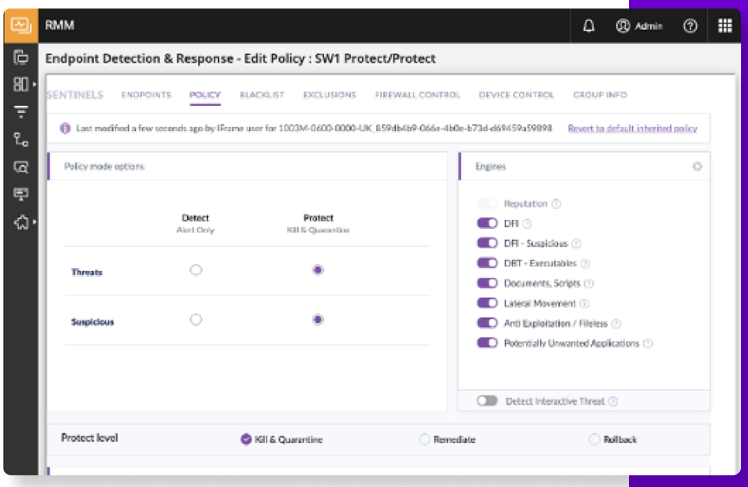
Endpoint Detection and Response

Eine integrierte Funktion von N-able RMM



Mit N-able™ Endpoint Detection and Response (EDR), einer in N-able RMM integrierten Funktion, beugen IT-Techniker stets neuen Bedrohungen vor und können Angriffe erkennen und behandeln. Praktisch im Fall von Ransomware-Angriffen: Die befallenen Systeme lassen sich schnell wiederherstellen. Optionen für die Fehlerbehebung und den Rollback helfen, Auswirkungen von Angriffen zu beseitigen, Systemausfallzeiten zu minimieren und Geräte in ihren vorherigen Zustand zurückzuversetzen. IT-Teams haben die Sicherheit aller Endgeräte stets zentral im Blick.

Cyberangriffe verhindern

- Schützt vor neuesten Bedrohungen ohne langwierige Scans oder Updates von Virusdefinitionen
- Reagiert praktisch sofort auf Bedrohungen an Endgeräten
- Richtliniengesteuerte Blockierung/Zulassung von USB-Geräten und Datenverkehr auf Endgeräten – an Ihre Geschäftsbedingungen anpassbar

Mit Hilfe von Automatisierung wirksam reagieren

- Automatisierte Reaktionen für zügige Eindämmung von Bedrohungen
- Unterstützt die Fehlerbehebung nach Angriffen durch Beseitigung der Auswirkungen

Mit SentinelOne

- N-able EDR enthält SentinelOne® Control
- Steuerung von Geräten und Endgeräte-Firewalls und Remote-Ausführung von Shellbefehlen
- Integrierte Lizenzberichte

Rollback bei Angriffen

- Ersetzen beschädigter Dateien durch intakte vorherige Versionen (nur Microsoft® Windows®)
- Einblick in den Endgeräteschutz durch Berichte aus dem RMM
- Plattformdienstüberprüfungen
- Einfache Installation und Verwaltung von Agenten über RMM

Bedrohungen durch KI-Analyse von Verhaltensweisen erkennen

- **Dashboard-Widgets mit Überblicks- und Detailberichten zum Status aller Geräte**
- **Warnungen zu befallenen Geräten und Dienstausfällen direkt im RMM-Dashboard**
- Einfache Ermittlung des Ursprungs und Zeitpunkts eines Angriffs
- Bedrohungscenter mit erweiterter Statusleiste: weniger Warnmeldungen und direkte Möglichkeit zur Reaktion von dort aus