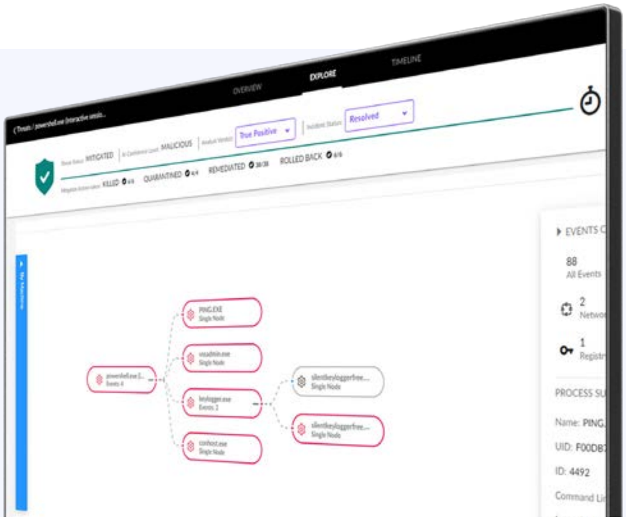
N-ABLE™

DATASHEET

Endpoint Detection and Response

A standalone N-able solution powered by SentinelOne®

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. Security professionals benefit from easy automation manager policy (AMP)-based deployment and an EDR status check within the N-able remote monitoring and management platforms.



Leverage multiple AI detection engines

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

Help prevent cyber attacks

- Protect against the latest threats without waiting for recurring scans or malware definition updates
- Enforce policy-driven protection tailored to your users: allow/block USB and device connections as needed

Respond effectively through automation

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

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

Powered by SentinelOne®,

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

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

Easily connect to third-party systems

- Streamline Syslog events to your SIEM
- Leverage granular notifications to prioritize and route tickets through your PSA ticketing system
- Leverage API services

Based on the Singularity™ platform

- Singularity™ Control and Complete platform packages available
- Includes device and endpoint firewall control, remote shell execution, network quarantine, and anti-tampering

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.

Connection® we solve IT®

Contact an Account Manager for more information.
1.800.800.0014 ▪ www.connection.com/N-able

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein. 1880015 0822