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

Le previsioni stimano che nel 2021 ogni 11 secondi un'impresa cadrà vittima di un attacco ransomware.

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

Nell'ambito di questo modello sono due le soluzioni disponibili per proteggere gli utenti finali: gli **antivirus e le soluzioni di rilevamento e risposta per gli endpoint (EDR).** Entrambi offrono vantaggi agli MSP, ma con diversi livelli di protezione. Nessuna delle due rappresenta una soluzione adatta a tutte le esigenze, poiché risolvono problemi diversi.

Per scegliere tra i due approcci è importante considerare diversi fattori, ad esempio il tipo di azienda che va protetta, i relativi utenti finali e i costi di ogni soluzione. SolarWinds MSP mette a disposizione entrambe le soluzioni per aiutare gli MSP a garantire il migliore livello di servizio ai clienti.

	ANTIVIRUS	EDR
Dati su contesto e forensi per le minacce	Limitati	Completi
Eliminazione, messa in quarantena, applicazione di rimedi e rollback	Solo eliminazione/ quarantena	Tutti
Utilizzo del database Common Vulnerabilities and Exposures (CVE)	No	Sì
Protezione utenti offline	Richiede definizioni aggiornate	Sì
Criteri per consentire/bloccare dispositivi USB per fornitore/classe/ seriale/prodotto	No	Sì
Criterio per contenere le minacce mediante disconnessione dalla rete	No	Sì
Criterio per controllare le impostazioni del firewall dell'endpoint	No	Sì
Previene e rileva una più ampia gamma di minacce quasi in tempo reale	No	Sì
Utilizzo delle risorse	Moderato	Lieve
Blocca le minacce "packer" (comportamento benigno)	No	Sì
Blocca le minacce "wrapper/variazioni/obfuscator"	Richiede definizioni aggiornate	Sì
Blocca gli attacchi senza file	No	Sì
Blocca le minacce sconosciute ("zero day")	Richiede definizioni aggiornate	Sì
Impiega il rilevamento basato su firme	Sì	Sì
Costo	Basso	Moderato
Profilo di rischio dell'utente	Basso	Elevato

Per maggiori informazioni: https://www.solarwindsmsp.com/it/prodotti/endpoint-detection-and-response

[1] "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Coveware. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate (consultato a giugno 2020).