N-ABLE | XDR v MDR:

Selecting the best solution for your organization

Organizations face increasing cyber threats and regulatory obligations with exhausted resources and limited budgets. That's why leveraging existing security investments to help maximize the return from endpoint, cloud access, VPNs, perimeter security, and logging systems is crucial.

This chart provides three primary threat management services: Managed Detection and Response (MDR), Extended Detection and Response (XDR), and N-able MDR. Compare insights on each service to help you decide where to invest your limited budget and maximize your cyber protection.

	MDR	XDR	N-able MDR
Who manages what?	Managed Service	Managed Service or Customer Manages	Managed Service or Customer Manages
Data Sources	◢ Endpoint ◢ Network Traffic ◢ Cloud services	◢ Endpoint ◢ Network Traffic ◢ Perimeter ◢ Cloud services ◢ Active Directory ◢ Email	◢ Endpoint ◢ Network Traffic ◢ Perimeter ◢ Cloud services ◢ Active Directory ◢ Email
Detections	◢ Malware/IoCs ◢ Fileless attacks	◢ Malware/IoCs ◢ Fileless attacks ◢ Behavioral anomalies ◢ Machine Learning	◢ Malware/IoCs ◢ Fileless attacks ◢ Behavioral anomalies ◢ Machine Learning
Investigation	Included in SOC service (varies)	◢ Requires managed SOC service ◢ SOC conducts investigations	◢ Included in SOC service ◢ Included in SOC service
Response	MDR SOC Service: Manage Yourself	Requires managed SOC service	SOC Service: Extended Security Team
Remediation	◢ Endpoint isolation and blocking ◢ Traffic blocking (source IP/DNS) ◢ Cloud access reset or disabling	◢ Endpoint isolation and blocking ◢ Traffic blocking (source IP/DNS) ◢ Account/Group reset or disabling ◢ Cloud access reset or disabling	◢ Endpoint isolation and blocking ◢ Traffic blocking (source IP/DNS) ◢ Account/Group reset or disabling ◢ Cloud access reset or disabling
Reporting	Based on SOC capability	◢ Requires managed SOC service ◢ Co-managed reporting	◢ Detections ◢ Investigations ◢ Custom reports ◢ Compliance insights ◢ Compliance examiner reports ◢ Executive summaries
Threat Intelligence	Basic	Basic	◢ Dedicated Threat Intelligence team and researchers ◢ Threat intelligence feed ◢ Dark web monitoring ◢ Managed deception technology
Deployment Speed	◢ Requires services licenses first ◢ Weeks to configure and tune	◢ Requires services licenses first ◢ Weeks to configure and tune	◢ Deployed in days ◢ Agent deploys via global policy object (GPO)
Visibility	SOC requests for reports or investigation information	Co-management varies	◢ 100% fully visible to customer: The customer sees and has access to the same portal as the SOC ◢ Real-time customer reporting
Context	◢ SOC requests for reports or investigation information ◢ Limited compliance reporting	Co-management varies	◢ A simplified view: The customer sees and has access to the same portal as the SOC ◢ Threats and detections ◢ At-risk programs ◢ Network Health Policy violations ◢ Compliance insights

Illuminate Threats and Eliminate Risks

Learn more about how N-able' Managed Detection and Response Services and Security Operations Platform can empower your team to illuminate threats, reduce cyber risk, and command authority.

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