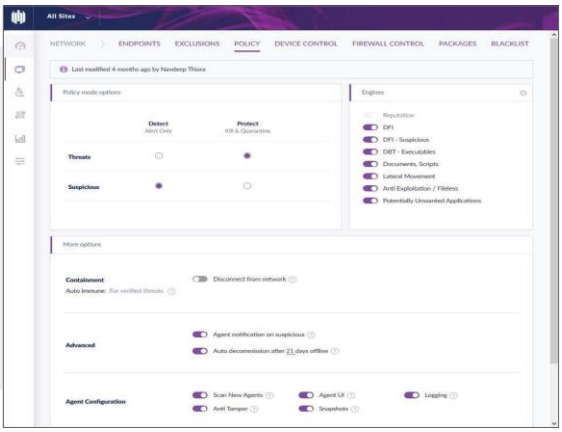
Endpoint Detection & Response:

A feature available with SolarWinds® RMM

Endpoint Detection and Response (EDR) helps prevent, detect, and respond to ever-changing threats—and recover quickly when ransomware or other exploits strike. Remediation and rollback help reverse the effects of an attack and restore endpoints to their pre-attack healthy state to minimize customer downtime.



PREVENT CYBERATTACKS

- ✓ Near real-time file analysis: The system can analyze files continuously, replacing time-intensive recurring scans.
- ✓ Signatureless approach: Fight back against the latest threats without having to wait for daily definition updates.
- ✓ Offline protection: Artificial intelligence data is stored on the endpoint to keep it protected while offline—and to help you avoid waiting for signature updates or waiting for the endpoint to connect to the cloud to check against reputation scores.
- ✓ Machine learning: The system uses machine learning to determine how to best respond to threats and adjusts those responses over time.
- ✓ Autonomous action: Leverage policy-based endpoint protection to neutralize threats at the endpoint automatically.

DETECT THREATS WITH BEHAVIORAL AI

- ✓ Behavioral artificial intelligence engines: The feature includes eight AI engines that analyze multiple data points to identify threats and determine if a response is necessary.
- ✓ Near real-time alerts: Discover threat activity quickly with alerts whenever a threat is detected or neutralized.
- ✓ Easy-to-use dashboard: View threat information at a glance on a single dashboard that includes quick links to key remediation actions.
- ✓ Executive insight and key findings: See aggregated data on threats over time. For example, you can view the current number of active threats, the number of threats found in a specified time period, and view threats and fixes over time.
- ✓ Forensics: See an overview and the storyline of an attack, so you can quickly understand the threat.
- ✓ Threat summaries: Review information on specific threats, such as dates they were identified, dates they were reported, and their file names. Summaries also include links to the Google threat database and Virus Total websites for more information.
- ✓ Raw data report: Dig into the details on threat information, including timing, activities taken by the file, and its SHA1 has

RESPOND EFFECTIVELY THROUGH AUTOMATION

- ✓ Custom policies: Use policy-driven protection tailored to your customer, which allows/blocks USB, allows/blocks endpoint traffic, and specifies the best automated response.
- ✓ Multiple recovery options: Choose your preferred recovery option after attacks—from partial recoveries to fully-automated responses.
- ✓ Enhanced quarantine: Select the Disconnect from Network option to prevent machines from further infecting the network.
- ✓ Automatic rollback: Attacks are automatically contained, and neutralized, and compromised files are automatically replaced by the last known healthy version.