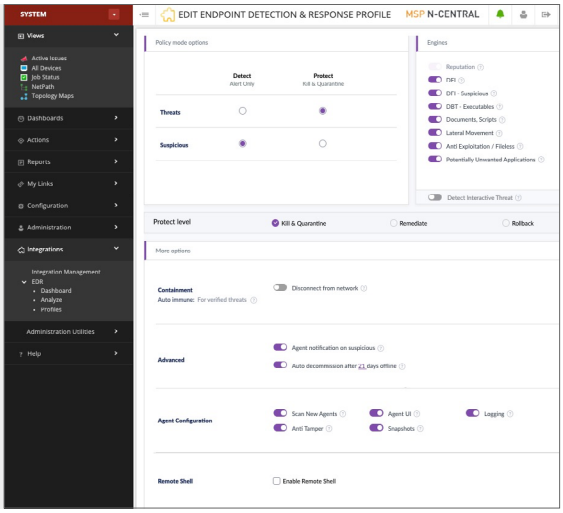
Endpoint Detection and Response:

Eine Funktion von SolarWinds N-central

SolarWinds® Endpoint Detection and Response (EDR) unterstützt MSP dabei, stets neuen Bedrohungen vorzubeugen, sie zu erkennen und darauf zu reagieren. Und ermöglicht im Falle eines erfolgreichen Angriffs mit Ransomware oder anderer Schadsoftware die schnelle Wiederherstellung von Daten. Fehlerbehebungen und Rollbacks können Angriffsspuren beseitigen und stellen den einwandfreien vorherigen Zustand der Endpunkte wieder her – das minimiert die Ausfallzeiten für den Kunden. Aufgrund der Einbindung in N-central® können Sie EDR schnell und einfach implementieren und konfigurieren und von nur einem Dashboard aus auf eventuelle Probleme reagieren.



CYBERANGRIFFE VERHINDERN

- Schutz vor neuesten Bedrohungen ohne langwierige Scans oder Updates von Signaturen für Virendefinitionen
- Reaktion auf Bedrohungen für Endpunkte nahezu in Echtzeit
- Durchsetzung kundenspezifischer Richtlinien durch gezieltes Blockieren/Zulassen des Zugriffs auf Dateien auf USB-Geräten und des Datenverkehrs auf Endpunkten

BEDROHUNGEN DURCH KI-ANALYSE VON VERHALTENSWEISEN ERKENNEN

- Einfache Ermittlung, wie und wann ein Angriff anfing
- Zusammenfassungen oder detaillierte Informationen zu Bedrohungen lassen sich von einem zentralen Dashboard abrufen

EINFACHE IMPLEMENTIERUNG UND KONFIGURATION

- Automatisierung der Implementierung von EDR anhand von Regeln
- Bereitstellung von EDR auf Windows®- und macOS®-Geräten
- Optimierung von PSA-Workflows zur Verwaltung von EDR-Warnungen
- Management von EDR-Lizenzen mit dem Lizenznutzungsbericht
- Alles von nur einem Dashboard aus

AUTOMATISIERUNG FÜR EFFEKTIVE REAKTIONEN

- Automatisierte Reaktionen für zügige Eindämmung von Bedrohungen
- Abfederung von Angriffen durch Beseitigung der Auswirkungen
- Datenwiederherstellung nach Angriffen durch Überschreibungen der beschädigten Dateien durch die intakten vorherigen Versionen (nur Windows-Betriebssystem)