili dalla dashboard integrata.
- Al termine del periodo di prova, dovrete rivolgervi a un rappresentante SolarWinds per confermare la migrazione della licenza dalla soluzione standalone a quella integrata. Se una soluzione EDR integrata scade, è disponibile un periodo di grazia minimo di sette giorni per rimuovere gli agent EDR dai dispositivi inclusi nella prova.

SentinelOne EDR non fornito da SolarWinds:

- La migrazione sostitutiva non è compatibile con un agent SentinelOne non gestito dalla versione standalone di SolarWinds EDR. I tentativi di attivare la funzionalità EDR su tali dispositivi comporterà la mancata riuscita dell'implementazione della funzionalità EDR.
- La migrazione sostitutiva continuerà a tentare il trasferimento degli endpoint finché:
    - La funzionalità EDR sull'endpoint non viene disattivata
    - L'agent SentinelOne del fornitore terzo non viene rimosso e può essere installato l'agent SolarWinds EDR

Q. Cos'altro dovrei sapere della versione integrata?

È possibile implementare la funzionalità EDR integrata solo nei servizi gestiti RMM. Al momento la funzione EDR integrata non è compatibile con dispositivi macOS® o Linux®.

Il nostro obiettivo è rendere l'esperienza con SolarWinds EDR integrato in RMM un'esperienza di livello superiore. Questo è solo il primo passo verso questa direzione.

Nota: si consiglia di testare la funzionalità EDR in un ambiente non di produzione, configurando i criteri per l'utilizzo della modalità di rilevamento in fase di test prima dell'implementazione globale.

In caso di domande o se necessitate di assistenza, contattate il team commerciale o visitate la pagina success.solarwindsmsp.com.