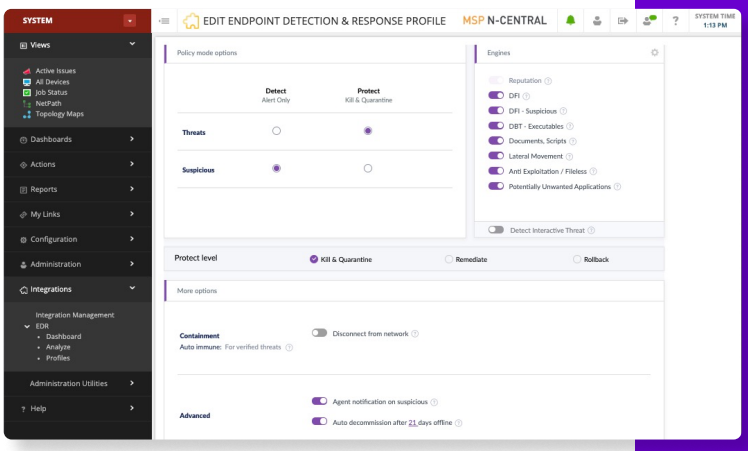
N-ABLE™

SCHEDA DELLE

Endpoint Detection and Response

Una funzionalità disponibile con N-able N-central



La funzionalità Endpoint Detection and Response (EDR) di N-able™ 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 N-central®, così è possibile implementare e configurare senza problemi e rapidamente EDR, oltre che 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'intelligenza artificiale comportamentale

- 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 dei report sull'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)