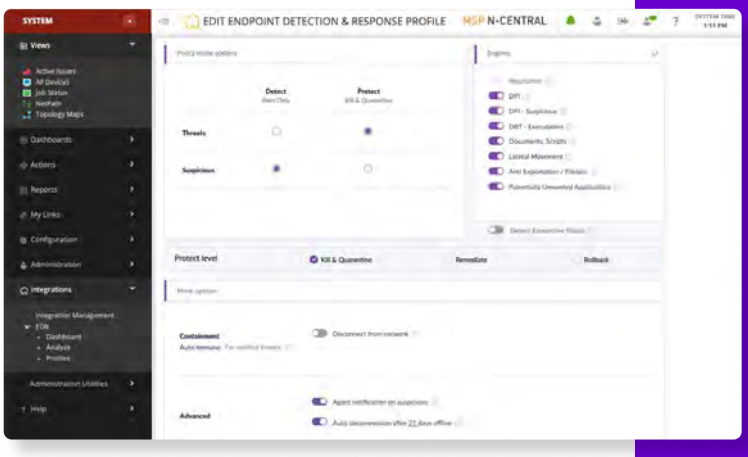
Endpoint Detection and Response:

Eine Funktion von N-able N-central



Mit N-able™ Endpoint Detection and Response (EDR) beugen MSP stets neuen Bedrohungen vor und können Angriffe erkennen und behandeln. Praktisch im Fall von Ransomware-Angriffen: Die befallenen Systeme lassen sich schnell wiederherstellen. 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

Mit Hilfe von Automatisierung wirksam reagieren

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