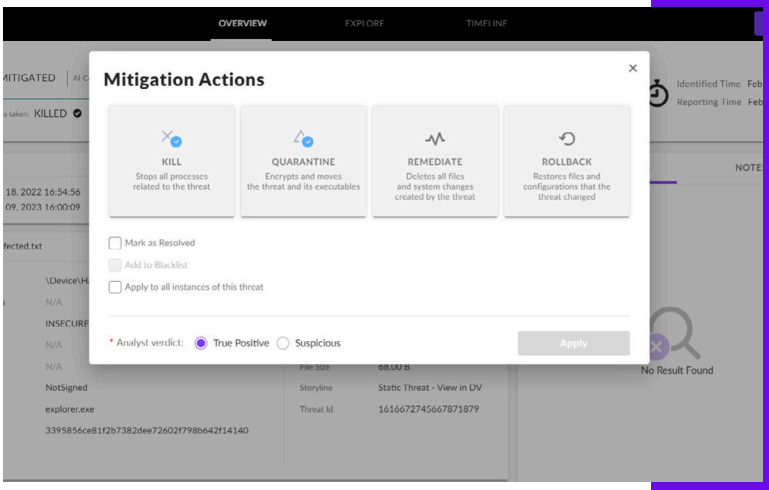
N-ABLE™ with LAPIS-IT

Endpoint Detection and Response

A feature available with N-able N-sight RMM

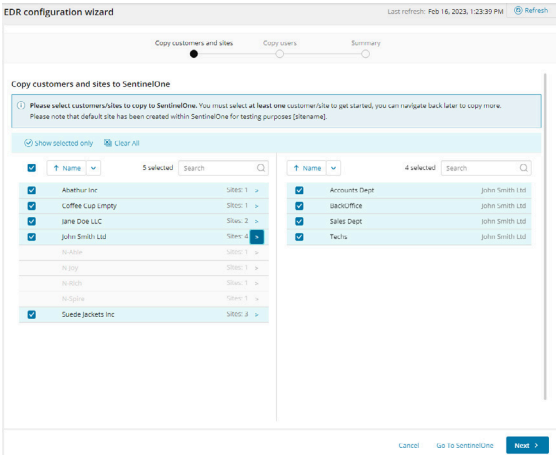


N-able™ Endpoint Detection and Response (EDR) helps MSPs and IT departments prevent, detect, and quickly respond to ever-changing cyberthreats with behavioral AI threat detection, automated remediation, and rollback.

Powered by SentinelOne, N-able EDR is a feature of N-able N-sight RMM allowing MSPs to get the best of both worlds: endpoint detection and response paired with remote monitoring and management for effective endpoint protection.

Unify endpoint management and protection with N-sight and SentinelOne

- Easily map your client and user hierarchies into SentinelOne using the uniquely designed EDR configuration wizard
- Individually or mass deploy Windows and Mac devices
- Monitor your devices in N-sight and access SentinelOne's direct console when they need attention
- Seamlessly log in from N-sight to the SentinelOne console to review and action threats
- Use SentinelOne's full EDR capabilities, including native reporting, alerts, and granular notifications
- Access SentinelOne's APIs to further integrate other third-party party security tools
- Get direct access to the SentinelOne console
- Get one unified N-able bill for all customers using N-able services, directly in your N-sight account



LAPIS-IT

Help prevent cyberattacks

- Protect against the latest threats without waiting for recurring scans or malware definition updates
- Enforce policy-driven protection tailored to your customers: allow/block USB and device connections as needed
- Get device and endpoint firewall control, network quarantine, and anti-tampering capabilities

Accelerate threat investigation

- Investigate using readily available threat intelligence from leading third-party feeds and SentinelOne sources
- Visualize threat activity—the full chain of events making up an attack—to quickly understand its context, root cause, and lateral movements

Leverage multiple AI detection engines

- Harness the power of AI to analyze new threat patterns and machine learning to evolve responses
- Detect malicious activities such as memory exploitation with behavioral AI
- Detect signature-less advanced file-based malware with static AI

Respond effectively through automation

- Automate quick threat containment, as well as "kill", quarantine, and remediation actions
- Rollback endpoints and compromised files to their pre-attack healthy state in case of ransomware (Windows OS only).

N-able EDR is powered by SentinelOne

leader in the 2022 MITRE Engenuity™ ATT&CK® Evaluation:

- 100% Protection & Detection
- Highest Visibility & Analytic Coverage
- 100% Real-Time. Zero Detection Delays.

About Lapis IT BV

Lapis IT BV is a MSP partner of N-able. We provide support to customers whom are aware of the cost and damage of downtime, data recovery, data loss or reputation damage.

Contact:
Telephone : +31(0) 35 712 33 90
E-mail : info@lapisit.nl
Website : www.lapisit.nl

About N-able

N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com