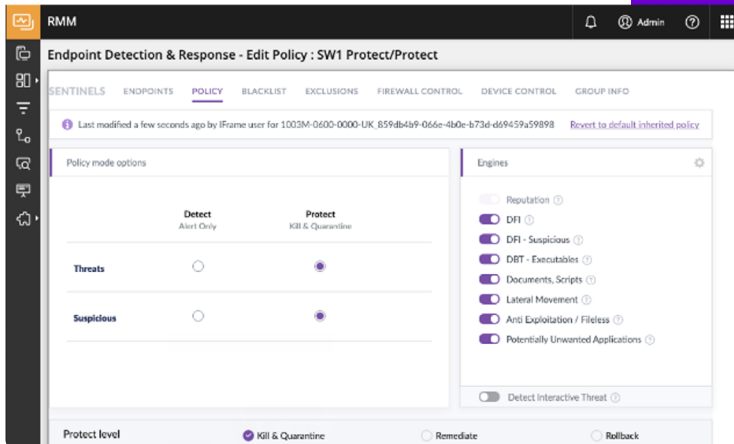# Endpoint Detection and Response

An integrated feature available with N-able RMM

N-able™ Endpoint Detection and Response (EDR), an integrated feature in N-able RMM, helps MSPs 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. Gain full monitoring and management of your endpoint security, all from a single dashboard.

Roll back attacks fast (Microsoft Windows OS only)

- Replace compromised files with pre-attack healthy versions (Microsoft® Windows® OS only)
- Gain transparency over endpoint protection by accessing native RMM reports
- Platform service checks
- Leverage RMM for easy agent deployment and management

Detect threats with behavioral AI

- At-a-glance dashboard widgets provide detailed or summary status on all devices
- Alerts for infected devices and service failure right in your RMM dashboard
- Easily determine how and when an attack started
- Threat center with enhanced status bar reduces alerts, and allows for mitigation without leaving the page

Prevent cyberattacks

- Help protect against the latest threats without waiting for recurring scans or updates to signature definitions
- Respond to threats at the endpoint almost immediately
- Allow/block USBs and endpoint traffic via policy-driven protection—customized for your end users—to determine the appropriate response

Powered by sentinelone

- N-able EDR is equivalent to SentinelOne® Control
- Includes device control, endpoint firewall control, and remote shell execution
- Integrated license reports

Respond effectively through automation

- Automate responses for quick threat containment
- Help remediate attacks by reversing the effects