Introduction to Integrated Endpoint Detection and Response (EDR) in RMM

Monitor and manage your endpoints within a single dashboard—from day one

Security threats multiply and morph daily. Once a new threat is resolved, cybercriminals find another angle to exploit. Customers expect you to stay on top of these threats—and keep them protected.

N-able™ RMM includes integrated N-able Endpoint Detection and Response (EDR), powered by SentinelOne®. This means you can easily roll out, configure, and monitor endpoint protection, quickly contain threats, and minimize customer downtime.

Q. What is EDR?
Unlike traditional antivirus, EDR offers continuous monitoring, collects and stores data, and uses behavioral AI to detect threats. If it detects a threat on a device, the EDR agent can automatically quarantine the threat to contain it and reverse the effects of the attack by rolling back to a healthy version (Windows® OS only). It can also provide valuable data for further analysis.

Q. Why adopt integrated EDR?
You need cybersecurity protection for yourself and your customers that goes beyond traditional antivirus. As workforces become increasingly distributed, EDR can help you take your security services—and your MSP business—to the next level:

• Protect your customers with enterprise-grade security
• Help generate additional recurring revenue
• Gain visibility and insights into attacks
• Remediate issues quickly and reduce customer churn
• Provide peace of mind with advanced threat protection

Q. What does integrated mean?
Our EDR console is embedded into the RMM solution to make your job easier. You can use RMM and its automation features to:

• Deploy and update the latest EDR agent versions for Windows OS devices using native RMM functionality
• Quickly configure EDR policies, exclusions, and other settings
• Leverage PSA workflows to manage EDR alerts, including notification of device infections
• View the at-a-glance dashboard widgets for detailed or summary status on all devices
• Reduce alerts and mitigate threats via the threat center with its enhanced status bar—without leaving the page
• Automate platform service checks

Q. How can I request a trial?
If you already have RMM, you can activate a 30-day trial of integrated EDR from within the application. Just follow these steps:

1. Activate your trial in our new Integration Management View for RMM, available in the left-hand navigation menu
2. Expand the Integrations menu in the left navigation
3. Select Integration Management
4. Click Activate
5. Create your EDR policies
6. Enable the EDR feature through RMM

Q. Can I activate an integrated EDR trial if I am currently using the standalone version with RMM?
Yes. You can migrate existing EDR agents deployed on endpoints already managed by RMM, and already registered to an N-able EDR management console, to integrated EDR.

Q. Is the asset-tracking-only option (which requires no monitoring fee) available for RMM with Integrated EDR?
Yes. The asset-tracking-only option is available for integrated EDR in RMM. To ensure your device is asset only and does not incur the monitoring fee for a fully managed device, please review this knowledge base article.

Q. What widgets are available to me in the dashboard?
• Unresolved Threats: investigate highest priority threats
• Infected Endpoints: view endpoints needing inspection
• S1 Agents Requiring Attention: uncover agents that need rebooting or other action
• S1 Agent Network Status: see availability of SentinelOne agents
• S1 Agent Version Coverage: observe agent version metrics in-network
• Threat Detection by Engine: assess threat types

Q. What are the migration considerations if I’m already using SentinelOne EDR?
N-able Standalone EDR:
If you have already deployed standalone EDR agents to RMM-managed devices, these agents will be available for a takeover migration, which will quickly and easily transition the EDR agent from the existing standalone dashboard to the new integrated dashboard.

While this takeover is an automated process, it requires creating appropriate policies and manually enabling (as described above) the EDR feature on the endpoints or set of endpoints. Creation of policies in the integrated interface does not provide for any direct policy or exclusion migration from standalone EDR to integrated EDR.

If you have the standalone version of N-able EDR, once you enable the integrated EDR feature for RMM your devices will automatically move to the integrated dashboard. As such, these endpoints will no longer be visible on the standalone EDR dashboard. Instead, they’ll now be visible and managed on the integrated dashboard.
At the conclusion of the trial period, you’ll need to speak with an N-able account representative to confirm the transition of license commitment from standalone to integrated. If an integrated EDR trial expires, there will be a minimum seven-day grace period to remove EDR agents from devices included in the trial.

**SentinelOne EDR that is not provided by N-able:**

The takeover migration will not support a SentinelOne agent that is not managed by the standalone version of N-able EDR. Attempts to enable the EDR feature on such devices will result in a failed state for the EDR feature deployment.

The takeover migration will continue attempts to migrate endpoints until either:

- The EDR feature on the endpoint is disabled, or
- The SentinelOne agent from another provider is removed and the N-able EDR agent can be installed

**Q. What else should I know about the integrated version?**

You can only deploy integrated EDR on RMM-managed devices. Currently, integrated EDR does not support macOS® or Linux® devices.

We’re committed to making the EDR experience with RMM a world-class experience. This is just the beginning of the journey.

Note: We recommend testing EDR in a non-production environment—configuring policies to use detect mode during testing—before deploying widely.

**If you have questions or need support, please contact your sales rep or visit success.n-able.com.**

---

**About N-able**

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

*n-able.com*