# FEATURE SHEET



# **Endpoint Detection and Response:**

A feature available with N-able N-central

SYSTEM		EDIT EN	IDPOINT DET	ECTION & RESPONSE PRO	DFILE MSP N-C	ENTRAL	۵ 🔺	₽	-	?
3 Views	× I	Policy mode options			Engin	15			0	
Active Issues All Devices Job Status NetPath Topology Maps			Detect Alert Only	Protect Kill & Quarantine	•	Reputation () DFI () DFI - Suspicious ()				
) Dashboards	>	Threats	0	•		DBT - Executables ① Documents, Scripts ④				
	•	Suspicious	٠	0		Lateral Movement  Anti Exploitation / Fileless				
	<b>`</b>				•	Potentially Unwan	ed Application	s 🕐		
	•									
Configuration	>					Detect Interactive	Threat			
	•	Protect level		🔮 Kill & Quarantine	O Remediate		O Rollbad	c.		
Integrations	~	More options								
Integration Management • EDR • Dashboard • Analyze • Profiles		Containment Auto immune: For v	rerified threats ①	Disconnect from network (?)						
Administration Utilities	>									
	,	Advanced		Agent notification on suspicion Auto decommission after 21.d						

N-able<sup>™</sup> Endpoint Detection and Response (EDR) helps MSPs prevent, detect, and respond to ever-changing threats—and recover quickly when ransomware or other exploits strike. Remediation and rollback can reverse the effects of an attack and restore endpoints to their pre-attack healthy state to minimize customer downtime. This feature is integrated into N-central<sup>®</sup>, so you can easily and quickly roll out and configure EDR, as well as respond to issues from a single dashboard.

#### Help prevent cyberattacks

- Protect against the latest threats without waiting for recurring scans or updates to definition signatures
- Respond to endpoint threats in near real time
- Enforce policy-driven protection tailored to your customers: allow/block USB and endpoint traffic to determine the appropriate response

#### Detect threats with behavioral AI

- Easily determine how and when an attack began
- View summaries or detailed threat information from a single dashboard

## Easily roll out and configure

- Use rules to automate how EDR is deployed
- Deploy EDR to Windows<sup>®</sup> and macOS<sup>®</sup> devices
- Leverage PSA workflows to manage EDR alerts
- Manage EDR licenses with the license usage report
- Operate from a single dashboard

## Respond effectively through automation

- Automate responses for quick threat containment
- Remediate attacks by reversing the effects
- Roll back attacks by replacing compromised files with pre-attack healthy versions (Windows OS only)