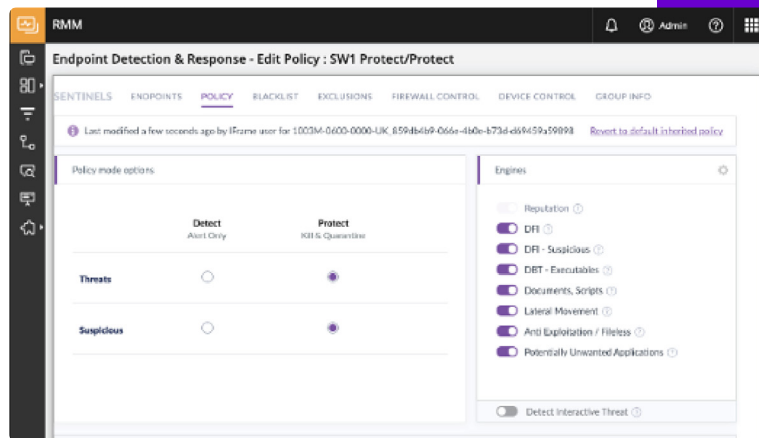


# Endpoint Detection and Response

An integrated feature available with N-able RMM



N-able™ Endpoint Detection and Response (EDR), an integrated feature in N-able RMM, helps IT teams prevent, detect, and respond to ever-changing threats—and recover quickly when ransomware or other threats strike. Remediation and rollback help reverse the effects of an attack and restore endpoints to their pre-attack healthy state to minimize downtime. Gain full monitoring and management of your endpoint security—all from a single dashboard.

## 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 business—to determine the appropriate response

## Respond effectively through automation

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

## Powered by SentinelOne

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

## Roll back attacks fast

- Replace compromised files with pre-attack healthy versions quickly (Microsoft® Windows® OS only)
- Gain transparency over endpoint protection by accessing native RMM reports
- Run 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