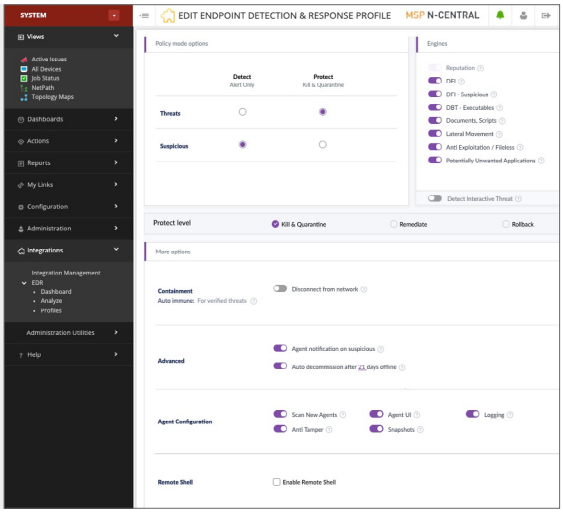
SCHEDA DELLE FUNZIONALITÀ

Endpoint Detection and Response

Funzionalità disponibile con SolarWinds N-Central

La funzionalità Endpoint Detection and Response (EDR) di SolarWinds® aiuta gli MSP a prevenire, rilevare e rispondere alle minacce in continuo cambiamento e a ripristinare rapidamente i sistemi a seguito di un attacco ransomware o di altri attacchi exploit. Tramite interventi correttivi e rollback è possibile annullare gli effetti di un attacco e di ripristinare gli endpoint allo stato precedente all'attacco al fine di ridurre i tempi di inattività per i clienti. Questa funzionalità è integrata in SolarWinds N-central®, così è possibile implementare e configurare senza problemi e rapidamente EDR oltre a rispondere a eventuali problemi da una singola dashboard.



SUPPORTO PER LA PREVENZIONE DEGLI ATTACCHI INFORMATICI

- Proteggete i clienti dalle nuove minacce senza attendere le scansioni ricorrenti o gli aggiornamenti alle definizioni delle firme
- Reagite alle minacce per gli endpoint quasi in tempo reale
- Applicate una protezione basata su criteri e personalizzata per i vostri clienti, bloccando o consentendo l'accesso alle unità USB e il traffico verso gli endpoint per determinare le misure più opportune

RILEVAMENTO DELLE MINACCE GRAZIE ALL'INTELLIGENZAARTIFICIALECOMPORTAMENTALE

- Stabilite in modo semplice quando e come è iniziato l'attacco
- Consultate riepiloghi o informazioni dettagliate sulle minacce da una singola dashboard

IMPLEMENTAZIONE E CONFIGURAZIONE SEMPLIFICATE

- Utilizzare le regole per automatizzare le modalità di implementazione di EDR
- Implementate EDR su dispositivi Windows® e MacOS®
- Sfruttate i flussi di lavoro PSA per gestire gli avvisi EDR
- Gestite le licenze EDR con l'ausilio del report relativo all'uso delle licenze
- Operate da una singola dashboard

RISPOSTE EFFICACI GRAZIE ALL'AUTOMAZIONE

- Risposte automatizzate per il rapido contenimento della minaccia
- Interventi correttivi per gli attacchi grazie all'annullamento dei relativi effetti
- Rollback degli attacchi mediante sostituzione dei file compromessi con le versioni precedenti all'attacco (solo su sistemi operativi Windows)